ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

Developer Guide - Cloud Essentials and Security

Product Version: 1907, Internal: V3.8.0

Document Version: 20200918

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Apsara Stack console 74
1.1. API overview 74
1.2. Call methods 74
1.2.1. Common parameters 74
1.2.2. Signature mechanism 75
1.2.3. Request structure 76
1.2.4. Response structure 77
1.3. Region-related APIs 81
1.3.1. getRegionList 81
1.3.2. getZoneList 90
1.4. User center-related APIs 101
1.4.1. User-related APIs 101
1.4.1.1. addUserInfo 101
1.4.1.2. ModifyUser 104
1.4.1.3. getUserList 105
1.4.2. Role-related API 109
1.4.2.1. getRolePage 109
1.4.3. Department-related APIs 112
1.4.3.1. addDepartment 112
1.4.3.2. delDepartment 113
1.4.3.3. editDepartment 114
1.4.3.4. getDeptRootTree 116
1.4.4. Project-related APIs 118
1.4.4.1. createProject 118
1.4.4.2. deleteProject 119
1.4.4.3. getProjectList 120

1.5. ECS-related APIs 122
1.5.1. ECS instance-related APIs 122
1.5.1.1. createDtcenterEcsInstance 123
1.5.1.2. deleteEcsInstance 127
1.5.1.3. resetInstancePassword 128
1.5.1.4. getCloudEcsList 129
1.5.1.5. getEcsDetailByInstanceId 136
1.5.1.6. startEcsInstance 141
1.5.1.7. rebootEcsInstance 142
1.5.1.8. stopEcsInstance 144
1.5.2. Security group-related APIs 145
1.5.2.1. createSecGroup 145
1.5.2.2. createSecGroupRule 147
1.5.2.3. deleteSecGroup 150
1.5.2.4. delSecGroupRule 151
1.5.2.5. modifySecGroup 154
1.5.2.6. getSecurityGroupList 155
1.5.2.7. getRuleList 160
1.5.2.8. getSecurityGroupRulesOfEcs 162
1.5.2.9. getSecurityGroupList 165
1.5.2.10. joinInstanceSecGroup 167
1.5.2.11. leaveSecurityGroup 169
1.5.3. Disk-related APIs 170
1.5.3.1. createCloudDisk 170
1.5.3.2. deleteCloudDisk 172
1.5.3.3. getCloudDiskList 173
1.5.3.4. getCloudDiskInfo 178
1.5.3.5. attachCloudDisk 183

1.5.3.6. detachCloudDisk 185
1.5.4. Image-related APIs 186
1.5.4.1. getImageList 186
1.6. RDS-related APIs 190
1.6.1. RDS instance-related APIs 190
1.6.1.1. createRdsInstance 190
1.6.1.2. deleteRdsInstance 194
1.6.1.3. modifyRdsInstanceSpec 195
1.6.1.4. getRdsInstanceList 197
1.6.1.5. getRdsInstanceAttribute 201
1.6.2. RDS database-related APIs 203
1.6.2.1. createRdsDatabase 204
1.6.2.2. deleteRdsDatabase 206
1.6.2.3. getRdsDatabaseList 207
1.6.3. RDS account-related APIs 209
1.6.3.1. createRdsAccount 210
1.6.3.2. deleteRdsAccount 212
1.6.3.3. getRdsAccountList 213
1.6.3.4. grantRdsAccountPrivilege 215
1.6.3.5. revokeRdsAccountPrivilege 217
1.6.3.6. resetRdsAccountPassword 218
1.7. SLB-related APIs 220
1.7.1. SLB instance-related APIs 220
1.7.1.1. createCloudSlbEntry 220
1.7.1.2. delCloudSlbEntry 223
1.7.1.3. setCloudSlbEntry 224
1.7.1.4. getCloudSlbEntryBaseInfoById 226
1.7.1.5. getCloudSlbList 229

1.7.2. SLB listener-related APIs 232
1.7.2.1. setHttpServiceListener 232
1.7.2.2. setTcpServiceListener 238
1.7.2.3. deleteServiceListener 241
1.7.2.4. getServiceListener 243
1.7.2.5. startServiceListener 250
1.7.2.6. stopServiceListener 251
1.7.3. SLB backend server-related APIs 253
1.7.3.1. addBackendServer 253
1.7.3.2. removeBackendServer 255
1.7.3.3. setBackendServer 256
1.7.3.4. getBackendServerList 258
1.7.3.5. getBackendServerHealthStatus 262
1.8. OSS-related APIs 265
1.8.1. Bucket attribute-related APIs 265
1.8.1.1. setBucketWebsite 265
1.8.1.2. getBucketWebsite 266
1.8.1.3. setBucketACL 268
1.8.1.4. getBucketACL 270
1.8.2. Bucket-related APIs 271
1.8.2.1. getBucketList 271
1.8.2.2. deleteBucket 274
1.8.2.3. createBucket 276
1.8.2.4. getBucketInfo 278
1.8.2.5. checkBucketName 280
1.8.3. Object-related APIs 281
1.8.3.1. addNewFolder 281
1.8.3.2. deleteObject 283

1.8.3.3. GetObjectList 284
1.8.3.4. getObjectAddress 287
1.8.3.5. getOssAccessKey 289
1.9. VPC-related APIs 290
1.9.1. createVpc 290
1.9.2. deleteVpc 292
1.9.3. modifyVpc 293
1.9.4. getVpcs 295
1.9.5. getVpcById 298
1.9.6. getVpcNetworkSegment 300
1.9.7. VSwitch-related APIs 302
1.9.7.1. createVswitch 302
1.9.7.2. deleteVswitch 304
1.9.7.3. modifyVswitch 306
1.9.7.4. getVswitchList 308
1.10. Monitoring center-related APIs 309
1.10.1. ECS monitoring-related APIs 309
1.10.1.1. InstallEcsCmsAgent 309
1.10.1.2. getMonitorHistory 310
1.10.1.3. getMonitorCurrent 312
1.10.2. OSS monitoring-related APIs 316
1.10.2.1. GetMonitorHistory 316
1.10.2.2. getMonitorCurrent 318
1.10.3. RDS monitoring-related APIs 321
1.10.3.1. getMonitorHistory 321
1.10.3.2. getMonitorCurrent 323
1.10.4. SLB monitoring-related APIs 329
1.10.4.1. getMonitorHistory 329

1.10.4.2. getMonitorCurrent 331
1.11. Data type 335
1.11.1. RDS data types 335
1.11.1.1. DBInstanceAttribute 335
1.11.1.2. DBInstanceEntity 337
1.11.1.3. DBInstanceNetInfo 339
1.11.1.4. DBInstanceStatus 339
1.11.1.5. ReadOnlyDBInstanceId 340
1.11.1.6. DBDatabaseEntity 340
1.11.1.7. DBAccountPrivilegeInfo 340
1.11.1.8. DBAccountEntity 340
1.11.1.9. DBDatabasePrivilege 341
1.11.1.10. DatabasePrivilege 341
1.11.2. OSS data types 341
1.11.2.1. BucketEntity 341
1.11.2.2. BucketInfo 342
1.11.2.3. ObjectInfo 343
1.11.3. VPC data types 343
1.11.3.1. NetworkEntity 343
1.11.3.2. VpcDetailInfo 344
1.11.3.3. VpcEntity 344
1.11.3.4. VrouterDetailInfo 345
1.11.3.5. vrouterRule 345
1.11.3.6. VswitchEntity - Alibaba Cloud regions 346
1.11.4. User center data types 346
1.11.4.1. AuthorizationDetail 346
1.11.4.2. PrivilegeEntity 347
1.11.4.3. RoleDetail 347

1.12. Appendix 348
1.12.1. Apsara resource table 348
1.12.2. Monitoring metrics in CoudMonitor 350
2.Cloud products 355
2.1. Elastic Compute Service (ECS) 355
2.1.1. API reference 355
2.1.1.1. List of operations 355
2.1.1.2. Make API requests 359
2.1.1.2.1. Overview 359
2.1.1.2.2. Request structure 360
2.1.1.2.3. API authorization 360
2.1.1.2.4. Signature mechanism 361
2.1.1.2.5. Responses 363
2.1.1.3. RAM authentication 364
2.1.1.4. Common parameters 367
2.1.1.5. Instances 369
2.1.1.5.1. RunInstances 369
2.1.1.5.2. CreateInstance 386
2.1.1.5.3. StartInstance 405
2.1.1.5.4. StopInstance 407
2.1.1.5.5. RebootInstance 409
2.1.1.5.6. DeleteInstance 411
2.1.1.5.7. AttachInstanceRamRole 413
2.1.1.5.8. DetachInstanceRamRole 416
2.1.1.5.9. DescribeInstanceStatus 419
2.1.1.5.10. DescribeInstances 422
2.1.1.5.11. DescribeInstanceVncUrl 427
2.1.1.5.12. DescribeUserdata 429

2.1.1.5.13. DescribeInstanceRamRole 431
2.1.1.5.14. DescribeInstanceTypeFamilies 433
2.1.1.5.15. DescribeInstanceTypes 435
2.1.1.5.16. ModifyInstanceAttribute 437
2.1.1.5.17. ModifyInstanceVpcAttribute 440
2.1.1.5.18. ModifyInstanceVncPasswd 443
2.1.1.6. Deployment set 444
2.1.1.6.1. CreateDeploymentSet 444
2.1.1.6.2. DeleteDeploymentSet 448
2.1.1.6.3. ModifyDeploymentSetAttribute 449
2.1.1.6.4. DescribeDeploymentSets 451
2.1.1.6.5. DescribeDeploymentSetTopology 453
2.1.1.7. Disks 454
2.1.1.7.1. CreateDisk 454
2.1.1.7.2. DescribeDisks 459
2.1.1.7.3. AttachDisk 466
2.1.1.7.4. DetachDisk 469
2.1.1.7.5. ModifyDiskAttribute 471
2.1.1.7.6. ReInitDisk 475
2.1.1.7.7. ResetDisk 477
2.1.1.7.8. ReplaceSystemDisk 480
2.1.1.7.9. ResizeDisk 484
2.1.1.7.10. DeleteDisk 486
2.1.1.7.11. migrate_disk 487
2.1.1.7.12. query_load_progress 489
2.1.1.8. Snapshots 490
2.1.1.8.1. CreateSnapshot 490
2.1.1.8.2. DeleteSnapshot 493

2.1.1.8.3. DescribeSnapshots 494
2.1.1.8.4. ImportSnapshot 499
2.1.1.8.5. ExportSnapshot 501
2.1.1.8.6. DescribeSnapshotLinks 503
2.1.1.8.7. CreateAutoSnapshotPolicy 508
2.1.1.8.8. DeleteAutoSnapshotPolicy 510
2.1.1.8.9. ModifyAutoSnapshotPolicyEx 511
2.1.1.8.10. DescribeAutoSnapshotPolicyEx 513
2.1.1.8.11. ApplyAutoSnapshotPolicy 515
2.1.1.8.12. CancelAutoSnapshotPolicy 516
2.1.1.9. Images 517
2.1.1.9.1. CreateImage 517
2.1.1.9.2. DescribeImages 523
2.1.1.9.3. ModifyImageAttribute 528
2.1.1.9.4. DeleteImage 531
2.1.1.9.5. CopyImage 532
2.1.1.9.6. CancelCopyImage 536
2.1.1.9.7. ModifyImageSharePermission 538
2.1.1.9.8. DescribeImageSharePermission 541
2.1.1.9.9. ImportImage 543
2.1.1.9.10. ExportImage 550
2.1.1.10. Network 553
2.1.1.10.1. AllocatePublicIpAddress 554
2.1.1.10.2. ModifyInstanceNetworkSpec 556
2.1.1.11. Security groups 559
2.1.1.11.1. CreateSecurityGroup 559
2.1.1.11.2. AuthorizeSecurityGroup 562
2.1.1.11.3. AuthorizeSecurityGroupEgress 568

2.1.1.11.4. RevokeSecurityGroup 574
2.1.1.11.5. RevokeSecurityGroupEgress 578
2.1.1.11.6. JoinSecurityGroup 583
2.1.1.11.7. LeaveSecurityGroup 586
2.1.1.11.8. DeleteSecurityGroup 588
2.1.1.11.9. DescribeSecurityGroupAttribute 589
2.1.1.11.10. DescribeSecurityGroups 593
2.1.1.11.11. DescribeSecurityGroupReferences 596
2.1.1.11.12. ModifySecurityGroupAttribute 599
2.1.1.11.13. ModifySecurityGroupPolicy 601
2.1.1.11.14. ModifySecurityGroupRule 603
2.1.1.12. SSH key pairs 609
2.1.1.12.1. CreateKeyPair 609
2.1.1.12.2. ImportKeyPair 612
2.1.1.12.3. AttachKeyPair 614
2.1.1.12.4. DetachKeyPair 617
2.1.1.12.5. DeleteKeyPairs 619
2.1.1.12.6. DescribeKeyPairs 621
2.1.1.13. Elastic network interfaces 624
2.1.1.13.1. CreateNetworkInterface 624
2.1.1.13.2. AttachNetworkInterface 628
2.1.1.13.3. DescribeNetworkInterfaces 631
2.1.1.13.4. DetachNetworkInterface 636
2.1.1.13.5. DeleteNetworkInterface 638
2.1.1.13.6. ModifyNetworkInterfaceAttribute 640
2.1.1.14. Regions and zones 643
2.1.1.14.1. DescribeRegions 643
2.1.1.14.2. DescribeZones 644

2.1.1.15. Tags 647
2.1.1.15.1. AddTags 648
2.1.1.15.2. RemoveTags 650
2.1.1.15.3. DescribeTags 653
2.1.1.16. Other operations 656
2.1.1.16.1. DescribeTasks 656
2.1.1.16.2. DescribeTaskAttribute 659
2.1.1.16.3. CancelTask 663
2.1.1.17. Data types 664
2.1.1.17.1. AvailableResourceCreationType 664
2.1.1.17.2. AvailableDiskCategoriesType 665
2.1.1.17.3. BandwidthPackageItemType 665
2.1.1.17.4. DiskItemType 666
2.1.1.17.5. DiskSetType 668
2.1.1.17.6. ImageType 669
2.1.1.17.7. InstanceMonitorDataType 670
2.1.1.17.8. InstanceStatusItemType 671
2.1.1.17.9. InstanceTypeItemType 671
2.1.1.17.10. IpAddressSetType 672
2.1.1.17.11. InstanceStatusSetType 672
2.1.1.17.12. NetworkInterfaceType 672
2.1.1.17.13. NetworkInterfaceSet 673
2.1.1.17.14. OperationLocksType 674
2.1.1.17.15. PermissionSetType 674
2.1.1.17.16. PermissionType 675
2.1.1.17.17. RegionType 675
2.1.1.17.18. SnapshotType 676
2.1.1.17.19. SecurityGroupIdSetType 677

2.1.1.17.20. SecurityGroupSetType 677
2.1.1.17.21. SecurityGroupItemType 677
2.1.1.17.22. AutoSnapshotPolicyType 678
2.1.1.17.23. AutoSnapshotExecutionStatusType 679
2.1.1.17.24. DiskDeviceMapping 680
2.1.1.17.25. VpcSetType 680
2.1.1.17.26. EipAddressAssociateType 681
2.1.1.17.27. EipAddressSetType 682
2.1.1.17.28. InstanceAttributesType 682
2.1.1.17.29. VpcAttributesType 684
2.1.1.17.30. DiskMonitorDataType 684
2.1.1.17.31. AccountType 685
2.1.1.17.32. ShareGroupType 685
2.1.1.17.33. TagSetItem 686
2.1.1.17.34. ResourceTypeCountItem 686
2.1.1.17.35. AvailableInstanceTypesType 686
2.1.1.17.36. InstanceTypeFamilyItemType 686
2.1.1.17.37. AvailableResourcesType 687
2.1.1.17.38. TaskType 687
2.1.1.17.39. KeyPairSetType 688
2.1.1.17.40. KeyPairItemType 688
2.1.1.17.41. OperationProgressType 689
2.1.1.17.42. RelatedItemType 689
2.1.1.17.43. AccessPointSetType 690
2.1.1.17.44. AccessPointType 690
2.1.1.17.45. BandwidthPackageSetType 691
2.1.1.17.46. ForwardEntrySetType 691
2.1.1.17.47. ForwardEntryItemType 691

2.1.1.17.48. PublicIpAddressSetType 692
2.1.1.17.49. PublicIpAddressItemType 692
2.1.1.17.50. ZoneType 693
2.1.1.18. Appendix 693
2.1.1.18.1. Instance types 693
2.1.1.18.2. Glossary 717
2.1.1.18.3. Instance statuses 718
2.1.1.18.4. Common errors 718
2.1.1.18.5. Disk categories 721
2.1.1.18.6. How to ensure idempotency 721
2.1.1.18.7. API responses when an instance is locked for... 722
2.1.1.18.8. ISO 8601 date and time formats 724
2.1.2. SDK reference 724
2.1.2.1. Java SDK 724
2.1.2.1.1. Quick start 724
2.1.2.1.2. Use the Java SDK 726
2.1.2.2. Python SDK 726
2.1.2.2.1. Quick start 726
2.1.2.2.2. Use the Python SDK 728
2.1.2.3. PHP SDK 728
2.1.2.3.1. Quick start 728
2.1.2.4. Go SDK 730
2.1.2.4.1. Quick start 730
2.1.2.4.2. Use the Go SDK 732
2.1.2.5. .NET SDK 732
2.1.2.5.1. Quick start 732
2.1.2.5.2. Use the .NET SDK 733
2.1.3. Obtain an endpoint 734

2.1.4. Obtain an AccessKey pair 735
2.2. Container Service 735
2.2.1. Container Service API invocation 735
2.2.1.1. Overview 735
2.2.1.2. Common parameters 735
2.2.1.3. Request structure 737
2.2.1.4. Response parameters 738
2.2.1.5. Sign API requests 738
2.2.2. Cluster API list 743
2.2.2.1. Download cluster certificates 743
2.2.2.2. Create Kubernetes clusters 744
2.2.2.3. Add ECS instances to clusters 753
2.2.2.4. Get kubeconfig files 756
2.2.2.5. View clusters 757
2.2.2.6. Expand Kubernetes clusters 760
2.2.2.7. Delete clusters 763
2.3. Auto Scaling (ESS) 764
2.3.1. API reference 764
2.3.1.1. API usage instructions 764
2.3.1.2. Make API requests 765
2.3.1.3. Request structure 765
2.3.1.4. Common parameters 765
2.3.1.4.1. Common request parameters 765
2.3.1.4.2. Common response parameters 767
2.3.1.5. Responses 767
2.3.1.5.1. Successful response examples 767
2.3.1.5.2. Error response examples 768
2.3.1.6. Request signatures 769

2.3.1.7. Scaling groups 771
2.3.1.7.1. CreateScalingGroup 771
2.3.1.7.2. ModifyScalingGroup 777
2.3.1.7.3. EnableScalingGroup 781
2.3.1.7.4. DisableScalingGroup 786
2.3.1.7.5. DeleteScalingGroup 787
2.3.1.7.6. DescribeScalingGroups 789
2.3.1.7.7. DescribeScalingInstances 795
2.3.1.7.8. DescribeScalingActivities 799
2.3.1.8. Scaling configurations 803
2.3.1.8.1. CreateScalingConfiguration 803
2.3.1.8.2. DescribeScalingConfigurations 811
2.3.1.8.3. DeleteScalingConfiguration 815
2.3.1.9. Scaling rules 817
2.3.1.9.1. CreateScalingRule 817
2.3.1.9.2. ModifyScalingRule 820
2.3.1.9.3. DescribeScalingRules 823
2.3.1.9.4. DeleteScalingRule 826
2.3.1.10. Scaling tasks 827
2.3.1.10.1. ExecuteScalingRule 827
2.3.1.10.2. AttachInstances 831
2.3.1.10.3. RemoveInstances 836
2.3.1.10.4. DetachInstances 839
2.3.1.11. Scheduled tasks 841
2.3.1.11.1. CreateScheduledTask 841
2.3.1.11.2. ModifyScheduledTask 845
2.3.1.11.3. DescribeScheduledTasks 850
2.3.1.11.4. DeleteScheduledTask 853

2.3.1.12. Error codes 854
2.3.1.12.1. Client errors 854
2.3.1.12.2. Server errors 856
2.3.1.13. Ensure idempotence 856
2.3.2. SDK reference 856
2.3.2.1. Java SDK 857
2.3.2.1.1. Quick start 857
2.3.2.1.2. Use the Java SDK 859
2.3.2.2. Python SDK 860
2.3.2.2.1. Quick start 860
2.3.2.2.2. Use the Python SDK 861
2.3.2.3. PHP SDK 861
2.3.2.3.1. Quick start 861
2.3.2.4. Go SDK 863
2.3.2.4.1. Quick start 863
2.3.2.4.2. Use the Go SDK 865
2.3.2.5. .NET SDK 865
2.3.2.5.1. Quick start 865
2.3.2.5.2. Use the .NET SDK 866
2.3.3. Obtain an endpoint 866
2.3.4. Obtain an AccessKey pair 868
2.4. Object Storage Service (OSS) 868
2.4.1. API reference 868
2.4.1.1. OSS API reference overview 868
2.4.1.2. API overview 868
2.4.1.3. Access control 871
2.4.1.3.1. Verify user signature 871
2.4.1.3.2. Add signatures to headers 871

2.4.1.3.3. Generate a signed URL 878
2.4.1.3.4. Authorized temporary access 880
2.4.1.3.5. Bucket permission control 882
2.4.1.4. Definitions of common HTTP headers 882
2.4.1.5. Service-relevant operations 884
2.4.1.5.1. GetService 884
2.4.1.6. Bucket-relevant operations 889
2.4.1.6.1. PutBucket 889
2.4.1.6.2. PutBucketACL 891
2.4.1.6.3. PutBucketLogging 892
2.4.1.6.4. PutBucketWebsite 897
2.4.1.6.5. PutBucketReferer 900
2.4.1.6.6. PutBucketLifecycle 903
2.4.1.6.7. PutBucketTagging 907
2.4.1.6.8. GetBucket 909
2.4.1.6.9. GetBucketAcl 918
2.4.1.6.10. GetBucketLocation 920
2.4.1.6.11. GetBucketInfo 921
2.4.1.6.12. GetBucketLogging 925
2.4.1.6.13. GetBucketWebsite 927
2.4.1.6.14. GetBucketReferer 930
2.4.1.6.15. GetBucketLifecycle 932
2.4.1.6.16. GetBucketTagging 934
2.4.1.6.17. DeleteBucket 936
2.4.1.6.18. DeleteBucketLogging 937
2.4.1.6.19. DeleteBucketWebsite 938
2.4.1.6.20. DeleteBucketLifecycle 939
2.4.1.6.21. DeleteBucketTagging 939

2.4.1.6.22. ListBucketByTagging 940
2.4.1.7. Object-relevant operations 942
2.4.1.7.1. PutObject 942
2.4.1.7.2. GetObject 946
2.4.1.7.3. CopyObject 952
2.4.1.7.4. AppendObject 955
2.4.1.7.5. DeleteObject 960
2.4.1.7.6. DeleteMultipleObjects 961
2.4.1.7.7. HeadObject 966
2.4.1.7.8. GetObjectMeta 968
2.4.1.7.9. PutObjectACL 969
2.4.1.7.10. GetObjectACL 971
2.4.1.7.11. PostObject 973
2.4.1.7.12. PutSymlink 982
2.4.1.7.13. GetSymlink 984
2.4.1.7.14. Callback 985
2.4.1.7.15. RestoreObject 997
2.4.1.7.16. SelectObject 1000
2.4.1.7.17. PutObjectTagging 1032
2.4.1.7.18. GetObjectTagging 1034
2.4.1.7.19. DeleteObjectTagging 1036
2.4.1.8. Multipart upload-relevant operations 1037
2.4.1.8.1. Overview 1037
2.4.1.8.2. InitiateMultipartUpload 1037
2.4.1.8.3. UploadPart 1041
2.4.1.8.4. UploadPartCopy 1042
2.4.1.8.5. CompleteMultipartUpload 1045
2.4.1.8.6. AbortMultipartUpload 1049

2.4.1.8.7. ListMultipartUploads 1050
2.4.1.8.8. ListParts 1055
2.4.1.9. CORS 1060
2.4.1.9.1. Overview 1060
2.4.1.9.2. PutBucketcors 1061
2.4.1.9.3. GetBucketcors 1064
2.4.1.9.4. DeleteBucketcors 1067
2.4.1.9.5. OptionObject 1067
2.4.1.10. OSS error response 1069
2.4.1.11. S3 API compatibility instructions 1074
2.4.2. SDK reference 1076
2.4.2.1. Java SDK 1076
2.4.2.1.1. Preface 1077
2.4.2.1.2. Installation 1077
2.4.2.1.3. Initialization 1079
2.4.2.1.4. Quick start 1083
2.4.2.1.5. Manage buckets 1086
2.4.2.1.6. Upload objects 1092
2.4.2.1.7. Download objects 1120
2.4.2.1.8. Manage objects 1129
2.4.2.1.9. Authorized access 1148
2.4.2.1.10. Manage lifecycle rules 1152
2.4.2.1.11. CORS 1155
2.4.2.1.12. Set access logging 1157
2.4.2.1.13. Static website hosting 1158
2.4.2.1.14. Hotlinking 1159
2.4.2.1.15. IMG 1160
2.4.2.1.16. Exception handling 1165

2.4.2.1.17. FAQs 1168
2.4.2.2. Python-SDK 1178
2.4.2.2.1. Installation 1178
2.4.2.2.2. Quick start 1180
2.4.2.2.3. Initialization 1182
2.4.2.2.4. Manage buckets 1182
2.4.2.2.5. Upload objects 1184
2.4.2.2.6. Download objects 1190
2.4.2.2.7. Manage objects 1192
2.4.2.2.8. Authorized access 1196
2.4.2.2.9. Static website hosting 1198
2.4.2.2.10. Manage lifecycle rules 1198
2.4.2.2.11. CORS 1201
2.4.2.2.12. Set access logging 1202
2.4.2.2.13. Hotlinking 1203
2.4.2.2.14. Handle errors 1204
2.4.2.2.15. Chinese character and time 1206
2.4.2.2.16. IMG 1207
2.4.2.3. PHP-SDK 1213
2.4.2.3.1. Installation 1213
2.4.2.3.2. Initialization 1216
2.4.2.3.3. Quick start 1217
2.4.2.3.4. Manage buckets 1220
2.4.2.3.5. Upload objects 1226
2.4.2.3.6. Download objects 1241
2.4.2.3.7. Manage objects 1246
2.4.2.3.8. Authorized access 1257
2.4.2.3.9. Exception handling 1260

2.4.2.4. C-SDK 1262
2.4.2.4.1. Preface 1262
2.4.2.4.2. Installation 1263
2.4.2.4.3. Initialization 1267
2.4.2.4.4. Quick start 1269
2.4.2.4.5. Manage buckets 1275
2.4.2.4.6. Upload objects 1279
2.4.2.4.7. Download objects 1295
2.4.2.4.8. Manage objects 1298
2.4.2.4.9. Authorized access 1309
2.4.2.4.10. Error handling 1316
2.4.2.5. Go-SDK 1318
2.4.2.5.1. Installation 1318
2.4.2.5.2. Quick start 1320
2.4.2.5.3. Manage buckets 1324
2.4.2.5.4. Upload objects 1328
2.4.2.5.5. Download objects 1340
2.4.2.5.6. Manage objects 1346
2.4.2.5.7. Set ACLs 1359
2.4.2.5.8. Troubleshooting 1361
2.4.3. Obtain an endpoint 1365
2.4.4. Obtain an AccessKey pair 1366
2.5. Table Store 1367
2.5.1. API reference 1367
2.5.1.1. API-based operations 1367
2.5.1.1.1. GetRow 1367
2.5.1.1.2. PutRow 1370
2.5.1.1.3. UpdateRow 1372

2.5.1.1.4. DeleteRow 1374
2.5.1.1.5. GetRange 1376
2.5.1.1.6. BatchGetRow 1379
2.5.1.1.7. BatchWriteRow 1380
2.5.1.1.8. CreateTable 1382
2.5.1.1.9. ListTable 1383
2.5.1.1.10. DeleteTable 1384
2.5.1.1.11. UpdateTable 1384
2.5.1.1.12. DescribeTable 1385
2.5.1.1.13. ComputeSplitPointsBySize 1387
2.5.1.1.14. ListStream 1389
2.5.1.1.15. DescribeStream 1390
2.5.1.1.16. GetShardIterator 1392
2.5.1.1.17. GetStreamRecord 1392
2.5.1.1.18. Table Store ProtocolBuffer message definitions 1393
2.5.1.2. DataType 1403
2.5.1.2.1. ActionType 1404
2.5.1.2.2. CapacityUnit 1404
2.5.1.2.3. ColumnPaginationFilter 1404
2.5.1.2.4. ComparatorType 1405
2.5.1.2.5. CompositeColumnValueFilter 1405
2.5.1.2.6. Condition 1406
2.5.1.2.7. ConsumedCapacity 1406
2.5.1.2.8. Direction 1407
2.5.1.2.9. Error 1407
2.5.1.2.10. Filter 1407
2.5.1.2.11. PrimaryKeyOption 1408
2.5.1.2.12. FilterType 1408

2.5.1.2.13. LogicalOperator 1408
2.5.1.2.14. OperationType 1409
2.5.1.2.15. PartitionRange 1409
2.5.1.2.16. PlainBuffer 1409
2.5.1.2.17. PrimaryKeySchema 1413
2.5.1.2.18. PrimaryKeyType 1413
2.5.1.2.19. ReservedThroughput 1414
2.5.1.2.20. ReservedThroughputDetails 1414
2.5.1.2.21. ReturnContent 1415
2.5.1.2.22. ReturnType 1415
2.5.1.2.23. RowExistenceExpectation 1415
2.5.1.2.24. RowInBatchGetRowResponse 1416
2.5.1.2.25. RowInBatchWriteRowRequest 1416
2.5.1.2.26. RowInBatchWriteRowResponse 1417
2.5.1.2.27. SingleColumnValueFilter 1418
2.5.1.2.28. StreamDetails 1419
2.5.1.2.29. StreamRecord 1419
2.5.1.2.30. StreamSpecification 1420
2.5.1.2.31. TableInBatchGetRowRequest 1420
2.5.1.2.32. TableInBatchGetRowResponse 1422
2.5.1.2.33. TableInBatchWriteRowRequest 1422
2.5.1.2.34. TableInBatchWriteRowResponse 1423
2.5.1.2.35. TableMeta 1423
2.5.1.2.36. TableOptions 1424
2.5.1.2.37. TimeRange 1424
2.5.2. SDK reference 1425
2.5.2.1. Java SDK 1425
2.5.2.1.1. Quick start 1425

2.5.2.1.2. Use the SDK 1426
2.5.2.2. Python SDK 1426
2.5.2.2.1. Quick start 1426
2.5.2.2.2. Use the SDK 1426
2.5.2.3. C++ SDK 1426
2.5.2.3.1. Quick start 1426
2.5.2.3.2. Use the SDK 1427
2.5.2.4. Go SDK 1427
2.5.2.4.1. Quick start 1427
2.5.2.4.2. Use the SDK 1427
2.5.2.5. NodeJS SDK 1427
2.5.2.5.1. Quick start 1428
2.5.2.5.2. Use the SDK 1428
2.5.2.6. .NET SDK 1428
2.5.2.6.1. Quick start 1428
2.5.2.6.2. Use the SDK 1429
2.5.2.7. Obtain an AccessKey pair 1429
2.6. Network Attached Storage (NAS) 1430
2.6.1. List of operations by function 1430
2.6.2. Make API requests 1431
2.6.2.1. Common parameters 1431
2.6.2.2. Structure of a request 1433
2.6.3. Region 1433
2.6.3.1. DescribeRegions 1433
2.6.4. NAS instance 1435
2.6.4.1. CreateFileSystem 1436
2.6.4.2. DeleteFileSystem 1437
2.6.4.3. DescribeFileSystems 1438

2.6.4.4. ModifyFileSystem 1441
2.6.5. Mount point 1442
2.6.5.1. CreateMountTarget 1442
2.6.5.2. DeleteMountTarget 1444
2.6.5.3. DescribeMountTargets 1444
2.6.5.4. ModifyMountTarget 1447
2.6.6. Permission group 1448
2.6.6.1. CreateAccessGroup 1448
2.6.6.2. CreateAccessRule 1449
2.6.6.3. DeleteAccessGroup 1450
2.6.6.4. DeleteAccessRule 1451
2.6.6.5. DescribeAccessGroups 1452
2.6.6.6. DescribeAccessRules 1455
2.6.6.7. ModifyAccessGroup 1457
2.6.6.8. ModifyAccessRule 1458
2.6.7. Appendix: Error codes 1460
2.6.8. Obtain an endpoint 1464
2.6.9. Obtain an AccessKey pair 1465
2.7. Apsara File Storage for HDFS 1466
2.7.1. API reference 1466
2.7.1.1. List of operations by function 1466
2.7.1.2. Make API requests 1468
2.7.1.2.1. Common parameters 1468
2.7.1.2.2. Request structure 1470
2.7.1.3. Regions 1470
2.7.1.3.1. ListRegions 1470
2.7.1.3.2. GetRegion 1472
2.7.1.4. File systems 1473

2.7.1.4.1. CreateFileSystem 1473
2.7.1.4.2. DeleteFileSystem 1475
2.7.1.4.3. ModifyFileSystem 1476
2.7.1.4.4. GetFileSystem 1477
2.7.1.4.5. ListFileSystems 1479
2.7.1.5. Permissions 1481
2.7.1.5.1. CreateAccessGroup 1481
2.7.1.5.2. DeleteAccessGroup 1482
2.7.1.5.3. ModifyAccessGroup 1483
2.7.1.5.4. GetAccessGroup 1484
2.7.1.5.5. ListAccessGroups 1486
2.7.1.5.6. CreateAccessRule 1488
2.7.1.5.7. DeleteAccessRule 1490
2.7.1.5.8. ModifyAccessRule 1490
2.7.1.5.9. GetAccessRule 1492
2.7.1.5.10. ListAccessRules 1493
2.7.1.6. Mount points 1496
2.7.1.6.1. CreateMountPoint 1496
2.7.1.6.2. DeleteMountPoint 1497
2.7.1.6.3. ModifyMountPoint 1498
2.7.1.6.4. GetMountPoint 1499
2.7.1.6.5. ListMountPoints 1501
2.7.1.7. Appendix: Error codes 1504
2.7.2. SDK reference 1509
2.7.2.1. Overview 1509
2.7.2.2. File system SDK 1509
2.7.2.3. Management Java SDK 1512
2.7.2.3.1. Java SDK 1512

2.7.3. Obtain an AccessKey pair 1512
2.7.4. Obtain an endpoint 1512
2.8. ApsaraDB for RDS 1513
2.8.1. API reference 1513
2.8.1.1. List of operations by function 1514
2.8.1.2. Make API requests 1517
2.8.1.2.1. Request structure 1517
2.8.1.2.2. Common parameters 1518
2.8.1.2.2.1. Common request parameters 1518
2.8.1.2.2.2. Common response parameters 1519
2.8.1.2.3. Responses 1519
2.8.1.2.3.1. Success responses 1519
2.8.1.2.3.2. Error responses 1520
2.8.1.2.4. Request signatures 1520
2.8.1.3. Instance management 1523
2.8.1.3.1. CreateDBInstance 1523
2.8.1.3.2. DeleteDBInstance 1525
2.8.1.3.3. RestartDBInstance 1526
2.8.1.3.4. DescribeDBInstanceAttribute 1527
2.8.1.3.5. DescribeDBInstances 1533
2.8.1.3.6. ModifyDBInstanceSpec 1540
2.8.1.3.7. AllocateInstancePublicConnection 1543
2.8.1.3.8. ReleaseInstancePublicConnection 1544
2.8.1.3.9. SwitchDBInstanceNetType 1545
2.8.1.3.10. DescribeDBInstanceNetInfo 1546
2.8.1.3.11. ModifyDBInstanceConnectionString 1546
2.8.1.3.12. ModifyDBInstanceConnectionMode 1547
2.8.1.3.13. ModifyDBInstanceNetworkType 1548

2.8.1.3.14. DescribeDBInstanceIPArrayList 1549
2.8.1.3.15. ModifySecurityIps 1549
2.8.1.3.16. DescribeRegions 1551
2.8.1.3.17. DescribeDBInstanceHAConfig 1552
2.8.1.3.18. MigrateToOtherZone 1553
2.8.1.3.19. PurgeDBInstanceLog 1554
2.8.1.3.20. UpgradeDBInstanceEngineVersion 1555
2.8.1.3.21. ModifyDBInstanceDescription 1556
2.8.1.3.22. ModifyDBInstanceMaintainTime 1557
2.8.1.3.23. ModifyDBInstanceHAConfig 1559
2.8.1.3.24. SwitchDBInstanceHA 1559
2.8.1.3.25. CreateReadOnlyDBInstance 1560
2.8.1.3.26. DescribeDBInstanceSSL 1562
2.8.1.3.27. ModifyDBInstanceSSL 1563
2.8.1.3.28. DescribeDBInstanceTDE 1564
2.8.1.3.29. ModifyDBInstanceTDE 1564
2.8.1.4. Database management 1565
2.8.1.4.1. CreateDatabase 1565
2.8.1.4.2. DeleteDatabase 1566
2.8.1.4.3. DescribeDatabases 1568
2.8.1.4.4. ModifyDBDescription 1570
2.8.1.5. Account management 1571
2.8.1.5.1. CreateAccount 1571
2.8.1.5.2. DeleteAccount 1573
2.8.1.5.3. DescribeAccounts 1574
2.8.1.5.4. GrantAccountPrivilege 1576
2.8.1.5.5. RevokeAccountPrivilege 1577
2.8.1.5.6. ModifyAccountDescription 1578

2.8.1.5.7. ResetAccountPassword 1580
2.8.1.5.8. ResetAccount 1581
2.8.1.6. Backup and restoration 1581
2.8.1.6.1. CreateBackup 1581
2.8.1.6.2. CloneDBInstance 1583
2.8.1.6.3. DescribeBackups 1584
2.8.1.6.4. CreateTempDBInstance 1586
2.8.1.6.5. DescribeBackupPolicy 1587
2.8.1.6.6. ModifyBackupPolicy 1588
2.8.1.6.7. RestoreDBInstance 1589
2.8.1.6.8. DeleteBackup 1590
2.8.1.7. Monitoring management 1591
2.8.1.7.1. DescribeResourceUsage 1591
2.8.1.7.2. DescribeDBInstancePerformance 1592
2.8.1.7.3. DescribeDBInstanceMonitor 1594
2.8.1.7.4. ModifyDBInstanceMonitor 1595
2.8.1.8. Parameter management 1595
2.8.1.8.1. DescribeParameterTemplates 1595
2.8.1.8.2. DescribeParameters 1597
2.8.1.8.3. ModifyParameter 1599
2.8.1.9. Log management 1601
2.8.1.9.1. DescribeSlowLogs 1601
2.8.1.9.2. DescribeSlowLogRecords 1604
2.8.1.9.3. DescribeErrorLogs 1607
2.8.1.9.4. DescribeBinlogFiles 1609
2.8.1.9.5. DescribeSQLCollectorPolicy 1612
2.8.1.9.6. ModifySQLCollectorPolicy 1613
2.8.1.9.7. DescribeSQLLogRecords 1613

2.8.1.9.8. DescribeSQLLogFiles 1616
2.8.1.10. Data migration 1617
2.8.1.10.1. ImportDatabaseBetweenInstances 1618
2.8.1.10.2. CancelImport 1619
2.8.1.11. Tag management 1620
2.8.1.11.1. AddTagsToResource 1620
2.8.1.11.2. DescribeTags 1621
2.8.1.11.3. RemoveTagsFromResource 1622
2.8.1.12. RAM authorization 1623
2.8.1.13. Appendix 1627
2.8.1.13.1. Error codes on the client 1627
2.8.1.13.1.1. Common errors 1627
2.8.1.13.1.2. Specific errors 1628
2.8.1.13.2. Error codes on the server 1633
2.8.1.13.3. Instance states 1634
2.8.1.13.4. Performance parameters 1634
2.8.1.13.5. Forbidden keywords 1636
2.8.1.13.6. Instance types 1636
2.8.2. SDK reference 1640
2.8.2.1. Java SDK 1641
2.8.2.1.1. Quick start 1641
2.8.2.1.2. Use the SDK 1642
2.8.2.1.2.1. Install the Java SDK 1642
2.8.2.1.2.2. Configure identity verification credentials 1643
2.8.2.1.2.3. Initiate a request 1643
2.8.2.1.2.4. Troubleshooting 1644
2.8.2.1.2.5. Call an API through CommonRequest 1645
2.8.2.1.2.6. Common errors 1648

2.8.2.2. Python SDK 1650
2.8.2.2.1. Quick start 1650
2.8.2.2.2. Use the SDK 1651
2.8.2.2.2.1. Install the Python SDK 1651
2.8.2.2.2.2. Configure identity verification credentials 1652
2.8.2.2.2.3. Initiate a request 1653
2.8.2.2.2.4. Set HTTPS requests 1653
2.8.2.2.2.5. Troubleshooting 1654
2.8.2.2.2.6. Call an API through CommonRequest 1655
2.8.2.2.2.7. Common errors 1656
2.8.2.3. PHP SDK 1657
2.8.2.3.1. Quick start 1657
2.8.2.4. C# SDK 1659
2.8.3. Obtain an endpoint 1659
2.8.4. Obtain an AccessKey pair 1660
2.9. KVStore for Redis 1661
2.9.1. API reference 1661
2.9.1.1. API overview 1661
2.9.1.2. Request structure 1662
2.9.1.3. Common parameters 1663
2.9.1.4. Responses 1664
2.9.1.5. Request signatures 1666
2.9.1.6. RAM-based authorization 1668
2.9.1.6.1. Grant resource permissions to a RAM user 1668
2.9.1.6.2. Authorized resource type for a RAM user 1668
2.9.1.6.3. Operation permissions granted to a RAM user 1668
2.9.1.6.4. API authentication rules 1669
2.9.1.7. Manage the lifecycle 1671

2.9.1.7.1. CreateInstance 1671
2.9.1.7.2. DeleteInstance 1675
2.9.1.7.3. ModifyInstanceSpec 1676
2.9.1.8. Manage instances 1678
2.9.1.8.1. DescribeInstanceAttribute 1678
2.9.1.8.2. DescribeInstances 1681
2.9.1.8.3. DescribeRegions 1687
2.9.1.8.4. DescribeSecurityIps 1689
2.9.1.8.5. FlushInstance 1691
2.9.1.8.6. ModifyInstanceAttribute 1692
2.9.1.8.7. ModifyInstanceMaintainTime 1694
2.9.1.8.8. ModifyInstanceNetExpireTime 1695
2.9.1.8.9. ModifySecurityIps 1697
2.9.1.8.10. SwitchNetwork 1698
2.9.1.9. Backup and recovery 1700
2.9.1.9.1. CreateBackup 1700
2.9.1.9.2. ModifyBackupPolicy 1701
2.9.1.9.3. DescribeBackupPolicy 1702
2.9.1.9.4. DescribeBackups 1704
2.9.1.9.5. RestoreInstance 1707
2.9.1.10. Manage monitoring 1708
2.9.1.10.1. DescribeMonitorItems 1709
2.9.1.10.2. DescribeHistoryMonitorValues 1710
2.9.1.11. Manage parameters 1712
2.9.1.11.1. DescribeInstanceConfig 1712
2.9.1.11.2. ModifyInstanceConfig 1714
2.9.1.12. Appendixes 1715
2.9.1.12.1. Instance types 1715

2.9.1.12.2. Error codes 1719
2.9.1.12.3. Instance configurations 1724
2.9.2. SDK reference 1728
2.9.2.1. Java SDK 1728
2.9.2.1.1. Quick start 1728
2.9.2.1.2. Use the Java SDK 1730
2.9.2.1.2.1. Install the Java SDK 1731
2.9.2.1.2.2. Configure authentication credentials 1731
2.9.2.1.2.3. Make API requests 1732
2.9.2.1.2.4. Process errors 1732
2.9.2.1.2.5. Use CommonRequest to make a request 1733
2.9.2.1.2.6. Common errors 1736
2.9.2.2. Python SDK 1738
2.9.2.2.1. Quick start 1738
2.9.2.2.2. Use the Python SDK 1739
2.9.2.2.2.1. Install the Python SDK 1739
2.9.2.2.2.2. Configure authentication credentials 1740
2.9.2.2.2.3. Make API requests 1741
2.9.2.2.2.4. Set HTTPS requests 1741
2.9.2.2.2.5. Process errors 1742
2.9.2.2.2.6. Use CommonRequest to make a request 1743
2.9.2.2.2.7. Common errors 1744
2.9.2.3. PHP SDK 1746
2.9.2.3.1. Quick start 1746
2.9.2.4. Go SDK 1747
2.9.2.4.1. Quick start 1747
2.9.2.4.2. Use the Go SDK 1749
2.9.2.4.2.1. Install the Go SDK 1749

2.9.2.4.2.2. Configure authentication credentials 1750
2.9.2.4.2.3. Make API requests 1750
2.9.2.4.2.4. Process errors 1752
2.9.2.4.2.5. Custom configurations 1753
2.9.2.4.2.6. Make asynchronous requests 1754
2.9.2.4.2.7. Use CommonRequest to make a request 1755
2.9.2.4.2.8. Common errors 1756
2.9.2.5. .NET SDK 1758
2.9.2.5.1. Quick start 1758
2.9.2.5.2. Use the .NET SDK 1761
2.9.2.5.2.1. Install the .NET SDK 1761
2.9.2.5.2.2. Configure authentication credentials 1761
2.9.2.5.2.3. Make API requests 1762
2.9.2.5.2.4. Process errors 1762
2.9.2.5.2.5. Use CommonRequest to make a request 1763
2.9.2.5.2.6. Common errors 1767
2.9.2.6. Obtain an AccessKey pair 1768
2.9.2.7. Obtain an endpoint 1768
2.10. ApsaraDB for MongoDB 1769
2.10.1. List of operations by function 1769
2.10.1.1. Lifecycle management 1769
2.10.1.2. Instance management 1770
2.10.1.3. Account management 1770
2.10.1.4. Database security management 1770
2.10.1.5. Backup and restoration management 1771
2.10.1.6. Monitoring alert management 1771
2.10.2. Make API requests 1771
2.10.2.1. Request structure 1771

2.10.2.2. Common parameters 1771
2.10.2.2.1. Common request parameters 1772
2.10.2.2.2. Common response parameters 1773
2.10.2.2.2.1. Responses 1773
2.10.2.3. Sign signatures 1773
2.10.3. Lifecycle management 1775
2.10.3.1. CreateDBInstance 1775
2.10.3.1.1. Description 1775
2.10.3.1.2. Request parameters 1775
2.10.3.1.3. Response parameters 1777
2.10.3.2. ModifyDBInstanceSpec 1777
2.10.3.2.1. Description 1777
2.10.3.2.2. Request parameters 1777
2.10.3.2.3. Response parameters 1778
2.10.3.3. DeleteDBInstance 1778
2.10.3.3.1. Description 1778
2.10.3.3.2. Request parameters 1778
2.10.3.3.3. Response parameters 1779
2.10.3.4. RenewDBInstance 1779
2.10.3.4.1. Description 1779
2.10.3.4.2. Request parameters 1779
2.10.3.4.3. Response parameters 1779
2.10.4. Instance management 1780
2.10.4.1. DescribeRegions 1780
2.10.4.1.1. Description 1780
2.10.4.1.2. Request parameters 1780
2.10.4.1.3. Response parameters 1780
2.10.4.1.3.1. Region data structure 1780

2.10.4.1.3.2. Zones 1781
2.10.4.2. DescribeDBInstances 1781
2.10.4.2.1. Description 1781
2.10.4.2.2. Request parameters 1781
2.10.4.2.3. Response parameters 1782
2.10.4.2.3.1. DBInstance data structure 1782
2.10.4.2.3.2. Mongos 1783
2.10.4.2.3.3. Shard 1783
2.10.4.3. RestartDBInstance 1783
2.10.4.3.1. Description 1784
2.10.4.3.2. Request parameters 1784
2.10.4.3.3. Response parameters 1784
2.10.4.4. ModifyDBInstanceMaintainTime 1784
2.10.4.4.1. Description 1784
2.10.4.4.2. Request parameters 1784
2.10.4.4.3. Response parameters 1785
2.10.4.5. ModifyDBInstanceDescription 1785
2.10.4.5.1. Description 1785
2.10.4.5.2. Request parameters 1785
2.10.4.5.3. Response parameters 1785
2.10.4.6. DescribeInstanceAttribute 1786
2.10.4.6.1. Description 1786
2.10.4.6.2. Request parameters 1786
2.10.4.6.3. Response parameters 1786
2.10.4.6.3.1. DBInstance parameters 1786
2.10.4.7. DescribeReplicaSetRole 1787
2.10.4.7.1. Description 1787
2.10.4.7.2. Request parameters 1787

2.10.4.7.3. Response parameters 1788
2.10.4.7.3.1. ReplicaSetRole data structure 1788
2.10.4.8. ModifyDBInstanceNetworkType 1788
2.10.4.8.1. Description 1788
2.10.4.8.2. Request parameters 1789
2.10.4.8.3. Response parameters 1789
2.10.4.9. ModifyDBInstanceNetExpireTime 1790
2.10.4.9.1. Description 1790
2.10.4.9.2. Request parameters 1790
2.10.4.9.3. Response parameters 1790
2.10.5. Account management 1790
2.10.5.1. ResetAccountPassword 1790
2.10.5.1.1. Description 1791
2.10.5.1.2. Request parameters 1791
2.10.5.1.3. Response parameters 1791
2.10.5.2. DescribeAccounts 1791
2.10.5.2.1. Description 1791
2.10.5.2.2. Request parameters 1791
2.10.5.2.3. Response parameters 1792
2.10.5.2.3.1. Account data structure 1792
2.10.5.3. ModifyAccountDescription 1792
2.10.5.3.1. Description 1792
2.10.5.3.2. Request parameters 1792
2.10.5.3.3. Response parameters 1793
2.10.6. Database security management 1793
2.10.6.1. DescribeSecurityIps 1793
2.10.6.1.1. Description 1793
2.10.6.1.2. Request parameters 1793

2.10.6.1.3. Response parameters 1793
2.10.6.2. ModifySecurityIps 1794
2.10.6.2.1. Description 1794
2.10.6.2.2. Request parameters 1794
2.10.6.2.3. Response parameters 1795
2.10.6.3. DescribeAuditRecords 1795
2.10.6.3.1. Description 1795
2.10.6.3.2. Request parameters 1796
2.10.6.3.3. Response parameters 1797
2.10.6.4. DescribeAuditFiles 1798
2.10.6.4.1. Description 1798
2.10.6.4.2. Request parameters 1798
2.10.6.4.3. Response parameters 1799
2.10.7. Backup and restoration management 1800
2.10.7.1. DescribeBackupPolicy 1800
2.10.7.1.1. Description 1800
2.10.7.1.2. Request parameters 1800
2.10.7.1.3. Response parameters 1800
2.10.7.2. ModifyBackupPolicy 1801
2.10.7.2.1. Description 1801
2.10.7.2.2. Request parameters 1801
2.10.7.2.3. Response parameters 1802
2.10.7.3. CreateBackup 1802
2.10.7.3.1. Description 1802
2.10.7.3.2. Request parameters 1802
2.10.7.3.3. Response parameters 1802
2.10.7.4. DescribeBackups 1803
2.10.7.4.1. Description 1803

2.10.7.4.2. Request parameters 1803
2.10.7.4.3. Response parameters 1804
2.10.7.5. RestoreDBInstance 1805
2.10.7.5.1. Description 1805
2.10.7.5.2. Request parameters 1805
2.10.7.5.3. Response parameters 1806
2.10.8. Performance monitoring management 1806
2.10.8.1. DescribeDBInstancePerformance 1806
2.10.8.1.1. Description 1806
2.10.8.1.2. Request parameters 1806
2.10.8.1.3. Response parameters 1807
2.10.9. Appendix 1808
2.10.9.1. Error codes 1808
2.11. AnalyticDB for PostgreSQL 1814
2.11.1. API reference 1814
2.11.1.1. List of operations by function 1814
2.11.1.2. Request structure 1816
2.11.1.3. Common parameters 1816
2.11.1.4. Responses 1818
2.11.1.5. Request signatures 1819
2.11.1.6. RAM authorization 1821
2.11.1.6.1. Use RAM to authorize resources 1821
2.11.1.6.2. Resources that can be authorized in RAM 1821
2.11.1.6.3. Operations that can be authorized in RAM 1822
2.11.1.6.4. Authentication rules of API operations 1822
2.11.1.7. Instance management 1824
2.11.1.7.1. CreateDBInstance 1824
2.11.1.7.2. DeleteDBInstance 1827

2.11.1.7.3. DescribeDBInstanceAttribute 1828
2.11.1.7.4. DescribeDBInstances 1833
2.11.1.7.5. DescribeRegions 1844
2.11.1.7.6. DescribeResourceUsage 1853
2.11.1.7.7. ModifyDBInstanceConnectionMode 1855
2.11.1.7.8. ModifyDBInstanceDescription 1856
2.11.1.7.9. ModifyDBInstanceMaintainTime 1857
2.11.1.7.10. RestartDBInstance 1858
2.11.1.7.11. DescribeDBInstancePerformance 1859
2.11.1.8. Database management 1867
2.11.1.8.1. DeleteDatabase 1867
2.11.1.8.2. DescribeAccounts 1868
2.11.1.8.3. ModifyAccountDescription 1870
2.11.1.9. Account management 1872
2.11.1.9.1. CreateAccount 1872
2.11.1.9.2. ResetAccountPassword 1873
2.11.1.10. Security management 1875
2.11.1.10.1. DescribeDBInstanceIPArrayList 1875
2.11.1.10.2. ModifySecurityIps 1877
2.11.1.11. Log management 1879
2.11.1.11.1. DescribeSlowLogRecords 1879
2.11.1.11.2. DescribeSQLCollectorPolicy 1883
2.11.1.11.3. DescribeSQLLogFiles 1884
2.11.1.11.4. DescribeSQLLogRecords 1887
2.11.1.11.5. ModifySQLCollectorPolicy 1890
2.11.1.12. Network management 1891
2.11.1.12.1. AllocateInstancePublicConnection 1891
2.11.1.12.2. DescribeDBInstanceNetInfo 1893

2.11.1.12.3. ModifyDBInstanceConnectionString 1895
2.11.1.12.4. ModifyDBInstanceNetworkType 1896
2.11.1.12.5. ReleaseInstancePublicConnection 1898
2.11.1.13. Appendix 1899
2.11.1.13.1. Error codes 1899
2.11.1.13.1.1. Client error codes 1899
2.11.1.13.1.2. Server error codes 1907
2.11.1.13.2. Instance types 1907
2.11.1.13.3. Performance parameters 1907
2.11.1.13.4. Instance states 1908
2.11.1.13.5. Terms 1909
2.11.2. SDK reference 1910
2.11.2.1. Java SDK 1910
2.11.2.1.1. Quick start 1910
2.11.2.1.2. Use the Java SDK 1912
2.11.2.1.2.1. Install the Java SDK 1912
2.11.2.1.2.2. Configure authentication credentials 1913
2.11.2.1.2.3. Initiate a request 1913
2.11.2.1.2.4. Troubleshooting 1914
2.11.2.1.2.5. Common errors 1915
2.11.2.2. Python SDK 1916
2.11.2.2.1. Quick start 1916
2.11.2.2.2. Use the Python SDK 1918
2.11.2.2.2.1. Install the Python SDK 1918
2.11.2.2.2.2. Configure authentication credentials 1919
2.11.2.2.2.3. Initiate a request 1919
2.11.2.2.2.4. Set HTTPS requests 1920
2.11.2.2.2.5. Troubleshooting 1920

2.11.2.2.2.6. Common errors 1921
2.11.2.3. Obtain an AccessKey pair 1922
2.11.2.4. Obtain an endpoint 1922
2.12. Data Transmission Service (DTS) 1923
2.12.1. API reference 1924
2.12.1.1. Call OpenAPI 1924
2.12.1.1.1. API overview 1924
2.12.1.2. Data migration APIs 1925
2.12.1.2.1. ConfigureMigrationJob 1925
2.12.1.2.1.1. Overview 1925
2.12.1.2.1.2. Request parameters 1925
2.12.1.2.1.3. MigrationObject parameter definitions 1929
2.12.1.2.1.4. Response parameters 1931
2.12.1.2.1.5. Example 1931
2.12.1.2.2. CreateMigrationJob 1932
2.12.1.2.2.1. Overview 1932
2.12.1.2.2.2. Request parameters 1932
2.12.1.2.2.3. Response parameters 1933
2.12.1.2.2.4. Examples 1933
2.12.1.2.3. DeletetMigrationJob 1933
2.12.1.2.3.1. Overview 1933
2.12.1.2.3.2. Request parameters 1934
2.12.1.2.3.3. Response parameters 1934
2.12.1.2.3.4. Examples 1934
2.12.1.2.4. DescribeMigrationJobDetail 1934
2.12.1.2.4.1. Overview 1934
2.12.1.2.4.2. Request parameters 1935
2.12.1.2.4.3. Response parameters 1936

2.12.1.2.4.4. StructureInitializationDetail parameter defi... 1936
2.12.1.2.4.5. DataInitializationDetail parameter definitio... 1937
2.12.1.2.4.6. DataSynchronizationDetail parameter defi... 1938
2.12.1.2.4.7. Examples 1938
2.12.1.2.5. DescribeMigrationJobStatus 1940
2.12.1.2.5.1. Overview 1940
2.12.1.2.5.2. Request parameters 1940
2.12.1.2.5.3. Response parameters 1940
2.12.1.2.5.4. Endpoint parameter definitions 1942
2.12.1.2.5.5. MigrationMode parameter definitions 1942
2.12.1.2.5.6. PrecheckStatus parameter definitions 1942
2.12.1.2.5.7. CheckItem parameter definitions 1943
2.12.1.2.5.8. StructureInitializationStatus parameter def... 1943
2.12.1.2.5.9. DataInitializationStatus parameter definitio... 1944
2.12.1.2.5.10. DataSynchronizationStatus parameter def... 1944
2.12.1.2.5.11. Examples 1944
2.12.1.2.6. StartMigrationJob 1947
2.12.1.2.6.1. Overview 1947
2.12.1.2.6.2. Request parameters 1948
2.12.1.2.6.3. Response parameters 1948
2.12.1.2.6.4. Examples 1948
2.12.1.2.7. StopMigrationJob 1948
2.12.1.2.7.1. Overview 1948
2.12.1.2.7.2. Request parameters 1949
2.12.1.2.7.3. Response parameters 1949
2.12.1.2.7.4. Examples 1949
2.12.1.2.8. SuspendMigrationJob 1949
2.12.1.2.8.1. Overview 1949

2.12.1.2.8.2. Request parameters 1949
2.12.1.2.8.3. Response parameters 1950
2.12.1.2.8.4. Examples 1950
2.12.1.3. Data subscription APIs 1950
2.12.1.3.1. ConfigureSubscriptionInstance 1950
2.12.1.3.1.1. Overview 1950
2.12.1.3.1.2. Request parameters 1951
2.12.1.3.1.3. SubscriptionObject parameter definitions 1951
2.12.1.3.1.4. Response parameters 1952
2.12.1.3.1.5. Example 1952
2.12.1.3.2. CreateSubscriptionInstance 1953
2.12.1.3.2.1. Overview 1953
2.12.1.3.2.2. Request parameters 1953
2.12.1.3.2.3. Response parameters 1954
2.12.1.3.2.4. Examples 1954
2.12.1.3.3. DeleteSubscriptionInstance 1955
2.12.1.3.3.1. Overview 1955
2.12.1.3.3.2. Request parameters 1955
2.12.1.3.3.3. Response parameters 1955
2.12.1.3.3.4. Examples 1956
2.12.1.3.4. DescribeSubscriptionInstances 1956
2.12.1.3.4.1. Overview 1956
2.12.1.3.4.2. Request parameters 1956
2.12.1.3.4.3. Response parameters 1957
2.12.1.3.4.4. Examples 1957
2.12.1.3.5. DescribeSubscriptionInstanceStatus 1957
2.12.1.3.5.1. Overview 1958
2.12.1.3.5.2. Request parameters 1958

2.12.1.3.5.3. Response parameters 1958
2.12.1.3.5.4. Endpoint parameter definitions 1959
2.12.1.3.5.5. SubscriptionObject parameter definitions 1960
2.12.1.3.5.6. Examples 1960
2.12.1.3.6. ModifyComsumptionTimestamp 1960
2.12.1.3.6.1. Overview 1960
2.12.1.3.6.2. Request parameters 1960
2.12.1.3.6.3. Response parameters 1961
2.12.1.3.6.4. Examples 1961
2.12.1.3.7. ModifySubscriptionObject 1962
2.12.1.3.7.1. Overview 1962
2.12.1.3.7.2. Request parameters 1962
2.12.1.3.7.3. SubscriptionObject parameter definitions 1962
2.12.1.3.7.4. Response parameters 1963
2.12.1.3.7.5. Examples 1963
2.12.1.3.8. StartSubscriptionInstance 1964
2.12.1.3.8.1. Overview 1964
2.12.1.3.8.2. Request parameters 1964
2.12.1.3.8.3. Response parameters 1964
2.12.1.3.8.4. Examples 1964
2.12.1.4. Data synchronization APIs 1965
2.12.1.4.1. ConfigureSynchronizationJob 1965
2.12.1.4.1.1. Overview 1965
2.12.1.4.1.2. Request parameters 1965
2.12.1.4.1.3. Response parameters 1967
2.12.1.4.1.4. Example 1967
2.12.1.4.2. CreateSynchronizationJob 1968
2.12.1.4.2.1. Overview 1968

2.12.1.4.2.2. Request parameters 1968
2.12.1.4.2.3. Response parameters 1970
2.12.1.4.2.4. Examples 1971
2.12.1.4.3. DeleteSynchronizationJob 1971
2.12.1.4.3.1. Overview 1971
2.12.1.4.3.2. Request parameters 1971
2.12.1.4.3.3. Response parameters 1972
2.12.1.4.3.4. Examples 1972
2.12.1.4.4. DescribeDataLoadStatus 1972
2.12.1.4.4.1. Overview 1972
2.12.1.4.4.2. Request parameters 1972
2.12.1.4.4.3. Response parameters 1973
2.12.1.4.4.4. Examples 1974
2.12.1.4.5. DescribeSynchronizationJobStatus 1975
2.12.1.4.5.1. Overview 1975
2.12.1.4.5.2. Request parameters 1975
2.12.1.4.5.3. Response parameters 1975
2.12.1.4.5.4. PrecheckStatus parameter definitions 1977
2.12.1.4.5.5. CheckItem parameter definitions 1977
2.12.1.4.5.6. StructureInitializationStatus parameter def... 1977
2.12.1.4.5.7. DataInitializationStatus parameter definitio... 1978
2.12.1.4.5.8. DataSynchronizationStatus parameter defi... 1978
2.12.1.4.5.9. Performance parameter definitions 1978
2.12.1.4.5.10. Examples 1979
2.12.1.4.6. DescribeSynchronizationJobs 1981
2.12.1.4.6.1. Overview 1981
2.12.1.4.6.2. Request parameters 1981
2.12.1.4.6.3. Response parameters 1982

2.12.1.4.6.4. SynchronizationInstance parameter definit... 1982
2.12.1.4.6.5. PrecheckStatus parameter definitions 1984
2.12.1.4.6.6. CheckItem parameter definitions 1984
2.12.1.4.6.7. StructureInitializationStatus parameter defi... 1984
2.12.1.4.6.8. DataInitializationStatus parameter definiti... 1985
2.12.1.4.6.9. DataSynchronizationStatus parameter defi... 1985
2.12.1.4.6.10. Performance parameter definitions 1986
2.12.1.4.6.11. Examples 1986
2.12.1.4.7. DescribeObjectModifyStatus 1988
2.12.1.4.7.1. Overview 1988
2.12.1.4.7.2. Request parameters 1988
2.12.1.4.7.3. Response parameters 1989
2.12.1.4.7.4. PrecheckStatus parameter definitions 1989
2.12.1.4.7.5. CheckItem parameter definitions 1990
2.12.1.4.7.6. StructureInitializationStatus parameter defi... 1990
2.12.1.4.7.7. DataInitializationStatus parameter definitio... 1991
2.12.1.4.7.8. DataSynchronizationStatus parameter defi... 1991
2.12.1.4.7.9. Examples 1991
2.12.1.4.8. ModifySynchronizationObject 1993
2.12.1.4.8.1. Overview 1993
2.12.1.4.8.2. Request parameters 1993
2.12.1.4.8.3. Response parameters 1993
2.12.1.4.8.4. Examples 1994
2.12.1.4.9. StartSynchronizationJob 1994
2.12.1.4.9.1. Overview 1994
2.12.1.4.9.2. Request parameters 1994
2.12.1.4.9.3. Response parameters 1995
2.12.1.4.9.4. Examples 1995

2.12.1.4.10. SuspendSynchronizationJob 1995
2.12.1.4.10.1. Overview 1995
2.12.1.4.10.2. Request parameters 1996
2.12.1.4.10.3. Response parameters 1996
2.12.1.4.10.4. Examples 1996
2.12.2. Call the Java SDK 1996
2.12.2.1. Quick start 1996
2.12.2.2. User manual 1998
2.12.2.2.1. Install the Java SDK 1998
2.12.2.2.2. Configure identity verification credentials 1998
2.12.2.2.3. Initiate a call 1999
2.12.2.2.4. Troubleshooting 2000
2.12.2.2.5. Errors and troubleshooting 2000
2.13. Server Load Balancer (SLB) 2002
2.13.1. API reference 2002
2.13.1.1. List of operations by function 2002
2.13.1.2. Make API requests 2005
2.13.1.3. RAM authentication 2007
2.13.1.4. Common parameters 2010
2.13.1.5. Obtain an AccessKey pair 2012
2.13.1.6. Obtain an endpoint 2012
2.13.1.7. SLB instance 2014
2.13.1.7.1. CreateLoadBalancer 2014
2.13.1.7.2. DeleteLoadBalancer 2016
2.13.1.7.3. SetLoadBalancerStatus 2017
2.13.1.7.4. SetLoadBalancerName 2019
2.13.1.7.5. DescribeLoadBalancers 2020
2.13.1.7.6. DescribeLoadBalancerAttribute 2025

2.13.1.7.7. DescribeRegions 2029
2.13.1.7.8. DescribeZones 2031
2.13.1.8. Listener 2033
2.13.1.8.1. TCP listener 2033
2.13.1.8.2. UDP listener 2033
2.13.1.8.3. HTTP listener 2033
2.13.1.8.4. HTTPS listener 2033
2.13.1.8.5. Access control 2033
2.13.1.8.6. Forwarding rules 2033
2.13.1.8.7. DeleteLoadBalancerListener 2033
2.13.1.8.8. StartLoadBalancerListener 2034
2.13.1.8.9. StopLoadBalancerListener 2036
2.13.1.9. Server certificate 2037
2.13.1.9.1. UploadServerCertificate 2037
2.13.1.9.2. DeleteServerCertificate 2039
2.13.1.9.3. DescribeServerCertificates 2040
2.13.1.9.4. SetServerCertificateName 2043
2.13.1.9.5. UploadCACertificate 2045
2.13.1.9.6. DeleteCACertificate 2046
2.13.1.9.7. DescribeCACertificates 2047
2.13.1.9.8. SetCACertificateName 2049
2.13.1.10. Backend server 2050
2.13.1.10.1. AddBackendServers 2050
2.13.1.10.2. RemoveBackendServers 2052
2.13.1.10.3. SetBackendServers 2054
2.13.1.10.4. DescribeHealthStatus 2056
2.13.1.10.5. AddNcServers 2058
2.13.1.10.6. RemoveNcServers 2060

2.13.1.10.7. SetNcServers 2061
2.13.1.11. VServer group 2063
2.13.1.11.1. CreateVServerGroup 2063
2.13.1.11.2. SetVServerGroupAttribute 2065
2.13.1.11.3. AddVServerGroupBackendServers 2068
2.13.1.11.4. RemoveVServerGroupBackendServers 2070
2.13.1.11.5. ModifyVServerGroupBackendServers 2072
2.13.1.11.6. DeleteVServerGroup 2075
2.13.1.11.7. DescribeVServerGroups 2076
2.13.1.11.8. DescribeVServerGroupAttribute 2078
2.13.1.12. Primary/secondary VServer group 2081
2.13.1.12.1. CreateMasterSlaveServerGroup 2081
2.13.1.12.2. DeleteMasterSlaveServerGroup 2083
2.13.1.12.3. DescribeMasterSlaveServerGroupAttribute 2084
2.13.1.12.4. DescribeMasterSlaveServerGroups 2087
2.13.1.13. Tags 2088
2.13.1.13.1. AddTags 2088
2.13.1.13.2. DescribeTags 2090
2.13.1.13.3. RemoveTags 2093
2.13.1.14. Error codes 2095
2.13.2. SDK reference 2105
2.13.2.1. Java SDK 2105
2.13.2.1.1. Quick start 2105
2.13.2.1.2. Use the SDK 2107
2.13.2.1.2.1. Install Java SDK 2107
2.13.2.1.2.2. Configure identity verification credentials 2108
2.13.2.1.2.3. Initiate a call 2108
2.13.2.1.2.4. Handle errors 2109

2.13.2.1.2.5. Common errors 2110
2.13.2.2. Python SDK 2112
2.13.2.2.1. Quick start 2112
2.13.2.2.2. Use the SDK 2113
2.13.2.2.2.1. Install Python SDK 2113
2.13.2.2.2.2. Configure identity verification credentials 2114
2.13.2.2.2.3. Initiate a call 2114
2.13.2.2.2.4. Set HTTPS requests 2115
2.13.2.2.2.5. Handle errors 2116
2.13.2.2.2.6. Common errors 2116
2.13.2.3. PHP SDK 2117
2.13.2.3.1. Quick start 2117
2.13.2.4. Go SDK 2119
2.13.2.4.1. Quick start 2119
2.13.2.4.2. Use the SDK 2120
2.13.2.4.2.1. Install Go SDK 2121
2.13.2.4.2.2. Configure identity verification credentials 2121
2.13.2.4.2.3. Initiate a call 2122
2.13.2.4.2.4. Handle errors 2123
2.13.2.4.2.5. Customize configurations 2124
2.13.2.4.2.6. Asynchronous calls 2125
2.13.2.4.2.7. Use CommonRequest 2127
2.13.2.4.2.8. Common errors 2127
2.13.2.5. .NET SDK 2129
2.13.2.5.1. Quick start 2129
2.13.2.5.2. Use the SDK 2131
2.13.2.5.2.1. Install .NET SDK 2131
2.13.2.5.2.2. Configure identity verification credentials 2132

2.13.2.5.2.3. Initiate a call 2132
2.13.2.5.2.4. Handle errors 2133
2.13.2.5.2.5. Use CommonRequest 2134
2.13.2.5.2.6. Common errors 2137
2.13.2.6. Obtain an AccessKey pair 2137
2.13.2.7. Obtain an endpoint 2138
2.14. Virtual Private Cloud (VPC) 2139
2.14.1. API reference 2139
2.14.1.1. List of operations by function 2139
2.14.1.2. Call VPC APIs 2143
2.14.1.2.1. Request structure 2143
2.14.1.2.2. API authorization 2144
2.14.1.2.3. Request signature 2144
2.14.1.2.4. Obtain an AccessKey pair 2145
2.14.1.2.5. Obtain an endpoint 2146
2.14.1.3. RAM authentication 2147
2.14.1.4. Common parameters 2151
2.14.1.5. VPC 2153
2.14.1.5.1. CreateVpc 2153
2.14.1.5.2. DeleteVpc 2155
2.14.1.5.3. DescribeVpcs 2156
2.14.1.5.4. ModifyVpcAttribute 2160
2.14.1.5.5. DescribeVpcAttribute 2162
2.14.1.6. VRouter 2166
2.14.1.6.1. DescribeVRouters 2166
2.14.1.6.2. ModifyVRouterAttribute 2168
2.14.1.7. VSwitch 2169
2.14.1.7.1. CreateVSwitch 2170

2.14.1.7.2. DeleteVSwitch 2172
2.14.1.7.3. ModifyVSwitchAttribute 2173
2.14.1.7.4. DescribeVSwitches 2174
2.14.1.7.5. DescribeVSwitchAttributes 2177
2.14.1.8. Routing table 2180
2.14.1.8.1. CreateRouteEntry 2180
2.14.1.8.2. DeleteRouteEntry 2184
2.14.1.8.3. DescribeRouteTables 2185
2.14.1.9. Elastic IP Address (EIP) 2190
2.14.1.9.1. AllocateEipAddress 2190
2.14.1.9.2. AssociateEipAddress 2192
2.14.1.9.3. UnassociateEipAddress 2193
2.14.1.9.4. ModifyEipAddressAttribute 2194
2.14.1.9.5. ReleaseEipAddress 2196
2.14.1.9.6. DescribeEipAddresses 2196
2.14.1.10. Router interface 2200
2.14.1.10.1. ConnectRouterInterface 2200
2.14.1.10.2. DeactivateRouterInterface 2202
2.14.1.10.3. ModifyRouterInterfaceSpec 2203
2.14.1.10.4. DeleteRouterInterface 2204
2.14.1.10.5. DescribeRouterInterfaces 2206
2.14.1.10.6. ActivateRouterInterface 2211
2.14.1.10.7. ModifyRouterInterfaceAttribute 2212
2.14.1.10.8. CreateRouterInterface 2214
2.14.1.11. Physical connection 2218
2.14.1.11.1. CreatePhysicalConnection 2218
2.14.1.11.2. CancelPhysicalConnection 2221
2.14.1.11.3. DeletePhysicalConnection 2222

2.14.1.11.4. ModifyPhysicalConnectionAttribute 2223
2.14.1.11.5. DescribePhysicalConnections 2225
2.14.1.11.6. TerminatePhysicalConnection 2230
2.14.1.11.7. EnablePhysicalConnection 2231
2.14.1.12. Virtual border router 2233
2.14.1.12.1. CreateVirtualBorderRouter 2233
2.14.1.12.2. DeleteVirtualBorderRouter 2235
2.14.1.12.3. DescribeVirtualBorderRouters 2236
2.14.1.12.4. DescribeVirtualBorderRoutersForPhysicalConn... 2241
2.14.1.12.5. ModifyVirtualBorderRouterAttribute 2245
2.14.1.12.6. TerminateVirtualBorderRouter 2247
2.14.1.12.7. RecoverVirtualBorderRouter 2248
2.14.1.13. NAT Gateway 2250
2.14.1.13.1. CreateNatGateway 2250
2.14.1.13.2. DeleteNatGateway 2254
2.14.1.13.3. ModifyNatGatewaySpec 2255
2.14.1.13.4. ModifyNatGatewayAttribute 2257
2.14.1.13.5. DescribeNatGateways 2258
2.14.1.13.6. CreateBandwidthPackage 2263
2.14.1.13.7. ModifyBandwidthPackageSpec 2265
2.14.1.13.8. DescribeBandwidthPackages 2266
2.14.1.13.9. ModifyBandwidthPackageAttribute 2272
2.14.1.13.10. DeleteBandwidthPackage 2273
2.14.1.13.11. AddBandwidthPackageIps 2274
2.14.1.13.12. RemoveBandwidthPackageIps 2275
2.14.1.13.13. CreateForwardEntry 2277
2.14.1.13.14. DeleteForwardEntry 2278
2.14.1.13.15. ModifyForwardEntry 2279

2.14.1.13.16. DescribeForwardTableEntries 2281
2.14.1.13.17. CreateSnatEntry 2284
2.14.1.13.18. DeleteSnatEntry 2286
2.14.1.13.19. ModifySnatEntry 2287
2.14.1.13.20. DescribeSnatTableEntries 2288
2.14.1.14. High-Availability Virtual IP 2292
2.14.1.14.1. CreateHaVip 2292
2.14.1.14.2. ModifyHaVipAttribute 2295
2.14.1.14.3. DeleteHaVip 2296
2.14.1.14.4. AssociateHaVip 2298
2.14.1.14.5. UnassociateHaVip 2300
2.14.1.14.6. DescribeHaVips 2303
2.14.1.15. DescribeRegions 2307
2.14.1.16. DescribeZones 2309
2.14.1.17. DescribeAccessPoints 2311
2.14.2. SDK reference 2314
2.14.2.1. Call the SDK for Java 2314
2.14.2.1.1. Quick start 2314
2.14.2.1.2. Usage 2315
2.14.2.1.2.1. Install the SDK for Java 2315
2.14.2.1.2.2. Configure identity verification credentials 2316
2.14.2.1.2.3. Call a service 2316
2.14.2.1.2.4. Handle exceptions 2317
2.14.2.1.2.5. Common errors 2318
2.14.2.2. Call the SDK for Python 2319
2.14.2.2.1. Quick start 2319
2.14.2.2.2. Usage 2321
2.14.2.2.2.1. Install the SDK for Python 2321

2.14.2.2.2.2. Configure identity verification credentials 2322
2.14.2.2.2.3. Call a service 2322
2.14.2.2.2.4. Set HTTPS requests 2323
2.14.2.2.2.5. Handle exceptions 2324
2.14.2.2.2.6. Common errors 2324
2.14.2.3. Call the SDK for PHP 2325
2.14.2.3.1. Quick start 2325
2.14.2.4. Call the SDK for Go 2326
2.14.2.4.1. Quick start 2326
2.14.2.4.2. Usage 2328
2.14.2.4.2.1. Install the VPC SDK for Go 2328
2.14.2.4.2.2. Configure identity verification credentials 2329
2.14.2.4.2.3. Call a service 2329
2.14.2.4.2.4. Handle exceptions 2331
2.14.2.4.2.5. Customize configurations 2332
2.14.2.4.2.6. Asynchronous method invocation 2333
2.14.2.4.2.7. Use CommonRequest 2335
2.14.2.4.2.8. Common errors 2335
2.14.2.5. Call the SDK for .NET 2337
2.14.2.5.1. Quick start 2337
2.14.2.5.2. Usage 2339
2.14.2.5.2.1. Install the SDK for .NET 2339
2.14.2.5.2.2. Configure identity verification credentials 2340
2.14.2.5.2.3. Call a service 2340
2.14.2.5.2.4. Handle exceptions 2341
2.14.2.5.2.5. Call an API through CommonRequest 2342
2.14.2.5.2.6. Common errors 2345
2.14.2.6. Obtain an endpoint 2345

2.14.2.7. Obtain an AccessKey pair 2346
2.15. Log Service 2347
2.15.1. API reference 2347
2.15.1.1. Overview 2347
2.15.1.2. Obtain an AccessKey pair 2348
2.15.1.3. Common request headers 2348
2.15.1.4. Common response headers 2350
2.15.1.5. Request signature 2351
2.15.1.6. Common error codes 2357
2.15.1.7. Logstore operations 2359
2.15.1.7.1. CreateLogstore 2359
2.15.1.7.2. DeleteLogstore 2362
2.15.1.7.3. UpdateLogstore 2363
2.15.1.7.4. GetLogstore 2366
2.15.1.7.5. ListLogstore 2368
2.15.1.7.6. ListShards 2370
2.15.1.7.7. SplitShard 2374
2.15.1.7.8. MergeShards 2378
2.15.1.7.9. GetCursor 2382
2.15.1.7.10. PullLogs 2385
2.15.1.7.11. PostLogStoreLogs 2388
2.15.1.7.12. GetLogs 2391
2.15.1.7.13. GetHistograms 2396
2.15.1.7.14. CreateIndex 2402
2.15.1.7.15. DeleteIndex 2407
2.15.1.7.16. GetIndex 2409
2.15.1.7.17. UpdateIndex 2415
2.15.1.8. Logtail machine group operations 2420

2.15.1.8.1. CreateMachineGroup 2420
2.15.1.8.2. DeleteMachineGroup 2424
2.15.1.8.3. UpdateMachineGroup 2426
2.15.1.8.4. ListMachineGroup 2430
2.15.1.8.5. GetMachineGroup 2432
2.15.1.8.6. ApplyConfigToMachineGroup 2436
2.15.1.8.7. RemoveConfigFromMachineGroup 2438
2.15.1.8.8. ListMachines 2440
2.15.1.8.9. GetAppliedConfigs 2444
2.15.1.9. Logtail configuration operations 2447
2.15.1.9.1. CreateConfig 2447
2.15.1.9.2. ListConfig 2454
2.15.1.9.3. GetAppliedMachineGroups 2456
2.15.1.9.4. GetConfig 2459
2.15.1.9.5. DeleteConfig 2464
2.15.1.9.6. UpdateConfig 2466
2.15.1.10. Consumer group operations 2472
2.15.1.10.1. CreateConsumerGroup 2472
2.15.1.10.2. DeleteConsumerGroup 2474
2.15.1.10.3. GetCheckPoint 2476
2.15.1.10.4. HeartBeat 2479
2.15.1.10.5. ListConsumerGroup 2481
2.15.1.10.6. UpdateCheckPoint 2483
2.15.1.10.7. UpdateConsumerGroup 2486
2.15.1.11. Project operations 2489
2.15.1.11.1. CreateProject 2489
2.15.1.11.2. DeleteProject 2491
2.15.1.11.3. GetProject 2492

2.15.1.11.4. ListProject 2494
2.15.1.11.5. GetProjectLogs 2498
2.15.1.12. Description of common resources 2502
2.15.1.12.1. Data model 2502
2.15.1.12.2. Data encoding methods 2506
2.15.1.12.3. Logstores 2507
2.15.1.12.4. Shard 2508
2.15.1.12.5. Logtail configuration 2509
2.15.1.12.6. Logtail machine group 2512
2.15.2. SDK reference 2514
2.15.2.1. Introduction 2514
2.15.2.1.1. Overview 2514
2.15.2.1.2. SDK configurations 2515
2.15.2.1.3. Troubleshooting 2517
2.15.2.1.4. API specifications 2522
2.15.2.2. Java SDK 2525
2.15.2.3. .NET SDK 2531
2.15.2.4. Use .NET Core SDK 2532
2.15.2.5. PHP SDK 2533
2.15.2.6. Python SDK 2537
2.15.2.7. Android SDK 2541
2.15.2.8. C SDK 2541
2.15.2.9. GO SDK 2541
2.15.2.10. iOS SDK 2541
2.16. Apsara Stack Security 2542
2.16.1. API overview 2542
2.16.2. Apsara Stack Security Console 2542
2.16.2.1. List of operations 2542

2.16.2.2. Make API requests 2543
2.16.2.2.1. Request structure 2543
2.16.2.2.2. Signature mechanism 2544
2.16.2.2.3. Common request parameters 2546
2.16.2.2.4. Response structure 2547
2.16.2.3. APIs 2547
2.16.2.3.1. DescribeAliyunAccounts 2547
2.16.2.3.2. ModifyAliyunAccount 2549
2.16.2.3.3. DescribeFeatures 2550
2.16.3. Threat Detection Service (TDS) 2551
2.16.3.1. List of operations 2551
2.16.3.2. Make API requests 2557
2.16.3.2.1. Request structure 2557
2.16.3.2.2. Signature mechanism 2558
2.16.3.2.3. Common request parameters 2560
2.16.3.2.4. Response structure 2561
2.16.3.3. Security overview operations 2561
2.16.3.3.1. DescribeDomain 2561
2.16.3.3.2. DescribeEventsCount 2562
2.16.3.3.3. DescribeOverviewEventsTrend 2564
2.16.3.4. Network traffic management operations 2566
2.16.3.4.1. DescribeHostTraffic 2566
2.16.3.4.2. DescribeHostTrafficTrend 2569
2.16.3.4.3. DescribeTopTraffic 2571
2.16.3.5. Access analysis operations 2573
2.16.3.5.1. DescribeAccessCount 2573
2.16.3.5.2. DescribeTopAccess 2575
2.16.3.5.3. DescribeAccessList 2576

2.16.3.5.4. DescribeAccessTypeCount 2578
2.16.3.5.5. DescribeMaliciousIpDetail 2580
2.16.3.5.6. DescribeMaliciousIpBehaviorList 2581
2.16.3.5.7. DescribeMaliciousIpBehaviorMap 2583
2.16.3.6. Large screen operations 2585
2.16.3.6.1. DescribeScreenName 2585
2.16.3.6.2. ModifyScreenName 2586
2.16.3.6.3. DescribeFlowMap 2587
2.16.3.6.4. DescribeFlowTop 2589
2.16.3.6.5. DescribeScore 2590
2.16.3.6.6. DescribeDailyCount 2592
2.16.3.6.7. DescribeScreenAttackCount 2594
2.16.3.6.8. DescribeScreenAttackTrend 2595
2.16.3.6.9. DescribeScreenHighRiskAssets 2597
2.16.3.7. Event analysis operations 2599
2.16.3.7.1. DescribeEventsTrend 2599
2.16.3.7.2. DescribeEventTypeCount 2601
2.16.3.7.3. DescribeSecurityEventCount 2602
2.16.3.7.4. DescribeSecurityEventList 2604
2.16.3.7.5. DescribeListByType 2607
2.16.3.7.6. DescribeDdosAnalyse 2610
2.16.3.7.7. DescribeDdosFlowDetail 2612
2.16.3.8. Security report operations 2615
2.16.3.8.1. AddReportConfig 2615
2.16.3.8.2. DescribeReportConfigs 2616
2.16.3.8.3. ModifyReportConfig 2618
2.16.3.8.4. DeleteReportConfigs 2620
2.16.3.9. Threat Detection Service operations 2621

2.16.3.9.1. DescribeTrendCount 2621
2.16.3.9.2. DescribeAttackDistribute 2623
2.16.3.9.3. DescribeAttackTrend 2624
2.16.3.9.4. DescribeAttackTypeCount 2626
2.16.3.9.5. DescribeAttackList 2628
2.16.3.9.6. DescribeCountByType 2630
2.16.3.9.7. DescribeSecurityThreatCount 2631
2.16.3.9.8. DescribeSecurityThreatList 2633
2.16.3.9.9. DescribeThreatCount 2636
2.16.3.9.10. DescribeThreatCountByType 2638
2.16.3.9.11. DescribeThreatTop 2639
2.16.3.9.12. DescribeThreatAnalyseList 2640
2.16.3.9.13. DescribeHighRiskAssets 2644
2.16.3.10. Asset management operations 2646
2.16.3.10.1. DescribeDistributionByCodeType 2646
2.16.3.10.2. DescribeSystemByCodeType 2648
2.16.3.10.3. DescribeAssetGroup 2649
2.16.3.10.4. CreateNatAsset 2651
2.16.3.10.5. ModifyRegion 2652
2.16.3.10.6. ModifyAssetGroup 2653
2.16.3.10.7. ModifyGroup 2654
2.16.3.10.8. ModifyAsset 2655
2.16.3.10.9. DescribeTotalAssetNumber 2656
2.16.3.10.10. DescribeAllDistribution 2657
2.16.3.10.11. DescribeAssetsList 2659
2.16.3.10.12. DescribeUuidIpList 2662
2.16.3.10.13. DescribeIpList 2663
2.16.3.10.14. DescribePortList 2664

2.16.3.10.15. DescribeThisMonthAssets 2666
2.16.3.10.16. DescribeAssetsTotalCount 2667
2.16.3.10.17. DeleteAsset 2668
2.16.3.11. Alerting setting operations 2669
2.16.3.11.1. CreateContact 2669
2.16.3.11.2. DescribeContactsList 2670
2.16.3.11.3. ModifyContact 2672
2.16.3.11.4. DeleteContact 2673
2.16.3.11.5. DescribeAlarmConfig 2674
2.16.3.11.6. ModifyAlarmConfig 2676
2.16.3.11.7. DescribeReadStatus 2677
2.16.4. Server Guard 2678
2.16.4.1. List of operations 2678
2.16.4.2. Make API requests 2684
2.16.4.2.1. Request structure 2684
2.16.4.2.2. Signature mechanism 2685
2.16.4.2.3. Common request parameters 2687
2.16.4.2.4. Response structure 2688
2.16.4.3. Asset management operations 2688
2.16.4.3.1. CreateGroup 2688
2.16.4.3.2. DescribeGroupSummary 2690
2.16.4.3.3. DescribeGroupStruct 2692
2.16.4.3.4. DeleteGroup 2694
2.16.4.3.5. DescribeAllTag 2695
2.16.4.3.6. DescribeBetachTag 2696
2.16.4.3.7. ModifyBetachTag 2697
2.16.4.3.8. DeleteTag 2698
2.16.4.3.9. DescribeAllEntity 2699

2.16.4.3.10. DescribeEntityList 2701
2.16.4.3.11. ModifyEntityGroup 2704
2.16.4.3.12. DescribeMachines 2705
2.16.4.3.13. DescribeMachineDetail 2707
2.16.4.3.14. DescribePropertyScheduleConfig 2709
2.16.4.3.15. ModifyPropertyScheduleConfig 2710
2.16.4.3.16. DescribePropertyStatistic 2712
2.16.4.3.17. DescribePropertyPortItem 2713
2.16.4.3.18. DescribePropertyPortDetail 2715
2.16.4.3.19. DescribePropertyPortDiff 2718
2.16.4.3.20. DescribePropertyProcItem 2720
2.16.4.3.21. DescribePropertyProcDetail 2722
2.16.4.3.22. DescribePropertyProcDiff 2725
2.16.4.3.23. DescribePropertySoftwareItem 2728
2.16.4.3.24. DescribePropertySoftwareDetail 2730
2.16.4.3.25. DescribePropertySoftwareDiff 2732
2.16.4.3.26. DescribePropertyUserItem 2735
2.16.4.3.27. DescribePropertyUserDetail 2737
2.16.4.3.28. DescribePropertyUserDiff 2740
2.16.4.3.29. PushAllTask 2743
2.16.4.3.30. DescribeTopRiskyAssets 2745
2.16.4.3.31. UnbindAegis 2747
2.16.4.3.32. UninstallAegis 2748
2.16.4.4. Vulnerability management operations 2749
2.16.4.4.1. DescribeTarget 2749
2.16.4.4.2. ModifyVulTarget 2750
2.16.4.4.3. DescribeVulTargetStatistics 2751
2.16.4.4.4. DescribeTargetConfig 2753

2.16.4.4.5. ModifyTargetConfig 2754
2.16.4.4.6. DescribeVulConfig 2755
2.16.4.4.7. ModifyVulConfig 2757
2.16.4.4.8. DescribeAutoDelConfig 2758
2.16.4.4.9. ModifyAutoDelConfig 2759
2.16.4.4.10. DescribeVulLevel 2760
2.16.4.4.11. ModifyVulLevel 2760
2.16.4.4.12. CreateVulWhitelist 2761
2.16.4.4.13. DescribeVulWhitelist 2762
2.16.4.4.14. DeleteVulWhitelist 2764
2.16.4.4.15. DescribeGroupedVul 2765
2.16.4.4.16. DescribeVulList 2770
2.16.4.4.17. DescribeVulDetails 2775
2.16.4.4.18. DescribeVulNumStatistics 2778
2.16.4.4.19. DescribeVulLevelStatistics 2780
2.16.4.4.20. DescribeVulMachineList 2782
2.16.4.4.21. OperateVul 2785
2.16.4.4.22. ModifyBatchIgnoreVul 2787
2.16.4.4.23. DeleteVulBatch 2788
2.16.4.4.24. ExportVul 2789
2.16.4.4.25. DescribeVulExportInfo 2791
2.16.4.5. Baseline check operations 2793
2.16.4.5.1. DescribeStrategy 2793
2.16.4.5.2. DescribeStratetyDetail 2796
2.16.4.5.3. ModifyStrategy 2800
2.16.4.5.4. DeleteStrategy 2801
2.16.4.5.5. DescribeStrategyTarget 2802
2.16.4.5.6. ModifyStrategyTarget 2804

2.16.4.5.7. DescribeUuidConfig 2805
2.16.4.5.8. ModifyMachineConfig 2806
2.16.4.5.9. DescribeUserSetting 2807
2.16.4.5.10. CreateUserSetting 2808
2.16.4.5.11. DescribeRiskWhiteList 2809
2.16.4.5.12. BatchDeleteWhiteList 2811
2.16.4.5.13. CreateUserWhiteList 2812
2.16.4.5.14. DescribeStratety 2813
2.16.4.5.15. DescribeStrategyExecDetail 2815
2.16.4.5.16. DescribeRiskType 2817
2.16.4.5.17. Describesummary 2819
2.16.4.5.18. OperateWarning 2822
2.16.4.5.19. ExportWarning 2823
2.16.4.5.20. DescribeExportInfo 2825
2.16.4.6. Unusual logon operations 2826
2.16.4.6.1. DescribeBaseConfigs 2826
2.16.4.6.2. ModifyBaseConfig 2829
2.16.4.6.3. DeleteBaseConfig 2831
2.16.4.6.4. DescribeSwitchConfigs 2832
2.16.4.6.5. ModifySwitchConfig 2834
2.16.4.6.6. DescribeConfigTarget 2836
2.16.4.7. Webshell detection operations 2837
2.16.4.7.1. DescribeWebPath 2837
2.16.4.7.2. ModifyWebPath 2839
2.16.4.7.3. DescribeCategoryCount 2840
2.16.4.7.4. DescribeWebshell 2841
2.16.4.7.5. OperateTrojan 2844
2.16.4.7.6. DescribeQuaraFile 2846

2.16.4.7.7. RollbackQuaraFile 2848
2.16.4.8. Server exception detection operations 2849
2.16.4.8.1. DescribeSuspEventTypes 2849
2.16.4.8.2. DescribeSuspTrendStatistics 2850
2.16.4.8.3. OperateSuspiciousEvent 2851
2.16.4.8.4. OperateLoginLog 2853
2.16.4.8.5. CreateSuspiciousExport 2854
2.16.4.8.6. DescribeSuspiciousExportInfo 2856
2.16.4.8.7. DescribeVirusInfo 2858
2.16.4.9. Server log retrieval operations 2859
2.16.4.9.1. CreateLogQuery 2859
2.16.4.9.2. DescribeLogQuery 2860
2.16.4.9.3. DeleteLogQuery 2862
2.16.4.9.4. DescribeFilterFields 2863
2.16.4.9.5. DescribeHistogram 2864
2.16.4.9.6. DescribeLogInfo 2866
2.16.4.9.7. DescribeLogItems 2869
2.16.5. Anti-DDoS 2872
2.16.5.1. List of operations 2872
2.16.5.2. Make API requests 2874
2.16.5.2.1. Request structure 2874
2.16.5.2.2. Signature mechanism 2875
2.16.5.2.3. Common request parameters 2877
2.16.5.2.4. Response structure 2878
2.16.5.3. APIs 2878
2.16.5.3.1. CheckIpSegment 2878
2.16.5.3.2. DescribeRegionName 2880
2.16.5.3.3. CreateIpSegment 2882

2.16.5.3.4. DescribeIpSegment 2883
2.16.5.3.5. DeleteIpSegment 2886
2.16.5.3.6. ModifyIpSegment 2887
2.16.5.3.7. CreateDdosPolicy 2888
2.16.5.3.8. DescribeDdosPolicies 2890
2.16.5.3.9. DeleteDdosPolicy 2892
2.16.5.3.10. ModifyDdosPolicy 2894
2.16.5.3.11. DescribeBlockSwitchs 2895
2.16.5.3.12. ModifyBlockSwitchs 2897
2.16.5.3.13. DescribeDdosEvents 2898
2.16.5.3.14. DescribeFlowAnalysisResult 2903
2.16.5.3.15. DescribeFlowDetails 2905
2.16.5.3.16. CancelCleanStatus 2907
2.16.5.3.17. CreateWhiteList 2908
2.16.5.3.18. DescribeWhiteList 2909
2.16.5.3.19. DeleteWhiteList 2911
2.16.5.3.20. DescribeConsoleDdosPolicies 2912
2.16.6. Error codes 2915
2.17. Key Management Service (KMS) 2923
2.17.1. API reference 2924
2.17.1.1. Make API requests 2924
2.17.1.1.1. Overview 2924
2.17.1.1.2. Request structure 2924
2.17.1.1.3. Common parameters 2924
2.17.1.1.4. Request signatures 2926
2.17.1.1.5. Responses 2928
2.17.1.2. Use RAM to authorize KMS resources 2931
2.17.1.3. Encryption Context 2933

2.17.1.4. Impact of CMK states on API calls 2934
2.17.1.5. API list 2935
2.17.1.5.1. CancelKeyDeletion 2935
2.17.1.5.2. CreateKey 2936
2.17.1.5.3. Decrypt 2938
2.17.1.5.4. DescribeKey 2940
2.17.1.5.5. DescribeRegions 2942
2.17.1.5.6. DisableKey 2943
2.17.1.5.7. EnableKey 2944
2.17.1.5.8. Encrypt 2945
2.17.1.5.9. GenerateDataKey 2947
2.17.1.5.10. ListKeys 2949
2.17.1.5.11. ScheduleKeyDeletion 2951
2.17.2. SDK reference 2953
2.17.2.1. Create an AccessKey pair 2953
2.17.2.2. SDK 2953
2.17.2.3. JAVA SDK sample code 2953
2.17.2.4. Create an AccessKey pair 2959
2.17.2.5. SDK 2959
2.17.2.6. JAVA SDK sample code 2959
2.18. Apsara Stack DNS 2966
2.18.1. Overview 2966
2.18.1.1. Calling methods 2966
2.18.1.2. Supported formats 2966
2.18.1.3. Instructions 2966
2.18.1.4. Time format 2966
2.18.2. List of operations by function 2966
2.18.3. Prerequisites 2966

2.18.3.1. Obtain an AccessKey pair ---- 2967
2.18.3.2. Obtain an endpoint ---- 2967
2.18.4. SDK example ---- 2968
2.18.4.1. Create a client ---- 2968
2.18.4.2. Obtain global authoritative zones ---- 2969
2.18.4.3. Obtain global authoritative RRSets ---- 2970
2.18.4.4. Add global RRSets ---- 2972
2.18.4.5. Delete global RRSets ---- 2976
2.18.4.6. Update global RRSets ---- 2978
2.18.4.7. Configure descriptions for global RRSets ---- 2981

1.Apsara Stack console

1.1. API overview

Apsara Stack console APIs are based on the RESTful architecture. You can develop APIs by using programming languages that support HTTP and using architectural principles and constraints defined by REST.

Currently, APIs released by the cloud platform are mainly those of the following products and their related businesses: Elastic Compute Service (ECS), Server Load Balancer (SLB), Object Storage Service (OSS), and ApsaraDB. You can log on to and manage the Apsara Stack console by using standard HTTP requests. URIs specify the locations of resources, and you can use POST, PUT, GET, and DELETE methods to perform operations on resources. For more information, see Operation instructions.

Operation instructions

Method	Description
GET	Queries resources
PUT	Modifies resources
POST	Creates resources
DELETE	Deletes resources

The current version only supports data transfer by using the JSON format. In the future, it can also support the XML format.

Different regions in the cloud platform support different APIs and have different parameter constraints. Therefore, you must first understand the components, supported product types, and network configurations of each region in the environment before using the APIs provided in this document for programming and development.

1.2. Call methods

1.2.1. Common parameters

Common request parameters are request parameters that all APIs must use. The parameters detailed in Common parameters must be placed in the HTTP request header.

Common parameters

Name	Type	Required	Description
AccessKeyId	String	Yes	The AccessKey ID is issued by the Apsara Stack console gateway for users to access services.
Signature	String	Yes	The signature result string. For more information about the signature algorithm, see Signature mechanism.

Name	Type	Required	Description
SignatureMethod	String	Yes	The signature method, which currently supports HMAC-SHA256.
Version	String	Yes	API version. Current version: 20160701.

Request example:

```
POST /gateway/api/cloudOts/createOtsInstance? clusterName=&departmentId=515&description=&instanceName=test17&projectId=45&regionId=cn-hangzhou-am24 HTTP/1.1
Signature: Y/U4K4bEMevzaqpCa19Jf4rt2mmSDyFLXwsqcO05****
SignatureMethod: HMAC-SHA256
Version: 20160701
AccessKeyId: QNHbByQaJHgE****
Host: localhost:8094
Connection: Keep-Alive
```

1.2.2. Signature mechanism

The Apsara Stack console authenticates each access request sender by using the symmetrical encryption with AccessKey ID and AccessKey Secret.

AccessKey ID is used to identify visitors. AccessKey Secret is used to encrypt the signature strings on the client side and verify the keys of these signature strings on the server side. AccessKey ID and AccessKey Secret are officially provided by the Apsara Stack console for visitors.

The signature algorithm is as follows:

```
public class Signature {
 AccessKeyId
 public final static String ACCESS_KEY_ID = "AccessKeyId";
 AccessKeyId signature method
 public final static String HTTP_HEADER_SIG_METHOD = "SignatureMethod";
 Version
 public final static String HTTP_HEADER_VERSION = "Version";
 public final static String SIGNATUREMETHOD = "HMAC-SHA256";
 public final static String VERSION = "20160701";

 Signature generation algorithm
 @param sHttpMethod HTTP request methods: POST, GET, PUT, and DELETE
 @param accessKeyId is provided by the Apsara Stack console offline for users
 @param accessSecret is provided by the Apsara Stack console offline for users
 @return generated signature

 String calcSignature(String sHttpMethod, String accessKeyId, String  accessSecret) {
      Map<String, String> parameterMap = new HashMap<String, String>();
      parameterMap.put(ACCESS_KEY_ID, accessKeyId);
      parameterMap.put(HTTP_HEADER_SIG_METHOD, SIGNATUREMETHOD);
      parameterMap.put(HTTP_HEADER_VERSION, SIGNATUREMETHOD);
      String sSignature = SignatureHelper.simpleSignRequest(sHttpMethod, parameterMap, accessSecret
);
      return sSignature;
   }
}
```

The `SignatureHelper. simpleSignRequest (String method, Map<String, String> parameters, String accessKeySecret)` method is provided by *the RESTful API signature SDK of Apsara Stack console*. Obtain this SDK from the operations personnel.

1.2.3. Request structure

Service address

The access address of API service: apigateway.dtdream.com.

Communication protocol

HTTP is the supported protocol for sending requests.

Request methods

HTTP GET, POST, PUT, and DELETE methods are supported for sending requests. Select a method according to the actual conditions of APIs.

Request parameters

Authentication-related request parameters must be placed in the HTTP request header.

Character encoding

Both requests and responses are encoded by using UTF-8 character set.

Character format

Both requests and responses are in the JSON format.

1.2.4. Response structure

Response structure parameters

Description about the response structure parameters are detailed in Parameter description.

Parameter description

Name	Type	Required	Description
result	String	Yes	The operation result, which has the following values: • *success*: indicates the request is successful. • *failed*: indicates the request is failed.
responseCode	String	Yes	Secondary error codes. This field is empty and reserved.
errorMsg	String	Yes	The error message. If the request is successful, this field is empty. If the request is failed, this field is the error message. Note If this field coexists with return_subCode, use return_subCode in priority.
errorDetail	String	Yes	The error details. If the request is successful, this field is empty. If the request is failed, this field is the error details. Note If this field coexists with return_subMsg, use return_subMsg in priority.
data	String	Yes	This field contains users' business data.
pageSize	Integer	No	The number of rows on each page in a paged query.

Name	Type	Required	Description
pageNum	Integer	No	The page number in a paged query.
totalRows	long	No	The total number of rows queried.
rows	String	No	Details list of the queried information.
return_subCode	String	Yes	The error message. If the request is successful, this field is empty. If the request is failed, this field is the error message.
return_subMsg	String	Yes	The error details. If the request is successful, this field is empty. If the request is failed, this field is the error details.

Response examples

- For APIs that successfully create an Elastic Compute Service (ECS) instance, the response example is as follows:

```
{
  "result": "success",
   "data": {
      "regionId": "97d83522-0d78-4e95-a8b5-361eaa580504",
      "successNum": 1,
      "taskId": "37b0deb0-9a80-467a-8e2a-0c7a56279065",
      "ecsList": [
         {
            "instanceId": "77cc5270-3cd5-4050-a48e-a1d77377****",
            "batchIndex": 0,
            "reservedType": "taskCreating"
         }
      ]
   },
   "errorDetail"": "",
   "responseCode": "200",
   "errorMsg"": ""
}
```

- For APIs that failed to create an ECS instance, the response example is as follows:

```
{
  "result":"failed",
  "responseCode":"",
  "data": "",
  "errorMsg":"Permission denied",
  "errorDetail":"XXX permission is required, but the user's permission is XXX"
}
```

- For APIs that obtain a list of server instances in a paged format, the response example is as follows:

```
{
  "result": "success",
  "responseCode": "200",
  "data": {
    "pageSize": 4,
    "totalRows": 93,
    "pageNum": 1,
    "rows": [
      {
        "instanceId": "i-25l93****",
        "instanceName": "iZ25l939****",
        ..........

      },
      {
        "instanceId": "i-25xev****",
        "instanceName": "iZ25xeve****",
        ...........
      },
      {
        "instanceId": "i-882ql****",
        "instanceName": "CreateE****",
        ............
      },
      {
        "instanceId": "i-8835j****",
        "instanceName": "lanlan****",
        .............
      }
    ]
  },
  "errorMsg": "",
  "errorDetail": ""
}
```


- For APIs that obtain a list of server instances in a non-paged format, the response example is as follows:

```
{
  "result": "success",
  "responseCode": "200",
  "data": {
    "totalRows": 4,
    "rows": [
      {
        "instanceId": "i-25l93****",
        "instanceName": "iZ25l939****",
        ..........

      },
      {
        "instanceId": "i-25xev****",
        "instanceName": "iZ25xeve****",
        ............
      },
      {
        "instanceId": "i-882ql****",
        "instanceName": "CreateE****",
        ..............
      },
      {
        "instanceId": "i-8835j****",
        "instanceName": "lanlan****",
        ...............
      }
    ]
  },
  "errorMsg": "",
  "errorDetail": ""
}
```


1.3. Region-related APIs

1.3.1. getRegionList

Description

Obtains the information of all regions and views the region type and product list supported by the cloud platform.

- All cloud service data and operations are based on regions. Therefore, you must obtain the related region information such as the region ID, region type, and product list to create and manage cloud resources.
- The region ID is the unique identifier of each region. It is used to specify a specific region to provide cloud services when you create and manage cloud resources.
- The product list contains the product types supported by each region. You must confirm that whether the region supports the required product type before creating cloud resources.
- The network types are divided into classic network type and Virtual Private Cloud (VPC) type. You can access the cloud products of classic network by using Internet. Cloud products of the VPC type can only be accessed within the VPC by default.

Name

getRegionList

URL

`{dtcenter_api_url}/gateway/api/region/list`

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameter

None.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
regionId	String	The region ID, which is the unique identifier of each region and is used to specify a specific region to provide cloud services when you create and manage cloud resources
regionName	String	The region name

Name	Type	Description
zoneList	List<Zone>	A list of zones. Zones are physical areas with isolated power and networks within a region. Zones can be interconnected by using the intranet. Fault isolation exists between different zones. For more information, see getZoneList. Values: • *zoneId*: the zone ID • *zoneName*: the zone name • *availResCreate*: the resource types that can be created • *availDiskCate*: the available data disk types • *availSysCate*: the available system disk types • *availableResources*: the available instance resources • *availableResourceCreation*: the resources that can be created in the zone
regionType	String	The region type Value: *regft* (Apsara Stack regions)
productProvided	ArrayList<String>	A list of products that are supported by the region

productNetworks	ArrayList-<RegionProductNetwork>	The product and network type
		Values:
		• *product*: the product type
		• *networks*: the network type
		  ◦ *VPC*: Virtual Private Cloud
		  ◦ *classic*: classic network
		For example, Elastic Compute Service (ECS) only supports the VPC network type.
		`{ "product": "ECS", "networks": [ "VPC" ] }`

Name	Type	Description

productNicTypes	ArrayList<RegionProductNicType>	The product and NIC type
		Values:
		• *product*: the product type
		• *nicType*: the NIC type
		  ○ *internet*: the public network
		  ○ *intranet*: the private network
		For example, Server Load Balancer (SLB) supports both Internet and intranet NIC types.
		`{ "product": "SLB", "nicType": [ "internet", "intranet" ] }`

lanType	String	The network type Value: *VPC* (Virtual Private Cloud)
eipSupport	boolean	Indicates whether this region supports Elastic IP Address (EIP) Values: • *true*: supported • *false*: not supported
switchControl	boolean	Indicates whether this region supports VRouter control Values: • *true*: supported • *false*: not supported
snapSupport	boolean	Indicates whether this region supports snapshot Values: • *true*: supported • *false*: not supported

Name	Type	Description
aliType	String	Region type Value: *private* (Apsara Stack regions)

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/region/list
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": [
{
"regionId": "cn-hangzhou-am24",
"regionName": "cn-hangzhou-am24",
"zoneList": [
{
"availDiskCate": [
"cloud"
],
"availResCreate": [
"instance",
"disk"
],
"availSysCate": [],
"availableResourceCreation": [],
"availableResources": [],
"zoneId": "cn-hangzhou-hsd-am24001-a,cn-hangzhou-hsd-am24001-b",
"zoneName": "cn-hangzhou-hsd-am24001-a,cn-hangzhou-hsd-am24001-b"
}
],
"regionType": "regft",
"productProvided": [
"ECS",
"RDS",
"SLB",
"OSS",
"CMS",
```

```
"RAM",
"AAS",
"AK",
"OTS",
"OTSTable",
"ORACLE",
"ADS",
"ODPS",
"VPC"
],
"productNetworks": [
{
"product": "ECS",
"networks": [
"VPC"
]
},
{
"product": "RDS",
"networks": [
"VPC"
]
},
{
"product": "ADS",
"networks": []
},
{
"product": "ODPS",
"networks": []
}
],
"slbInstanceTypes": [
{
"nicType": "intranet",
"networks": [
"classic",
"VPC"
]
},
{
"nicType": "internet"
```

```
"networks": [
"classic"
]
}
],
"lanType": "VPC",
"eipSupport": true,
"switchControl": false,
"snapSupport": true,
"aliType": "private"
},
{
"regionId": "cn-beijing",
"regionName": "ChinaNorth2",
"zoneList": [],
"regionType": "regft",
"productProvided": [
"RAM",
"CMS",
"AAS",
"VPC",
"ECS"
],
"productNetworks": [
{
"product": "ECS",
"networks": [
"classic",
"VPC"
]
}
],
"slbInstanceTypes": [],
"lanType": "VPC",
"eipSupport": false,
"switchControl": false,
"snapSupport": true,
"aliType": "private"
},
{
"regionId": "424f5a39-ec0b-441f-8f71-26b12ba496ea",
```

```
"regionName": "dtcube01",
"zoneList": [
{
"phynetworkName": "physnet2",
"vlanRanges": [
{
"vlanIdStart": 3001,
"vlanIdEnd": 3050
}
],
"zoneId": "nova",
"zoneName": "DefaultZone"
}
],
"regionType": "region-kspec",
"productProvided": [
"VPC",
"EIP",
"BACKUP",
"OSS",
"ECS",
"SLB"
],
"productNetworks": [
{
"product": "VPC",
"networks": [
"VPC"
]
},
{
"product": "EIP",
"networks": [
"VPC"
]
},
{
"product": "BACKUP",
"networks": [
"VPC"
]
```

```
},
{
"product": "OSS",
"networks": [
"VPC"
]
},
{
"product": "ECS",
"networks": [
"VPC"
]
},
{
"product": "SLB",
"networks": [
"VPC"
]
}
],
"productNicTypes": [
{
"product": "SLB",
"nicType": [
"intranet"
]
}
],
"lanType": "VLAN:physnet2:3001:3050",
"eipSupport": true,
"switchControl": false,
"routerType": "vRouter",
"snapSupport": true
}
],
"errorMsg": "",
"errorDetail": "",
 “return_subCode” : “” ,
 “return_subMsg” : “”
}
```

1.3.2. getZoneList

Description

Zones are physical areas with isolated power and networks within a region. Different zones can be interconnected by using the intranet and have fault isolation.

- The cloud service capabilities provided by different zones may be different. Therefore, when creating cloud resources, you can select different zones to obtain cloud resources with different capabilities. For example, when you create an Elastic Compute Service (ECS) instance, it is possible that zone one supports I/O optimization but zone two does not.
- When you create disks, the type and capacity of disks may be different depending on the selected zones. You must obtain the type and capacity supported by the zone before you configure the disks.

This API allows you to obtain a list of zones in Apsara Stack regions.

Name

getZoneList

URL

`{dtcenter_api_url}/gateway/api/region/zones`

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameter

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
zoneId	String	The zone ID
zoneName	String	The zone name

Name	Type	Description
dataDiskTypeList	ArrayNode	A list of data disk types and parameters Types: • *cloud*: basic cloud disk • *cloud_ssd*: SSD cloud disk • *cloud_efficiency*: ultra cloud disk
sysDiskTypeList	ArrayNode	A list of system disk types and parameters Types: • *cloud*: basic cloud disk • *cloud_ssd*: SSD cloud disk • *cloud_efficiency*: ultra cloud disk

Name	Type	Description

availableResourceCreationList	ArrayNode	A list of resources that can be created in zones:
		Values:
		• *VSwitch*: creates virtual subnets.
		  ○ *true*: supported
		  ○ *false*: not supported
		• *Instance* : creates ECS instances.
		  ○ *true*: supported
		  ○ *false*: not supported
		• *IoOptimized* : I/O optimization
		  ○ *true*: supported
		  ○ *false*: not supported
		• *Disk* : creates disks.
		  ○ *true*: supported
		  ○ *false*: not supported
		For example, the zone supports creating virtual subnets, ECS instances, and disks, and optimizing I/O:
		{
		"availableResourceCreationList": {
		"VSwitch": true,
		"Instance": true,
		"IoOptimized": true,
		"Disk": true
		}
		}

supportGenerations	ArrayNode	The supported ECS generations (Currently, Apsara Stack regions only support ecs-1.)

Name	Type	Description

availableInstanceTypes	ArrayNode	The instance types that instance resources are allowed to create
		Values:
		• *instanceType*: the instance type
		• *cpuNum*: the specific number of CPU cores of the instance type
		• *memory*: the specific memory size of the instance type
		• *instanceTypeFamily*: the instance type family
		• *isSupportIoOptimized*: indicates whether instances of this type support I/O optimization
		Values:
		○ *true*: supported
		○ *false*: not supported
		• *generation*: the instance generation
		Value:
		ecs-1: the first generation
		{
		"availableInstanceTypes": [
		{
		"instanceType": "ecs.s2.xlarge",
		"cpuNum": 2,
		"memory": 8,
		"instanceTypeFamily": "ecs.s2",
		"generation": "ecs-1",
		"isSupportIoOptimized": true
		}
		]
		}

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/region/zones?regionId=cn-shanghai
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": [
    {
      "zoneId": "cn-hangzhou-hsd-am24001-a",
      "zoneName": "cn-hangzhou-hsd-am24001-a",
      "availableResourceCreationList": {
        "VSwitch": true,
        "Instance": true,
        "IoOptimized": false,
        "Disk": true
      },
      "availableResources": [],
      "dataDiskTypeList": [
        {
          "diskType": "cloud_ssd",
          "typeName": "SSD cloud disk",
          "minSize": 20,
          "maxSize": 1024
        },
        {
          "diskType": "cloud_efficiency",
          "typeName": "Ultra cloud disk",
          "minSize": 20,
          "maxSize": 2048
        }
      ],
      "sysDiskTypeList": [
        {
          "diskType": "cloud_ssd",
          "typeName": "SSD cloud disk",
          "minSize": 20,
          "maxSize": 1024
        },
        {
```

```
        {
          "diskType": "cloud_efficiency",
          "typeName": "Ultra cloud disk",
          "minSize": 20,
          "maxSize": 2048
        }
      ],
      "supportGenerations": [
        "ecs-1"
      ],
      "availableInstanceTypes": [
        {
          "instanceType": "ecs.s2.xlarge",
          "cpuNum": 2,
          "memory": 8,
          "instanceTypeFamily": "ecs.s2",
          "generation": "ecs-1",
          "isSupportIoOptimized": true
        },
        {
          "instanceType": "ecs.s2.large",
          "cpuNum": 2,
          "memory": 4,
          "instanceTypeFamily": "ecs.s2",
          "generation": "ecs-1",
          "isSupportIoOptimized": true
        },
        {
          "instanceType": "ecs.s2.2xlarge",
          "cpuNum": 2,
          "memory": 16,
          "instanceTypeFamily": "ecs.s2",
          "generation": "ecs-1",
          "isSupportIoOptimized": true
        },
        {
          "instanceType": "ecs.s3.medium",
          "cpuNum": 4,
          "memory": 4,
          "instanceTypeFamily": "ecs.s3",
          "generation": "ecs-1",
          "isSupportIoOptimized": true
```

```
},
{
  "instanceType": "ecs.s1.small",
  "cpuNum": 1,
  "memory": 2,
  "instanceTypeFamily": "ecs.s1",
  "generation": "ecs-1",
  "isSupportIoOptimized": false
},
{
  "instanceType": "ecs.s3.large",
  "cpuNum": 4,
  "memory": 8,
  "instanceTypeFamily": "ecs.s3",
  "generation": "ecs-1",
  "isSupportIoOptimized": true
},
{
  "instanceType": "ecs.c1.small",
  "cpuNum": 8,
  "memory": 8,
  "instanceTypeFamily": "ecs.c1",
  "generation": "ecs-1",
  "isSupportIoOptimized": true
},
{
  "instanceType": "ecs.t1.small",
  "cpuNum": 1,
  "memory": 1,
  "instanceTypeFamily": "ecs.t1",
  "generation": "ecs-1",
  "isSupportIoOptimized": false
},
{
  "instanceType": "ecs.s2.small",
  "cpuNum": 2,
  "memory": 2,
  "instanceTypeFamily": "ecs.s2",
  "generation": "ecs-1",
  "isSupportIoOptimized": false
},
```

```
        {
          "instanceType": "ecs.s1.medium",
          "cpuNum": 1,
          "memory": 4,
          "instanceTypeFamily": "ecs.s1",
          "generation": "ecs-1",
          "isSupportIoOptimized": false
        }
      ]
    },
    {
      "zoneId": "cn-hangzhou-hsd-am24001-b",
      "zoneName": "cn-hangzhou-hsd-am24001-b",
      "availableResourceCreationList": {
        "VSwitch": true,
        "Instance": true,
        "IoOptimized": false,
        "Disk": true
      },
      "availableResources": [],
      "dataDiskTypeList": [
        {
          "diskType": "cloud_efficiency",
          "typeName": "Ultra cloud disk",
          "minSize": 20,
          "maxSize": 2048
        }
      ],
      "sysDiskTypeList": [
        {
          "diskType": "cloud_efficiency",
          "typeName": "Ultra cloud disk",
          "minSize": 20,
          "maxSize": 2048
        }
      ],
      "supportGenerations": [
        "ecs-1"
      ],
      "availableInstanceTypes": [
        {
          "instanceType": "ecs.s2.xlarge"
```

```
        "instanceType": "ecs.s2.xlarge",
        "cpuNum": 2,
        "memory": 8,
        "instanceTypeFamily": "ecs.s2",
        "generation": "ecs-1",
        "isSupportIoOptimized": true
      },
      {
        "instanceType": "ecs.m1.medium",
        "cpuNum": 4,
        "memory": 16,
        "instanceTypeFamily": "ecs.m1",
        "generation": "ecs-1",
        "isSupportIoOptimized": true
      },
      {
        "instanceType": "ecs.m2.medium",
        "cpuNum": 4,
        "memory": 32,
        "instanceTypeFamily": "ecs.m2",
        "generation": "ecs-1",
        "isSupportIoOptimized": true
      },
      {
        "instanceType": "ecs.s2.large",
        "cpuNum": 2,
        "memory": 4,
        "instanceTypeFamily": "ecs.s2",
        "generation": "ecs-1",
        "isSupportIoOptimized": true
      },
      {
        "instanceType": "ecs.s3.medium",
        "cpuNum": 4,
        "memory": 4,
        "instanceTypeFamily": "ecs.s3",
        "generation": "ecs-1",
        "isSupportIoOptimized": true
      },
      {
        "instanceType": "ecs.s2.2xlarge",
        "cpuNum": 2,
```

```
        "memory": 16,
        "instanceTypeFamily": "ecs.s2",
        "generation": "ecs-1",
        "isSupportIoOptimized": true
    },
    {
        "instanceType": "ecs.m1.xlarge",
        "cpuNum": 8,
        "memory": 32,
        "instanceTypeFamily": "ecs.m1",
        "generation": "ecs-1",
        "isSupportIoOptimized": true
    },
    {
        "instanceType": "ecs.s1.small",
        "cpuNum": 1,
        "memory": 2,
        "instanceTypeFamily": "ecs.s1",
        "generation": "ecs-1",
        "isSupportIoOptimized": false
    },
    {
        "instanceType": "ecs.c2.xlarge",
        "cpuNum": 16,
        "memory": 64,
        "instanceTypeFamily": "ecs.c2",
        "generation": "ecs-1",
        "isSupportIoOptimized": true
    },
    {
        "instanceType": "ecs.s1.large",
        "cpuNum": 1,
        "memory": 8,
        "instanceTypeFamily": "ecs.s1",
        "generation": "ecs-1",
        "isSupportIoOptimized": false
    },
    {
        "instanceType": "ecs.c2.large",
        "cpuNum": 16,
        "memory": 32,
```

```
            "instanceTypeFamily": "ecs.c2",
            "generation": "ecs-1",
            "isSupportIoOptimized": true
        },
        {
            "instanceType": "ecs.s3.large",
            "cpuNum": 4,
            "memory": 8,
            "instanceTypeFamily": "ecs.s3",
            "generation": "ecs-1",
            "isSupportIoOptimized": true
        },
        {
            "instanceType": "ecs.c1.small",
            "cpuNum": 8,
            "memory": 8,
            "instanceTypeFamily": "ecs.c1",
            "generation": "ecs-1",
            "isSupportIoOptimized": true
        },
        {
            "instanceType": "ecs.m2.xlarge",
            "cpuNum": 8,
            "memory": 64,
            "instanceTypeFamily": "ecs.m2",
            "generation": "ecs-1",
            "isSupportIoOptimized": true
        },
        {
            "instanceType": "ecs.c2.medium",
            "cpuNum": 16,
            "memory": 16,
            "instanceTypeFamily": "ecs.c2",
            "generation": "ecs-1",
            "isSupportIoOptimized": true
        },
        {
            "instanceType": "ecs.t1.small",
            "cpuNum": 1,
            "memory": 1,
            "instanceTypeFamily": "ecs.t1",
            "generation": "ecs-1",
```

```
            "isSupportIoOptimized": false
          },
          {
            "instanceType": "ecs.c1.large",
            "cpuNum": 8,
            "memory": 16,
            "instanceTypeFamily": "ecs.c1",
            "generation": "ecs-1",
            "isSupportIoOptimized": true
          },
          {
            "InstanceType": "ecs.s2.small",
            "cpuNum": 2,
             "memory": 2,
             "instanceTypeFamily": "ecs.s2",
            "generation": "ecs-1",
            "isSupportIoOptimized": false
          },
          {
            "instanceType": "ecs.s1.medium",
            "cpuNum": 1,
            "memory": 4,
            "instanceTypeFamily": "ecs.s1",
            "generation": "ecs-1",
            "isSupportIoOptimized": false
          }
        ]
      }
   ],
   "errorMsg"": "",
    "errorDetail": "",
  “return_subCode” : “” ,
  “return_subMsg” : “”
}
```


1.4. User center-related APIs

1.4.1. User-related APIs

1.4.1.1. addUserInfo

Description

Creates a user of the Apsara Stack console.

> Note This API depends on the getRolePage API that can return all roles in the system, so proceed with caution. To not open certain roles, process the role list by yourself.

Name

addUserInfo

URL

{dtcenter_api_url}/gateway/api/users

Request type

POST message.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
loginName	String	Yes	The logon name of the user, which must be 3 to 30 characters in length, start with letters, and only contain letters, numbers, or underscores (_)
fullName	String	Yes	The displayed name of the user, which must be 2 to 30 characters in length and only contain letters
departmentId	String	Yes	The department ID. For more information, see the getDeptRootTree API
cellphoneNum	String	Yes	The mobile phone number of the user
telephoneNum	String	No	The landline number of the user, which is in the format such as 010-86551122 and 01086551122

Name	Type	Required	Description
userEmail	String	Yes	The email address of the user
roleIdList	String	Yes	The string of role IDs, which can contain multiple IDs that are separated by commas (,) and be obtained by using the getRolePage API
mobileNationCode	String	No	The mobile phone area code. By default, no area code exists if not configured.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
UserId	String	The user ID

Examples

- Request example

```
https://apigateway.dtdream.com/gateway/api/users?cellphoneNum=1381111*****
&departmentId=2
&userEmail=someone@example.com
&fullName=test
&loginName=test
&roleIdList=4
&telephoneNum=
```

- Response example

```
{
"result": "success",
"respCode": "200",
"data": {"userId":"2"},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.4.1.2. ModifyUser

Description

Modifies user information.

Name

ModifyUser

URL

{dtcenter_api_url}/gateway/api/users/{userId}

Request type

POST message.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
fullName	String	Yes	The displayed name of the user, which must be 2 to 30 characters in length and only contain letters
departmentId	String	Yes	The department ID, which cannot be modified currently
cellphoneNum	String	Yes	The mobile phone number of the user
telephoneNum	String	No	The landline number of the user, which is in the format such as 010-86551122 and 01086551122
userEmail	String	Yes	The email address of the user
mobileNationCode	String	No	The mobile phone area code. By default, no area code exists if not configured.

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
https://apigateway.dtdream.com/gateway/api/users/9?cellphoneNum=1381111*****
&departmentId=2
&userEmail=test1@test.com
&fullName=wqd
&telephoneNum=
```

- Response example

```
{
"result": "success",
"respCode": "200",
"data": "",
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.4.1.3. getUserList

Description

Obtains user list.

Name

getUserList

URL

`{dtcenter_api_url}/gateway/api/users`

Request type

GET message.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
loginName	String	No	The logon name of the user, which must be 3 to 30 characters in length, start with letters, and only contain letters, numbers, or underscores (_).
pageNum	Integer	No	The page number in a paged query. You must specify pageNum and pageSize at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageNum and pageSize at the same time. If not, all data is obtained. Value range: 1 to 100
isHistoryUser	Boolean	No	The history user

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
userId	String	The user ID
loginName	String	The logon name of the user
fullName	String	The displayed name of the user
departmentName	String	The department name
departmentId	String	The department ID
cellphoneNum	String	The mobile phone number of the user
telephoneNum	String	The landline number of the user

Name	Type	Description
userEmail	String	The email address of the user
loginDataTime	String	The last logon time of the user
roleNames	String	The string of role names granted to the user
activeStatus	String	Whether the user is active. “ACTIVE” indicates the user is activated. “INACTIVE” indicates the user is deactivated.
mobileNationCode	String	The country code

Examples

- Request example

```
https://apigateway.dtdream.com/gateway/api/users?isHistoryUser=false
&pageNum=1
&pageSize=10
&loginName=wqdtest
```

- Response example


```
{
    "result": "success",
    "responseCode": "200",
    "data": {
      "totalRows": 2,
      "rows": [
        {
          "userId": "2932",
          "loginName": "dachuan01",
          "fullName": "chuanx86",
          "departmentName": "DTCenterDevelopmentDepartment",
          "cellphoneNum": "1381111*****",
          "telephoneNum": "1381111*****",
           "userEmail": "someone@example.com",
          "departmentId": "3",
          "activeStatus": "ACTIVE",
          "authorizations": [
            {
              "authId": 173,
              "serviceId": 1,
```

```
            "serviceName": "CloudPlatform",
            "loginName": "dachuan01",
            "userId": 2932,
            "roles": [
              {
                "roleId": "2",
                "roleName": "SystemAdministrator",
                "isActive": false,
                "isDefault": false,
                "level": 1
              }
            ]
          }
        ],
        "mobileNationCode": "86"
      },
      {
        "userId": "2933",
        "loginName": "dachuan03",
        "fullName": "dachuan03",
        "departmentName": "DTCenterDevelopmentDepartment",
        "cellphoneNum": "1381111****",
        "userEmail": "someone@example.com",
        "departmentId": "3",
        "activeStatus": "ACTIVE",
        "authorizations": [
          {
            "authId": 174,
            "serviceId": 1,
            "serviceName": "CloudPlatform",
            "loginName": "dachuan03",
            "userId": 2933,
            "roles": [
              {
                "roleId": "2",
                "roleName": "SystemAdministrator",
                "isActive": false,
                "isDefault": false,
                "level": 1
              }
            ]
```

```
            }
          ],
          "mobileNationCode": "86"
        }
      ]
    },
      "errorMsg": "",
      "errorDetail": ""
```

1.4.2. Role-related API

1.4.2.1. getRolePage

Description

Queries the role list based on the query conditions.

Name

getRolePage

URL

{dtcenter_api_url}/gateway/api/roles

Request type

GET message.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
roleName	String	No	The role name
pageNum	Integer	No	The current page number
pageSize	Integer	No	The number of rows on each page

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
roleId	String	The role ID

Name	Type	Description
roleName	String	The role name
privilege	String	The permissions of the role, which are separated by commas (,)
service	String	The name of the platform to which the role belongs
isActive	boolean	Whether the role is active
isDefault	boolean	Whether the role is the default role. “true” indicates the default role. “false” indicates the custom role.
userNum	Integer	The number of existing users under the role
level	Integer	The role priority. The smaller the number, the higher the priority.
serviceId	Long	The ID of the platform to which the role belongs
comment	String	The description of the role
privilegeList	List<PrivilegeEntity>	A collection of permissions. For more information about PrivilegeEntity, see PrivilegeEntity.

Examples

- Request example

```
https://apigateway.dtdream.com/gateway/api/roles?pageNum=1
&pageSize=10
&roleName=test
```

- Response example

```
{
  "result": "success",
  "respCode": "200",
  "data": {
    "totalRows": 1,
    "pageSize": 10,
    "pageNum": 1,
    "rows": [
```

```
        {
          "roleId": "7",
          "roleName": "test",
          "privilege": "UsageDeclaration,PermissionApplication,RangeOfCloudResourceManagementDe
partment,CloudResourceManagementRead",
          "service": "CloudPlatform",
          "isActive": true,
          "isDefault": true,
          "userNum": 1,
          "level": 3,
          "serviceId": 1,
          "comment": "The role has the permission to submit resource application tickets.",
          "privilegeList": [
            {
              "id": 25,
              "name": "PRIV_REPAIRE_REPORT_USE",
              "cnName": "UsageDeclaration",
              "comment": "Resource center initialization;organization initialization;system administrat
ion permissions;",
              "addTime": "Jun12,201611: 16: 28AM",
              "updateTime": "Jun22,20161: 57: 04PM"
            },
            {
              "id": 1,
              "name": "PRIV_RES_APPLICATION",
              "cnName": "PermissionApplication",
              "comment": "Resource center initialization;organization initialization;system administrat
ion permissions;",
              "addTime": "Jun12,201611: 16: 28AM",
              "updateTime": "Jun22,20161: 57: 04PM"
            },
            {
              "id": 20,
              "name": "PRIV_CLOUD_RESOURCE_RANGE_DEPT",
              "cnName": "RangeOfCloudResourceManagementDepartment",
              "comment": "Resource center initialization;organization initialization;system administrat
ion permissions;",
              "addTime": "Jun12,201611: 16: 28AM",
              "updateTime": "Jun22,20161: 57: 04PM"
            },
            {
```

```
                "id": 16,
                "name": "PRIV_CLOUD_RESOUCE_READ",
                "cnName": "CloudResourceManagementRead",
                "comment": "Resource center initialization;organization initialization;system administrat
ion permissions;",
                "addTime": "Jun12,201611: 16: 28AM",
                "updateTime": "Jun22,20161: 57: 04PM"
              }
            ]
          }
      ]
    },
    "errorMsg": "",
    "errorDetail": ""
}
```


1.4.3. Department-related APIs

1.4.3.1. addDepartment

Description

Creates a department.

- A department is the foundation for creating resources. A department is required when you create a project or a resource.
- Departments are stored as a tree structure that supports up to four levels. In other words, you can create departments of four levels at most.

Name

addDepartment

URL

`{dtcenter_api_url}/gateway/api/departments`

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
parentId	String	Yes	The parent department ID, which must be numbers and can be obtained by using the getDeptRootTree API
departmentName	String	Yes	The department name, which must be 2 to 50 characters in length and only contain letters or numbers
comment	String	No	The department description, which cannot exceed 255 characters in length

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
departmentId	String	The department ID

Examples

- Request example

```
https://apigateway.dtdream.com/gateway/api/departments?departmentName=test&parentId=1
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {"departmentId":"2"},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.4.3.2. delDepartment

Description

Deletes a department. Before deleting departments, make sure that:

- The department to be deleted cannot have sub-departments.
- The department to be deleted cannot have users.
- The department to be deleted cannot have projects.
- The department to be deleted cannot have resources.

Name

delDepartment

URL

{dtcenter_api_url}/gateway/api/departments/{departmentId}

Request type

DELETE method.

Request headers

For more information about the common headers, see Common parameters.

Request parameter

Name	Type	Required	Description
departmentId	String	Yes	The department ID, which must be numbers and can be obtained by using the getDeptRootTree API. The department ID is the departmentId value in URL.

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
https://apigateway.dtdream.com/gateway/api/departments/3
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": "",
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.4.3.3. editDepartment

Description

Modifies the department name.

Name

editDepartment

URL

{dtcenter_api_url}/gateway/api/departments/{departmentId}

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
departmentId	String	Yes	The department ID, which must be numbers and can be obtained by using the getDeptRootTree API. The department ID is the departmentId value in URL.
departmentName	String	Yes	The department name, which must be 2 to 50 characters in length and can only contain letters and numbers
comment	String	No	The department description, which cannot exceed 255 characters in length

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
https://apigateway.dtdream.com/gateway/api/departments/3?departmentName=test
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": "",
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.4.3.4. getDeptRootTree

Description

Obtains all departments and provides the department information for APIs that must specify a department. The department tree supports up to four levels of departments.

Name

getDeptRootTree

URL

`{dtcenter_api_url}/gateway/api/departments/tree`

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameter

None.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
departmentId	String	The department ID
departmentName	String	The department name
comment	String	The department description
parentId	String	The parent department ID
level	Integer	The department level
isIndependent	Boolean	Indicates whether the department resources are independent. *false* indicates that the parent department cannot perform operations on the resources of the department. *true* indicates that the parent department can perform operations on the resources of the department.
children	List<DepartmentDetail>	A collection of sub-departments. The data structure of DepartmentDetail is the same as the response parameter.

Examples

- Request example

```
https://apigateway.dtdream.com/gateway/api/departments/tree
```

- Response example


```
{
"result": "success",
"responseCode": "200",
"data": {
"departmentId": "1",
"departmentName": "root",
"comment": "The root department of the entire platform, which is unique. Both the super administrato
r and system administrator belong to this department.",
"parentId": "",
"level": 0,
"isIndependent": true,
"children": [
{
"departmentId": "3",
"departmentName": "wqd",
"comment": "",
"parentId": 1,
"level": 1,
"isIndependent": true,
"children": []
},
{
"departmentId": "4",
"departmentName": "TrustedCloud",
"comment": "",
"parentId": 1,
"level": 1,
"isIndependent": true,
"children": []
},
{
"departmentId": "2",
"departmentName": "CloudPlatformDevelopmentDepartment",
"comment": "",
"parentId": 1,
"level": 1,
"isIndependent": true,
```

```
"children": []
}
]
},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```


1.4.4. Project-related APIs

1.4.4.1. createProject

Description

Creates a project. A project is a container for storing resources. The application and creation of Elastic Compute Service (ECS) and Server Load Balancer (SLB) resources must be in a corresponding project. After being added to a project, users have the permission to perform operations on resources in the project. Deleting resources in the project does not affect users in the project, and deleting users in the project does not affect the resources in the project.

When creating a project, you must specify a department for the project.

Name

createProject

URL

`{dtcenter_api_url}/gateway/api/ProjectController/manage/CreateProject`

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
projectName	String	Yes	The project name, which must be 1 to 64 characters in length and can contain letters, numbers, and underscores (_). The name must start with a letter in uppercase or lowercase.
departmentId	String	Yes	The department ID, which must be numbers and can be obtained by using the getDeptRootTree API.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
progectId	String	The project ID

Examples

- Request example

```
https://apigateway.drdream.com/gateway/api/ProjectController/manage/CreateProject?projectName=test&departmentId=2
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {
"projectId": "2"
},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.4.4.2. deleteProject

Description

Deletes a project. A Project cannot be restored after being deleted, so proceed with caution. Before deleting projects, make sure that:

- The project to be deleted cannot have any resources. You must release the resources under the project before deleting the project.
- The project to be deleted cannot have added users. You must remove the added users from the project before deleting the project.

Name

deleteProject

URL

```
{dtcenter_api_url}/gateway/api/ProjectController/manage/DeleteProject
```

Request headers

For more information about the common headers, see Common parameters.

Request type

POST method.

Request parameters

Name	Type	Required	Description
projectId	String	Yes	The project ID, which must be numbers and can be obtained by using the getProjectList API

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
https://api.drdream.com/gateway/api/ProjectController/manage/DeleteProject?projectId=8
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": "",
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.4.4.3. getProjectList

Description

Obtains the project list and provides the project information according to the query conditions such as department name and project name. When specifying a project for the resource to be created, you can use this API to obtain the project information.

Name

getProjectList

URL

```
{dtcenter_api_url}/gateway/api/ProjectController/read/GetProjectList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
departmentId	String	No	The department ID, which must be numbers and can be obtained by using the getDeptRootTree API. You cannot filter multiple IDs at a time.
projectName	String	No	The project name, which must be 1 to 64 characters in length and can contain letters, numbers, and underscores (_). The name must start with a letter in uppercase or lowercase.
pageNum	Integer	No	The page number in a paged query. You must specify pageNum and pageSize at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageNum and pageSize at the same time. If not, all data is obtained. Value range: 1 to 100

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
projectId	String	The project ID
projectName	String	The project name
departmentName	String	The name of the department to which the project belongs
departmentId	String	The ID of the department to which the project belongs
createTime	String	The created time of the project. The format is 2016-06-15 16:08:26.
userNum	Integer	The number of users added to the project

Examples

- Request example

```
https://apigateway.drdream.com/gateway/api/ProjectController/read/GetProjectList?projectName=
&departmentId=2
```

- Response example

```
{
"result": "success",
"data": {
"totalRows": 3,
"pageSize": 10,
"pageNum": 1,
"rows": [
{
"projectId": "1",
"projectName": "TestProject",
"departmentName": "CloudPlatformDevelopmentDepartment",
"departmentId": "2",
"createTime": "2016-06-15 16:08:26",
"userNum": 1
},
{
"projectId": "2",
"projectName": "test",
"departmentName": "CloudPlatformDevelopmentDepartment",
"departmentId": "2",
"createTime": "2016-06-17 21:09:04",
"userNum": 0
}
]
},
"errorMsg": "",
"errorDetail": "",
"responseCode": "200"
}
```

1.5. ECS-related APIs

1.5.1. ECS instance-related APIs

1.5.1.1. createDtcenterEcsInstance

Description

Creates an Elastic Compute Service (ECS) instance. To create an ECS instance, you first create a task that returns the parameters for obtaining the ECS instance. Then, you can call the getEcsDetailByInstanceId API based on the returned parameters to obtain the details of the ECS instance.

- After calling this API to create an ECS instance, you can call the getEcsDetailByInstanceId API based on the following returned parameters to obtain the ECS instance status: instanceId, reservedType, taskId, batchIndex, and regionId.
- To create an ECS instance, you first create a task that returns the parameters for obtaining the ECS instance. At this time, the instanceId is a virtual ID instead of a real instance ID. Then, you can call the getEcsDetailByInstanceId API based on the returned parameters to obtain the real information of the instance. If the ECS instance is failed to be created, this API returns failure and the failure reason. Otherwise, this API returns success. You can call the getEcsDetailByInstanceId API to dynamically obtain the ECS instance status. If the ECS instance status changes to *running*, the entire creation process of the ECS instance is completed.

Name

createDtcenterEcsInstance

URL

```
{dtcenter_api_url}/gateway/api/cloudEcs/manage/createDtcenterEcsInstance
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API.
zoneId	String	Yes	The zone ID, which can be obtained by using the getZoneList API.
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API.
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API.

Name	Type	Required	Description
cpu	String	Yes	The number of CPU cores. This parameter is required in V2.1.2 or earlier versions, and not required for later versions.
memory	String	Yes	The memory size. This parameter is required in V2.1.2 or earlier versions, and not required for later versions.
imageId	String	Yes	The image ID, which can be obtained by using the getImageList API.
instanceName	String	No	The instance name, which must be 2 to 114 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). The name must start with a letter in uppercase or lowercase.
diskTypeList	List<String>	No	A list of data disk types. Values: • cloud: basic cloud disk • cloud_ssd: SSD cloud disk • cloud_efficiency: ultra cloud disk
diskSizeList	List<String>	No	A list of data disk sizes. Values: You can obtain the mapping between the type and size of data disks by using the getZoneList API.
diskDeviceList	List<String>	No	A list of data disk mount points. Value range: */dev/xvdb* to */dev/xvdz*
releaseWithEcs	List<String>	No	Configures whether data disks are released together with the instance. Values: • *true*: Disks are deleted after the ECS instance is deleted. • *false*: Disks are not deleted after the ECS instance is deleted.
networkType	String	Yes	The network type. Values: • *classic*: classic network • *vpc*: Virtual Private Cloud

Name	Type	Required	Description
vpcId	String	Yes	The VPC ID, which can be obtained by using the getVpcs API. If the network type is VPC, this parameter is required. If the network type is classic network, this parameter is not required.
vSwitchId	List<String>	Yes	The VSwitch ID, which can be obtained by using the getVswitchList API. If the network type is VPC, this parameter is required. If the network type is classic network, this parameter is not required.
createEcsNum	String	Yes	The number of ECS instances to be created. Value range: 1 to 50
systemDiskType	String	Yes	The system disk type. Values: • *cloud*: basic cloud disk • *cloud_ssd*: SSD cloud disk • *cloud_efficiency*: ultra cloud disk
securityGroupId	String	Yes	The security group ID, which can be obtained by using the getSecurityGroupList API.
password	String	No	The instance password, which must be 8 to 30 characters in length, contain letters in uppercase and lowercase, and numbers at the same time, and cannot contain special characters.
instanceType	String	Yes	The instance type. This parameter is not required in V2.1.2 or earlier versions but required for later versions.
ioOptimized	String	No	Whether I/O is optimized. You can obtain this value by querying the zone configurations. • *none*: I/O is not optimized. • *optimized*: I/O is optimized.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
successNum	String	The number of ECS instances created by the task.
regionId	String	The region ID.
taskId	String	The task ID.

Name	Type	Description
ecsList	List<ecsInfo>	Creates ECS information in batches and see the detailed parameters in the following table.

ecsInfo

Name	Type	Description
instanceId	String	The instance ID. This is a virtual ID and is deleted after the ECS instance is created.
batchIndex	String	The sequence number of the ECS instance in the task.
reservedType	String	Indicates that the ECS instance creation task is in progress.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudEcs/manage/createDtcenterEcsInstance?
bandwidth=1
&cpu=1
&createEcsNum=1
&departmentId=510
&diskDeviceList=%2Fdev%2Fxvdb
&diskSizeList=20
&diskTypeList=cloud_ssd
&imageId=aliyun1501_32_40G_aliaegis_20160222.vhd
&instanceName=test888
&memory=1
&networkType=vpc
&password=<yourPassword>
&projectId=58
&regionId=cn-hangzhou-am24
&releaseWithEcs=true
&securityGroupId=sg-886mpzp78
&systemDiskType=cloud_ssd
&vSwitchId=vsw-8877j****
&vpcId=vpc-88bp0****
&zoneId=cn-hangzhou-hsd-am24001-a
```

- Response example

```
{
"responseCode": "200",
"result": "success",
"data": {
"taskId": "e1349a6c-5d56-4729-8174-b97c37fac719",
"ecsList": [{
"instanceId": "c3efae0e-3bf2-4d5b-b973-163b13f2****",
"reservedType": "taskCreating",
"batchIndex": 0
}],
"successNum": 1,
"regionId": "cn-qingdao-sg-d01"
}
```


1.5.1.2. deleteEcsInstance

Description

Deletes a specified Elastic Compute Service (ECS) instance.

- After the ECS instance is deleted, disks that are mounted to the instance and are configured releaseWithEcs to *true* are deleted.
- After the ECS instance is deleted, all relevant data is lost and cannot be restored.

Name

deleteEcsInstance

URL

```
{dtcenter_api_url}/gateway/api/cloudEcs/manage/DeleteEcsInstance
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID
instanceId	String	Yes	The instance ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudEcs/manage/DeleteEcsInstance?instanceId=i-880r6****&regionId=cn-hangzhou-am24
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {
"requestId": "67D20225-9E75-4820-92B8-652EEB48F643"
},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.1.3. resetInstancePassword

Description

Modifies the logon password of a specified Elastic Compute Service (ECS) instance. After modifying the password, you must restart the instance for the new password to take effect.

This API is exclusive to Apsara Stack regions.

Name

resetInstancePassword

URL

```
{dtcenter_api_url}/gateway/api/cloudEcs/use/ResetInstancePwd
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
newPassword	String	Yes	The new password of the instance, which must be 8 to 30 characters in length and contain uppercase letters, lowercase letters, and numbers at the same time.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudEcs/use/ResetInstancePwd?instanceId=i-88ieq****
&newPassword=yourPassword&regionId=cn-hangzhou-am24
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {
"requestId": "09F5A6B7-E90A-48BD-A7F4-7FE76D97545A"
},
"errorMsg": "",
"errorDetail": ""
}
```

1.5.1.4. getCloudEcsList

Description

Queries a list of Elastic Compute Service (ECS) instances that meet the conditions. You can filter the ECS instances by regionId, instanceId, instanceName, ipAddress, instanceStatus, departmentId, vpcId, projectName, projectId, securityGroupId, cpu, memory, and imageId.

Name

getCloudEcsList

URL

```
{dtcenter_api_url}/gateway/api/cloudEcs/read/getCloudEcsList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	No	The region ID, which can be obtained by using the getRegionList API
instanceId	String	No	The instance ID
instanceName	String	No	The instance name
ipAddress	String	No	The IP address
instanceStatus	String	No	The instance status that can be queried Values: • *running*: running • *stopped*: stopped • *error*: error
departmentId	String	No	The department ID, which can be obtained by using the getDeptRootTree API
vpcId	String	No	The Virtual Private Cloud (VPC) ID
projectId	String	No	The project ID
projectName	String	No	The project name
securityGroupId	String	No	The security group ID

Name	Type	Required	Description
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100
cpu	String	No	The number of CPU cores
memory	String	No	The memory size
imageId	String	No	The image ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
instanceId	String	The instance ID
instanceName	String	The instance name
physicalHostName	String	The hostname of the virtual machine
vpcId	String	The VPC ID

Name	Type	Description
instanceStatus	String	The instance status Values: • *resizing*: adjusting • *running*: running • *stopped*: stopped • *stopping*: stopping • *suspended*: suspended • *starting*: starting • *building*: creating • *resetting*: initializing the operating system • *deleted*: deleted • *paused*: paused • *rebooting*: restarting • *hardRebooting*: hard rerestarting • *shelved*: shelved • *error*: error • *scheduling*: scheduling • *blockMapping*: mapping • *networking*: connecting the network • *spawning*: spawning • *taskProcessing*: A task is being created. • *taskDeleting*: A task is being deleted.
networkType	String	The network type Values: • vpc: Virtual Private Cloud • classic: classic network
innerIpAddress	String	The internal IP address of the instance
publicIp	String	The public IP address of the instance
natIpAddress	String	The Elastic IP Address (EIP) mapped to the ECS private NIC
eipAddress	String	The EIP
departmentName	String	The department name
description	String	The description
departmentId	String	The department ID
imageId	String	The image ID

Name	Type	Description
projectName	String	The project name
projectId	String	The project ID
privateIpAddress	String	The private IP address of the instance
regionType	String	The region type Value: *regft* (Apsara Stack regions)
regionName	String	The region name
zoneId	String	The zone ID
aliType	String	The Alibaba region type Value: *private* (Apsara Stack regions)
regionId	String	The region ID
config	String	Number of CPU cores/memory size/data disk size
GPUAmount	Integer	The GPU numbers of instance specifications
GPUSpec	String	The GPU type of instance specifications
createTime	String	The creation time of the instance. For example: "2019-07-2914:42:00"
CreationTimeStamp	Long	The timestamp when the instance is created. For example: 1564382520000
gpuType	String	The GPU type of the instance
serialNumber	String	The serial number of the instance
cpu	Long	The CPU core numbers
memory	Float	The memory size

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudEcs/read/getCloudEcsList/?
regionId=
&instanceId=
&instanceName=
&ipAddress=
&instanceStatus=
&departmentId=
&vpcId=
&pageNum=1
&pageSize=10
&projectName=
&projectId=
&securityGroupId=
&cpu=
&memory=
&imageId=
```

- Response example

```
{
  "errorMsg":"",
  "errorDetail":"",
  "result":"success",
  "requestId":null,
  "data":{
    "totalRows":7,
    "pageSize":10,
    "rows":[
      {
        "instanceId":"i-1ny05x1f7j2likel****",
        "instanceName":"iZ1ny05x1f7j2likelc****",
        "physicalHostName":"iZ1ny05x1f7j2likelc8zrZ",
        "osName":"CentOS  6.8 32Bit",
        "reservedType":"",
        "vpcId":"vpc-1ny6vayhz9m04j3hs****",
        "vSwitchId":"vsw-1nyg187bxg4w9bh14****",
        "instanceStatus":"running",
        "statusFlag":"stable",
        "networkType":"vpc",
        "innerIpAddress":"",
        "publicIp":"",
        "natIpAddress":"56.16.XX.XX",
```

```
            "eipAddress":"",
            "departmentName":"test0723",
            "description":"",
            "departmentId":"3",
            "systemDiskSize":"",
            "imageId":"centos_6_08_32_40G_alibase_20170710.raw",
            "expireDate":"",
            "createTime":"2019-07-29 14:42:00",
            "creationTimeStamp":1564382520000,
            "regionSnapSupport":true,
            "projectName":"testyundun",
            "projectId":"5000",
            "privateIpAddress":[
               "172.16.XX.XX"
            ],
            "regionType":"regft",
            "zoneId":"cn-qingdao-apsara-amtest18001-a",
            "regionName":"cn-qingdao-apsara-d02",
            "aliType":"private",
            "regionId":"cn-qingdao-apsara-d02",
            "securityGroupIdList":"[sg-1ny05rohy9qfc5l2x37o]",
            "cpu":1,
            "memory":2,
            "GPUAmount":0,
            "GPUSpec":"",
            "diskSize":43,
            "instanceType":"ecs.n4.small",
            "ioOptimized":"true",
            "config":"1/2.0/43",
            "userId":13,
            "userName":"123",
            "autoRenew":false,
            "serialNumber":"385ef6f7-4691-4140-b96b-c430006e0f45",
            "clusterId":"",
            "faultMessage":null,
            "gpuType":"",
            "vmwareTools":null,
            "isoId":null
         }
      ],
      "pageNum":1
   }
```

```
    },
    "return_subCode":null,
    "return_subMsg":null,
    "responseCode":"200"
}
```

1.5.1.5. getEcsDetailByInstanceId

Description

Queries the details of a specified Elastic Compute Service (ECS) instance.

Name

getEcsDetailByInstanceId

URL

```
{dtcenter_api_url}/gateway/api/cloudEcs/read/getEcsDetailByInstanceId
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
reservedType	String	No	The task status Value: *taskCreating* (The task is being created.)
taskId	String	No	The task ID
batchIndex	String	No	The sequence number of the ECS instance in the task

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
vpcName	String	The Virtual Private Cloud (VPC) name

Name	Type	Description
memory	String	The memory size
instanceName	String	The instance name
regionName	String	The region name
departmentId	String	The department ID
description	String	The description
securityGroupId	String	The security group ID
diskSize	String	The data disk size
instanceId	String	The instance ID
vSwitchId	String	The VSwitch ID
regionType	String	The region type Value: *regft* (Apsara Stack regions)
eipAddress	String	The Elastic IP Address (EIP)
vpcId	String	The VPC ID
physicalHostName	String	The hostname of the virtual machine
zoneId	String	The zone ID
zoneName	String	The zone name
networkType	String	The network type Values: • *vpc*: Virtual Private Cloud • *classic*: classic network
departmentName	String	The department name
imageId	String	The image ID
imageName	String	The image name
cpu	String	The number of CPU cores
osName	String	The name of the operating system

Name	Type	Description
instanceStatus	String	The instance status Values: • *resizing*: adjusting • *running*: running • *stopped*: stopped • *stopping*: stopping • *suspended*: suspended • *starting*: starting • *building*: creating • *resetting*: initializing operating system • *deleted*: deleted • *paused*: paused • *rebooting*: restarting • *hardRebooting*: hard rerestarting • *shelved*: shelved • *error*: error • *scheduling*: scheduling • *blockMapping*: mapping • *networking*: connecting the network • *spawning*: spawning • *taskProcessing*: A task is being created. • *taskDeleting*: A task is being deleted.
privateIpAddress	String	The private IP address of the instance
instanceType	String	The instance type
ioOptimized	String	Whether I/O is optimized Values: • *true*: I/O is optimized. • *false*: I/O is not optimized.
regionId	String	The region ID
natIpAddress	String	EIP mapped to the ECS intranet NIC
innerIpAddress	String	Internal IP address of the instance
projectName	String	The project name
ProjectId	String	The project ID of the instance
config	String	The number of CPU cores/memory size/data disk size

Name	Type	Description
deploymentSetId	String	The deployment set ID
publicIp	String	The public IP address of the instance
gpuType	String	The GPU type of the instance
createTime	String	The creation time of the instance. For example, 2019-07-2914:42:00
creationTimeStamp	Long	The timestamp when the instance is created. For example, 1564382520000
statusFlag	String	Whether the current instance is in stable status
bandwidth	Integer	The maximum outbound bandwidth of the public network
GPUSpec	String	The GPU type of instance specifications
GPUAmount	Integer	The GPU numbers of instance specifications

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudEcs/read/getEcsDetailByInstanceId?
instanceId=i-888jg****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
  "errorMsg":"",
  "errorDetail":"",
  "result":"success",
  "requestId":null,
  "data":{
    "physicalHostName":"iZ1ny05x1f7j2likelc8zrZ",
    "networkType":"vpc",
    "natIpAddress":"56.16.XX.XX",
    "eipAddress":"",
    "description":"",
    "vpcId":"vpc-1ny6vayhz9m04j3hs****",
    "config":"1/2.0/43",
    "reservedType":"",
    "deploymentSetId":"",
    "regionId":"cn-qingdao-apsara-d02",
```

```
"isoId":null,
"imageName":"centos_6_08_32_40G_alibase_20170710.raw",
"vSwitchId":"vsw-1nyg187bxg4w9bh14****",
"instanceChargeType":"PostPaid",
"cpu":1,
"regionName":"cn-qingdao-apsara-d02",
"eipBandwidth":"",
"securityGroupId":[
   "sg-1ny05rohy9qfc5l2****"
],
"period":"",
"publicIp":"",
"regionType":"regft",
"zoneName":"a",
"instanceType":"ecs.n4.small",
"vpcName":"bbbbbbb",
"gpuType":"",
"expireDate":"",
"expiredTime":"",
"ioOptimized":"true",
"projectName":"testyundun",
"osName":"CentOS 6.8 32Bit",
"createTime":"2019-07-29 14:42:00",
"projectCode":"",
"regionSnapSupport":true,
"statusFlag":"stable",
"instanceStatus":"running",
"imageVersion":"",
"projectId":"5000",
"privateIpAddress":[
   "172.16.XX.XX"
],
"bandwidth":0,
"imageId":"centos_6_08_32_40G_alibase_20170710.raw",
"systemDiskSize":"",
"privateNetwork":[

],
"innerIpAddress":"",
"instanceId":"i-1ny05x1f7j2likel****",
"departmentName":"test0723",
```

```
        "creationTimeStamp":1564382520000,
        "memory":2,
        "zoneId":"cn-qingdao-apsara-amtest18001-a",
        "instanceName":"iZ1ny05x1f7j2likelc****",
        "systemDiskType":"",
        "GPUSpec":"",
        "departmentId":"3",
        "GPUAmount":0,
        "clusterId":null,
        "diskSize":"43"
    },
    "return_subCode":"",
    "return_subMsg":"",
    "responseCode":"200"
}
```


1.5.1.6. startEcsInstance

Description

Starts a specified Elastic Compute Service (ECS) instance.

- You can only start an instance when it is in *stopped* status.
- After this API is called, the instance enters the *starting* status first. The instance status changes to *running* after the instance is started.

Name

startEcsInstance

URL

```
{dtcenter_api_url}/gateway/api/cloudEcs/use/StartEcsInstance
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudEcs/use/StartEcsInstance?
instanceId=i-880r6****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.1.7. rebootEcsInstance

Description

Restarts a specified Elastic Compute Service (ECS) instance.

- You can only restart an instance when it is in *running* status.
- After this API is called, the instance enters the *starting* status first. The instance status changes to *running* after the instance is restarted.

Name

rebootEcsInstance

URL

{dtcenter_api_url}/gateway/api/cloudEcs/use/RebootEcsInstance

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
rebootModel	boolean	Yes	The restarting method Values: • *true*: force to restart, which causes the loss of unsaved data on the ECS instance • *false*: restart

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudEcs/use/RebootEcsInstance?
instanceId=i-880r6****
&rebootModel=false
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "errorMsg":"",
   "errorDetail":"",
   "result":"success",
   "requestId":null,
   "data":{
      "requestId":"EC591E9D-8187-47A1-9941-A6A29A17DA38"
   },
   "return_subCode":"",
   "return_subMsg":"",
   "responseCode":"200"
}
```


1.5.1.8. stopEcsInstance

Description

Stops a specified Elastic Compute Service (ECS) instance.

- You can only stop an instance when it is in *running* status.
- After this API is called, the instance enters the *stopping* status first. The instance status changes to *stopped* after the instance is stopped.

Name

stopEcsInstance

URL

```
{dtcenter_api_url}/gateway/api/cloudEcs/use/StopEcsInstance
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudEcs/use/StopEcsInstance?
instanceId=i-880r6****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
"errorMsg":"",
"errorDetail":"",
"result":"success",
"requestId":null,
"data":{
"requestId":"F6B42C27-79F4-411D-BEEF-49EF5553D116"
},
"return_subCode":"",
"return_subMsg":"",
"responseCode":"200"
}
```

1.5.2. Security group-related APIs

1.5.2.1. createSecGroup

Description

Creates a security group. You can configure the firewall for a group of instances by adding the instances to a security group and configuring the security group firewall rules. A security group can contain multiple instances.

- By default, a newly created security group only allows access between instances within the security group and denies all other access. To allow the access from instances in other security groups or from the Internet, users can modify the firewall policy of the security group by authorizing the security group permission APIs.
- The firewall rules differentiate between the intranet and the Internet.
- Each user can create up to 100 security groups.
- To create a Virtual Private Cloud (VPC) security group, you must specify the VPC ID.

Name

createSecGroup

URL

```
{dtcenter_api_url}/gateway/api/secgroups/manage/createSG
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
vpcId	String	No	The VPC ID, which can be obtained by using the getVpcs API. To create a VPC security group, this parameter is required.
securityGroupName	String	Yes	The security group name, which must be 2 to 128 characters in length and can contain numbers, letters, periods (.), underscores (_), and hyphens (-). The name must start with a letter in uppercase or lowercase, but must not start with `http://` and `https://`.
description	String	No	The description of the security group, which must be 2 to 256 characters in length and must not start with `http://` and `https://`
departmentId	String	Yes	The department ID, which must be numbers and can be obtained by using the getDeptRootTree API
ProjectId	String	No	The project ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
securityGroupId	String	The security group ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/manage/createSG?
departmentId=12
&description=
&regionId=cn-hangzhou-am24
&securityGroupName=test
&vpcId=
```

- Response example

```
{
   "result": "success",
   "data": {
      "securityGroupId": "sg-88y1rsgp9"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.2.2. createSecGroupRule

Description

Creates an access rule of resources in a security group.

- Set the access permission of the security group direction.
- Supported authorization policies: *accept* (allow access) and *drop* (deny access)
- Different network types are supported. For example, you can set networkType to *internet* or *intranet*, which indicates the pubilc network and internal network respectively. Elastic Compute Service (ECS) instances of Virtual Private Cloud (VPC) only support the intranet type.
- Each security group can have up to 100 authorization rules.
- The priorities of security groups are in descending order based on the created time.
- The rule priority ranges from 1 to 100. The default value is 1, that is, the highest priority. The bigger the number, the lower the priority.
- For authorization rules with the same priority, *drop* rules take precedence.
- Authorization between security groups is only allowed in the intranet, that is, you must set networkType to *intranet*.

The following two authorization methods are supported:

- Allow other security groups within the same region (for classic network) or the same VPC (for VPC) to access the security group. Authorization across users is supported.

- Allow an IP address range (in the Classless Inter-Domain Routing (CIDR) format) to access the security group.

Name

createSecGroupRule

URL

```
{dtcenter_api_url}/gateway/api/secgroups/manage/{securityGroupId}/rules
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
securityGroupId	String	Yes	The security group ID
ipProtocol	String	Yes	IP protocols: • *tcp*: Transmission Control Protocol (TCP) • *udp*: User Datagram Protocol (UDP) • *icmp*: Internet Control Message Protocol (ICMP) • *gre*: Generic Routing Encapsulation (GRE) • *all*: All of the preceding four protocols are supported.
portRange	String	Yes	The range of ports related to the IP protocols: • If ipProtocol is set to *tcp* or *udp*, the default port number is displayed. The port number ranges from 1 to 65535. For example, 1/200 indicates the port number ranges from 1 to 200. If the value 200/1 is entered, an error is returned when the API is called. • If ipProtocol is set to *icmp*, the port range is -1/-1. • If ipProtocol is set to *gre*, the port range is -1/-1. • If ipProtocol is set to *all*, the port range is -1/-1.
sourceType	String	Yes	The authorization type: • *srcip*: IP address range access • *srcsecgroup*: security group access

Name	Type	Required	Description
sourceObject	String	Yes	The authorization object. Values: • If sourceType is *srcip*, enter an IP address as the authorization object. The default value is 0.0.0.0/0 (indicating no restrictions on access). Other supported formats include 10.159.6.18/12 or 10.159.6.186. Only IPv4 is supported. • If sourceType is *srcsecgroup*, the authorization object is the security group ID in the same region.
policy	String	No	The authorization policy. Values (*accept* by default): • *accept*: Access is allowed. • *drop*: Access is denied.
direction	String	Yes	The rule direction: • *egress*: outbound • *ingress*: inbound
networkType	String	No	The network type. Values (*internet* by default): • *internet* • *intranet*: If the region type is Apsara Stack or the authorization type is security group access, you must set networkType to *intranet*.
priority	String	No	The priority of the authorization policy, which cannot be configured currently. The default value is 1, that is, the highest priority. Value range: 1 to 100
description	String	No	The description

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/manage/sg-88dlq8rrz/rules?
direction=ingress
&ipProtocol=udp
&networkType=intranet
&policy=drop
&portRange=1%2F65535
&priority=1
&regionId=cn-hangzhou-am24
&sourceObject=0.0.0.0%2F0
&sourceType=srcip
```

- Response example

```
{
   "result": "success",
   "data": {
      "requestId":"CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.2.3. deleteSecGroup

Description

Deletes a specified security group.

You can only delete security groups that do not contain instances or are not referenced by security rules of other security groups.

Name

deleteSecGroup

URL

```
{dtcenter_api_url}/gateway/api/secgroups/manage/{securityGroupId}
```

Request type

DELETE method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
securityGroupId	String	Yes	The security group ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
reguestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/manage/sg-88yke5qnp?
regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result":"succcess",
   "responseCode":"",
   "data":{},
   "errorMsg":"",
   "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.2.4. delSecGroupRule

Description

Deletes an access rule of a security group.

Name

delSecGroupRule

URL

```
{dtcenter_api_url}/gateway/api/secgroups/manage/{securityGroupId}/delrules
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
securityGroupId	String	Yes	The security group ID
ipProtocol	String	No	IP protocols: • *tcp*: Transmission Control Protocol (TCP) • *udp*: User Datagram Protocol (UDP) • *icmp*: Internet Control Message Protocol (ICMP) • *gre*: Generic Routing Encapsulation (GRE) • *all*: All the preceding four protocols are supported.
portRange	String	No	The range of ports related to the IP protocols: • If ipProtocol is set to *tcp* or *udp*, the default port number is displayed. The port number ranges from 1 to 65535. For example, 1/200 indicates the port number ranges from 1 to 200. If the value 200/1 is entered, an error is returned when the API is called. • If ipProtocol is set to *icmp*, the port range is -1/-1. • If ipProtocol is set to *gre*, the port range is -1/-1. • If ipProtocol is set to *all*, the port range is -1/-1.
sourceType	String	No	The authorization type: • *srcip*: IP address range access • *srcsecgroup*: security group access

Name	Type	Required	Description
sourceObject	String	No	The authorization object Values: • If sourceType is set to *srcip*, enter an IP address as the authorization object. The default value is 0.0.0.0/0 (indicating no restrictions on access). Other supported formats include 10.159.6.18/12 or 10.159.6.186. Only IPv4 is supported. • If sourceType is set to *srcsecgroup*, the authorization object is the security group ID in the same region.
networkType	String	No	The network type Values: • *internet* • *intranet*
policy	String	No	The authorization policy Values: • *accept*: Access is allowed. • *drop*: Access is denied.
direction	String	No	The rule direction: • *egress*: outbound • *ingress*: inbound
priority	String	No	The priority of the authorization policy

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/manage/e731548a-a2ed-4dc1-ab48-b1c7c99
a6198/delrules?
direction=egress
&ipProtocol=%E5%85%A8%E9%83%A8&portRange=-1%2F-1
&regionId=97d83522-0d78-4e95-a8b5-361eaa580504
&securityGroupRuleId=faf9ed09-9771-463e-8ff5-6cacc4343d54
&sourceObject=0.0.0.0%2F0
&sourceType=srcip
```

- Response example

```
{
   "result": "success",
   "data": {},
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.2.5. modifySecGroup

Description

Modifies the attributes of a specified security group, including the security group name and description.

Name

modifySecGroup

URL

```
{dtcenter_api_url}/gateway/api/secgroups/manage/{securityGroupId}
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
securityGroupId	String	Yes	The security group ID to be modified
securityGroupName	String	Yes	The security group name, which must be 2 to 128 characters in length and can contain numbers, letters, periods (.), underscores (_), and hyphens (-). The name must start with a letter in uppercase or lowercase. This parameter is required.
description	String	Yes	The description of the security group, which must be 2 to 256 characters in length and must not start with `http://` or `https://`

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/manage/sg-889gj3idu?
description=qqq
&regionId=cn-hangzhou-am24
&securityGroupName=portal-pri
```

- Response example

```
{
   "result": "success",
   "data": {},
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.2.6. getSecurityGroupList

Description

Queries the basic information of all user-defined security groups. The query results appear on pages and each page has 10 query results by default. You can filter security groups by region, department, security group name, security group ID, and Virtual Private Cloud (VPC) ID.

Name

getSecurityGroupList

URL

```
{dtcenter_api_url}/gateway/api/secgroups/read/getSecurityGroupList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	No	The region ID, which can be obtained by using the getRegionList API
vpcId	String	No	The ID of VPC to which the security group belongs
securityGroupName	String	No	The security group name, which must be 2 to 128 characters in length and can contain numbers, letters, periods (.), underscores (_), and hyphens (-). The name must start with a letter in uppercase or lowercase.
securityGroupId	String	No	The security group ID
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100
departmentId	String	No	The department ID, which must be numbers and can be obtained by using the getDeptRootTree API
networkType	String	No	The network type: • *classic*: classic network • *vpc*: Virtual Private Cloud

Name	Type	Required	Description
isSync	Boolean	No	Whether synchronized
projectName	String	No	The name of the project where the security group resides

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
securityGroupName	String	The security group name
securityGroupId	String	The security group ID
regionId	String	The region ID
vpcId	String	The VPC ID
networkType	String	The network type: • *classic*: classic network • *vpc*: Virtual Private Cloud
createTime	String	The created time of the security group
creationTimeStamp	Long	The timestamp when the security group is created
description	String	The description of the security group
departmentId	String	The department ID
departmentName	String	The department name
projectId	String	The ID of the project where the security group resides
projectName	String	The name of the project where the security group resides

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/read/getSecurityGroupList?
departmentId=2
&pageNum=1
&pageSize=10
&regionId=cn-hangzhou-am24

&securityGroupId=
&securityGroupName=
&vpcId=
&projectName=
```

- Response example


```
{
  "errorMsg":"",
  "errorDetail":"",
  "result":"success",
  "requestId":null,
  "data":{
    "totalRows":4,
    "pageSize":10,
    "rows":[
      {
        "securityGroupName":"wlqdesec",
        "securityGroupId":"sg-1ny05okw5h0eybel6tj8",
        "instanceNum":0,
        "regionId":"cn-qingdao-apsara-d02",
        "vpcId":"vpc-1ny6vayhz9m04j3hs****",
        "vpcName":"bbbbbbb",
        "networkType":"vpc",
        "createTime":"2019-07-29 17:07:59",
        "description":"TestUse",
        "departmentId":3,
        "departmentName":"test0723",
        "securityGroupType":"others",
        "projectId":"5000",
        "creationTimeStamp":1564391279000,
        "projectName":"testyundun"
      },
      {
        "securityGroupName":"hhhhhhhhhhhhhhhh",
        "securityGroupId":"sg-1ny05roi2lefhluhl9jq",
```

```
        "instanceNum":0,
        "regionId":"cn-qingdao-apsara-d02",
        "vpcId":"vpc-1ny6vayhz9m04j3hs****",
        "vpcName":"bbbbbbb",
        "networkType":"vpc",
        "createTime":"2019-07-24 19:56:43",
        "description":"",
        "departmentId":3,
        "departmentName":"test0723",
        "securityGroupType":"others",
        "projectId":"",
        "creationTimeStamp":1563969403000,
        "projectName":""
    },
    {
        "securityGroupName":"yunduntest222",
        "securityGroupId":"sg-1ny05rohy9qfc5l2x37o",
        "instanceNum":3,
        "regionId":"cn-qingdao-apsara-d02",
        "vpcId":"vpc-1ny6vayhz9m04j3hs****",
        "vpcName":"bbbbbbb",
        "networkType":"vpc",
        "createTime":"2019-07-24 19:35:20",
        "description":"",
        "departmentId":3,
        "departmentName":"test0723",
        "securityGroupType":"others",
        "projectId":"5000",
        "creationTimeStamp":1563968120000,
        "projectName":"testyundun"
    },
    {
        "securityGroupName":"sdfsdfsd",
        "securityGroupId":"sg-um305roi2lefha0awxox",
        "instanceNum":3,
        "regionId":"cn-qingdao-apsara-d01",
        "vpcId":"vpc-um3ewtrvcfmgg659a****",
        "vpcName":"fffffffff",
        "networkType":"vpc",
        "createTime":"2019-07-24 19:33:10",
        "description":"",
```

```
            "departmentId":3,
            "departmentName":"test0723",
            "securityGroupType":"others",
            "projectId":"5000",
            "creationTimeStamp":1563967990000,
            "projectName":"testyundun"
          }
        ],
        "pageNum":1
    },
    "return_subCode":null,
    "return_subMsg":null,
    "responseCode":"200"
}
```


1.5.2.7. getRuleList

Description

Queries the security group rule list of a specified security group.

Name

getRuleList

URL

```
{dtcenter_api_url}/gateway/api/secgroups/read/{securityGroupId}/rules
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
securityGroupId	String	Yes	The security group ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
securityGroupId	String	The security group ID
policy	String	The authorization policy. Values: • *accept*: Access is allowed. • *drop* : Access is denied.
networkType	String	The network type. Values: • *internet* • *intranet*
ipProtocol	String	IP protocols: • *tcp*: Transmission Control Protocol (TCP) • *udp*: User Datagram Protocol (UDP) • *icmp*: Internet Control Message Protocol (ICMP) • *gre*: Generic Routing Encapsulation (GRE) • *all*: All of the preceding four protocols are supported.
portRange	String	The range of ports related to the IP protocols: • If ipProtocol is set to *tcp* or *udp*, the default port number is displayed. The port number ranges from 1 to 65535. For example, 1/200 indicates the port number ranges from 1 to 200. If the value 200/1 is entered, an error is returned when the API is called. • If ipProtocol is set to *icmp*, the port range is -1/-1. • If ipProtocol is set to *gre*, the port range is -1/-1. • If ipProtocol is set to *all*, the port range is -1/-1.
sourceType	String	The authorization type. Values: • *srcip*: IP address range access • *srcsecgroup*: security group access
sourceObject	String	The authorization object
priority	String	The priority of the authorization policy, which cannot be configured currently. Value ranges from 1 to 100. The default value is 1, that is, the highest priority.
direction	String	The rule direction. Values: • *egress*: outbound • *ingress*: inbound
description	String	The description

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/read/sg-25ze62245/rules?

regionId=cn-beijing
```

- Response example


```
{
  "errorMsg":"",
  "errorDetail":"",
  "result":"success",
  "requestId":null,
  "data":{
    "totalRows":1,
    "rows":[
      {
        "securityGroupId":"sg-1ny05okw5h0eybel6tj8",
        "policy":"accept",
        "networkType":"intranet",
        "ipProtocol":"all",
        "portRange":"-1/-1",
        "sourceType":"srcip",
        "sourceObject":"0.0.0.0/0",
        "priority":"1",
        "direction":"ingress",
        "securityGroupRuleId":"",
        "description":"TestUse"
      }
    ]
  },
  "return_subCode":null,
  "return_subMsg":null,
  "responseCode":"200"
}
```


1.5.2.8. getSecurityGroupRulesOfEcs

Description

Queries rules of all security groups of a specified Elastic Compute Service (ECS) instance.

Name

getSecurityGroupRulesOfEcs

URL

```
{dtcenter_api_url}/gateway/api/secgroups/read/getSecurityGroupRulesOfEcs
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The ECS instance ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
securityGroupId	String	The security group ID
policy	String	The authorization policy: • *accept*: Access is allowed. • *drop*: Access is denied.
networkType	String	The network type: • *internet* • *intranet*
ipProtocol	String	IP protocols: • *tcp*: Transmission Control Protocol (TCP) • *udp*: User Datagram Protocol (UDP) • *icmp*: Internet Control Message Protocol (ICMP) • *gre*: Generic Routing Encapsulation (GRE) • *all*: All the preceding four protocols are supported.

Name	Type	Description
portRange	String	The range of ports related to the IP protocols: • If ipProtocol is set to *tcp* or *udp*, the default port number is displayed. The port number ranges from 1 to 65535. For example, 1/200 indicates the port number ranges from 1 to 200. If the value 200/1 is entered, an error is returned when the API is called. • If ipProtocol is set to *icmp*, the port range is -1/-1. • If ipProtocol is set to *gre*, the port range is -1/-1. • If ipProtocol is set to *all*, the port range is -1/-1.
sourceType	String	The authorization type: • *srcip*: IP address range access • *srcsecgroup*: security group access
sourceObject	String	The authorization object
priority	String	The priority of the authorization policy, which cannot be configured currently. The default value is 1, that is, the highest priority. Value range: 1 to 100
direction	String	The rule direction: • *egress*: outbound • *ingress*: inbound
securityGroupRuleId	String	The security group rule ID
description	String	The description

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/read/getSecurityGroupRulesOfEcs?
instanceId=i-88wv6****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": {
    "totalRows": 1,
    "rows": [
      {
        "securityGroupId": "sg-88hlwxj50",
        "policy": "accept",
        "networkType": "intranet",
        "ipProtocol": "all",
        "portRange": "-1/-1",
        "sourceType": "srcip",
        "sourceObject": "0.0.0.0/0",
        "priority": "1",
        "direction": "ingress",
        "securityGroupRuleId": "",
        "description": ""
      }
    ]
  },
  "errorMsg": "",
  "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```


1.5.2.9. getSecurityGroupList

Description

Queries security groups of a specified Elastic Compute Service (ECS) instance.

Name

getSecurityGroupList

URL

```
{dtcenter_api_url}/gateway/api/secgroups/read/securitygroupbyecsinstance
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The ECS instance ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
regionId	String	The region ID
networkType	String	The network type: • *classic*: classic network • *vpc*: Virtual Private Cloud
securityGroupName	String	The security group name
vpcName	String	The Virtual Private Cloud (VPC) name
securityGroupId	String	The security group ID
vpcId	String	The VPC ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/read/securitygroupbyecsinstance?
instanceId=i-88lcd****
&regionId=cn-hangzhou-am24 http://api.dtdream.com/gateway/api
```

- Response example

```
{
  "result": "success",
  "data": {
    "totalRows": 2,
    "rows": [
      {
        "regionId": "cn-hangzhou-am24",
        "networkType": "vpc",
        "securityGroupName": "aaaaaa",
        "vpcName": "test1",
        "securityGroupId": "sg-88yke5qnp",
        "vpcId": "vpc-88hs1****"
      },
      {
        "regionId": "cn-hangzhou-am24",
        "networkType": "vpc",
        "securityGroupName": "aaaaaa",
        "vpcName": "test",
        "securityGroupId": "sg-88rlpl0h1",
        "vpcId": "vpc-88hs1****"
      }
    ]
  },
  "errorMsg": "",
  "errorDetail": "",
  "responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```


1.5.2.10. joinInstanceSecGroup

Description

Adds an Elastic Compute Service (ECS) instance to a specified security group. Make sure that:

- You can only add an instance in *stopped* or *running* status to a security group.
- An instance can belong to at most five security groups.
- A security group can have at most 1000 instances.

Name

joinInstanceSecGroup

URL

```
{dtcenter_api_url}/gateway/api/secgroups/manage/{securityGroupId}/joinInstance
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
securityGroupId	String	Yes	The security group ID
instanceId	String	Yes	The ECS instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/secgroups/manage/sg-889gj3idu/joinInstance?
departmentId=2
&instanceId=i-88neq****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "data": {},
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```


1.5.2.11. leaveSecurityGroup

Description

Removes an Elastic Compute Service (ECS) instance from a specified security group.

- You can only remove an instance in *stopped* or *running* status from a security group.
- An instance must belong to at least one security group. If an instance belongs to only one security group, you cannot remove it from that security group.

Name

leaveSecurityGroup

URL

```
{dtcenter_api_url}/gateway/api/secgroups/manage/{securityGroupId}/leaveInstance
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
securityGroupId	String	Yes	The security group ID
instanceId	String	Yes	The ECS instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://api.dtdream.com/gateway/api/secgroups/manage/sg-88muwnmu8/leaveInstance?
departmentId=12
&instanceId=i-88j5i****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "failed",
   "data": {},
   "errorMsg": "An ECS instance must be bound to a security group",
   "errorDetail": "",
   "responseCode": "",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.3. Disk-related APIs

1.5.3.1. createCloudDisk

Description

Creates a disk.

Name

createCloudDisk

URL

```
{dtcenter_api_url}/gateway/api/cloudDisk/manage/createCloudDisk
```

Request type

POST message.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
zoneId	String	Yes	The zone ID, which can be obtained by using the getZoneList API
departmentId	String	Yes	The department ID, which must be numbers and can be obtained by using the getDeptRootTree API
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API
category	String	Yes	The disk type, which can be obtained by using the getRegionList API
diskSize	String	Yes	Configures the disk size, whose range depends on the disk type
diskName	String	Yes	The disk name, which must be 2 to 128 characters in length and start with a letter in uppercase or lowercase. The name can contain letters, numbers, periods (.), underscores (_), and hyphens (-). The system displays the disk name in the console.
snapshotUse	Boolean	No	Whether to use snapshot
snapshotId	String	No	The snapshot ID
encrypted	Boolean	No	Whether to encrypt

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID
diskId	String	The ID of the newly created disk

Examples

- Request example

```
https://api.dtdream.com/gateway/api/cloudDisk/manage/createCloudDisk?
departmentId=2
&category=nova-ceph
&diskName=hhh
&diskSize=5
&projectId=1
&regionId=97d83522-0d78-4e95-a8b5-361eaa580504
&zoneId=nova
```

- Response example

```
{
   "result": "success",
   "data": {
      "requestId": "E61D51E5-DE93-4AF6-87F4-FE5E9A114266",
      "diskId": "d-886owreqz"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.3.2. deleteCloudDisk

Description

Deletes a specified disk.

Name

deleteCloudDisk

URL

```
{dtcenter_api_url}/gateway/api/cloudDisk/manage/deleteCloudDisk
```

Request type

POST message.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID
diskId	String	Yes	The disk ID

Response parameters

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudDisk/manage/deleteCloudDisk
?diskId=0481917e-6e97-4de4-a6a3-a03e9aa5994c
&regionId=97d83522-0d78-4e95-a8b5-361eaa580504
```

- Response example

```
{
   "errorMsg":"",
   "errorDetail":"",
   "result":"success",
   "requestId":null,
   "data":{
      "requestId":"B116DD03-C928-4F96-A6CF-3CC59BA8A069"
   },
   "return_subCode":"",
   "return_subMsg":"",
   "responseCode":"200"
}
```

1.5.3.3. getCloudDiskList

Description

Obtains the disk list. You can filter disks by region, department, disk name, disk ID, instance name, and automatic snapshot policy ID.

Name

getCloudDiskList

URL

{dtcenter_api_url}/gateway/api/cloudDisk/read/getCloudDiskList

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	No	The region ID, which can be obtained by using the getRegionList API
departmentId	String	No	The department ID, which can be obtained by using the getDeptRootTree API
conditionType	String	No	The type of query conditions. Values: • *diskName*: the disk name • *diskId*: the disk ID • *instanceName*: the instance name • *autoSnapshotPolicyId*: the automatic snapshot policy ID
conditionValue	String	No	The corresponding value of conditionType
diskType	String	No	The disk type: • *data*: the data disk • *system*: the system disk
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100
instanceId	String	No	The ID of the ECS instance to which the disk is mounted

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
diskId	String	The disk ID
diskName	String	The disk name
attachments	List<AttachInstanceInfo>	A list of instances to which disks are mounted. The list elements include the instance UUID and instance name of the host to which the disks are mounted. The AttachInstanceInfo structure is as follows: • *instanceName*: the name of the instance to which the disk is mounted • *device*: the disk mount point • *instanceId*: the ID of the instance to which the disk is mounted
instanceId	String	The ID of the instance to which the disk is mounted
instanceName	String	The name of the instance to which the disk is mounted
departmentName	String	The department name
projectName	String	The project name
projectId	String	The project ID
departmentId	String	The department ID
detach	Boolean	Whether the disk can be mounted independently. Values: • *true*: The disk can be mounted independently. • *false*: The disk cannot be mounted independently.
status	String	The disk status. Values: • *unrecognized*: unknown • *attached*: running • *available*: to be mounted • *attaching*: mounting • *detaching*: unmounting • *creating*: creating • *reIniting*: resetting • *error*: error • *deleting*: deleting

Name	Type	Description
statusFlag	String	Whether the disk status is stable. Values: • *stable*: stable status • *processing*: changing status
categoryName	String	The disk category Values: • *Basic cloud disk*: cloud • *SSD cloud disk*: cloud_ssd • *Ultra cloud disk*: cloud_efficiency
category	String	The disk category Values: • *cloud*: basic cloud disk • *cloud_ssd*: SSD cloud disk • *cloud_efficiency*: ultra cloud disk
type	String	The disk type. Values: • *system*: the system disk • *data*: the data disk
startTime	String	The created time
creationTimeStamp	Long	The timestamp of creation
diskSize	Integer	The disk size. Unit: GB.
device	String	The mount point
portable	Boolean	Whether the disk can be mounted and unmounted independently. Values: • *true*: The disk can be mounted and unmounted independently. • *false*: The disk cannot be mounted and unmounted independently.
regionId	String	The ID of the region where the disk resides
zoneId	String	The zone ID
regionType	String	The type of the region where the disk resides. Values: *regft* (Apsara Stack regions)

Name	Type	Description
regionSnapSupport	Boolean	Whether the region where the disk resides supports creating snapshots. Values: • *true*: supported • *false*: unsupported
regionName	String	The region name
autoSnapshotPolicyId	String	The automatic snapshot policy ID for the disk
encrypted	Boolean	Whether to encrypt
multiattach	Boolean	Whether to mount more

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudDisk/read/getCloudDiskList?
regionId=
&departmentId=
&conditionType=%E7%A3%81%E7%9B%98%E5%90%8D%E7%A7%B0
&conditionValue=
&pageNum=1
&pageSize=10
&diskType=data,system
```

- Response example

```
{
  "errorMsg":"",
  "errorDetail":"",
  "result":"success",
  "requestId":null,
  "data":{
    "totalRows":1,
    "pageSize":10,
    "rows":[
      {
        "diskId":"d-1ny05rohy9qhverkfd3z",
        "diskName":"newtest",
        "categoryName":"ecs.disk.type.cloud_efficiency",
```

```
            "category":"cloud_efficiency",
            "multiattach":false,
            "attachments":[
              {
                "instanceId":"",
                "instanceName":null
              }
            ],
            "departmentName":"test0723",
            "projectName":"testyundun",
            "projectId":"5000",
            "departmentId":3,
            "detach":"false",
            "status":"available",
            "statusFlag":"stable",
            "type":"data",
            "startTime":"2019-07-29 18:00:22",
            "diskSize":20,
            "device":"",
            "portable":"true",
            "regionId":"cn-qingdao-apsara-d02",
            "zoneId":"cn-qingdao-apsara-amtest18001-a",
            "regionType":"regft",
            "instanceId":"",
            "encrypted":false,
            "creationTimeStamp":1564394422000,
            "regionSnapSupport":true,
            "regionName":"cn-qingdao-apsara-d02",
            "autoSnapshotPolicyId":""
          }
        ],
        "pageNum":1
    },
    "return_subCode":null,
    "return_subMsg":null,
    "responseCode":"200"
}
```


1.5.3.4. getCloudDiskInfo

Description

Views disk details.

The disk must exist in the cloud platform.

Name

getCloudDiskInfo

URL

{dtcenter_api_url}/gateway/api/cloudDisk/read/getCloudDiskInfo

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The ID of the region where the disk resides. You can obtain the region ID by using the getRegionList API.
diskId	String	Yes	The disk ID.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
detach	Boolean	Whether the disk can be mounted independently Values: • *true*: The disk can be mounted independently. • *false*: The disk cannot be mounted independently.

Name	Type	Description
status	Stirng	The disk status Values: • *unrecognized*: unknown • *attached*: running • *available*: to be mounted • *attaching*: mounting • *detaching*: unmounting • *creating*: creating • *reIniting*: resetting • *error*: error • *deleting*: deleting
diskName	String	The disk name
regionName	String	The region name
attachments	List<AttachInstanceInfo>	A list of instances to which disks are mounted. The list elements include the instance UUID and instance name of the host to which the disks are mounted. The AttachInstanceInfo structure is as follows: • *instanceName*: the name of the instance to which the disk is mounted • *device*: the disk mount point • *instanceId*: the ID of the instance to which the disk is mounted
instanceId	String	The ID of the instance to which the disk is mounted
instanceName	String	The name of the instance to which the disk is mounted
device	String	The mount point of the disk
statusFlag	String	Whether the disk status is stable Values: • *stable*: stable status • *processing*: changing status
type	String	The disk type Values: • *system*: the system disk • *data*: the data disk

Name	Type	Description
departmentName	String	The name of the department where the disk resides
regionType	String	The type of the region where the disk resides Value: *regft* (Apsara Stack regions)
zoneId	String	The zone ID
size	Integer	The disk size. Unit: GB
startTime	String	The created time
category	String	The disk category Values: • *cloud*: basic cloud disk • *cloud_ssd*: SSD cloud disk • *cloud_efficiency*: ultra cloud disk
categoryName	String	The disk category Values: • *Basic cloud disk*: cloud • *SSD cloud disk*: cloud_ssd • *Ultra cloud disk*: cloud_efficiency
description	String	The disk description
deleteWithInstance	String	Whether the disk is released together with the instance Values: • *true*: The disk is released together with the instance. • *false*: The disk is not released together with the instance.
deleteAutoSnap	String	Whether the automatic snapshots are released together with the disk Values: • *true*: The automatic snapshots are released together with the disk. • *false*: The automatic snapshots are not released together with the disk.
projectName	String	The project name
diskId	String	The disk ID

Name	Type	Description
regionId	String	The region ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudDisk/read/getCloudDiskInfo?
diskId=d-88051vfbu
&regionId=cn-hangzhou-am24
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": {
    "detach": "false",
    "status": "available",
    "diskName": "testl",
    "regionName": "ApsaraStack",
    "statusFlag": "stable",
    "multiattach": false,
    "type": "data",
    "departmentName": "DoNotUseThisDepartment",
    "regionType": "regft",
    "zoneId": "cn-hangzhou-hsd-am24001-a",
    "size": 20,
    "startTime": "2016-08-15 13:39:24",
    "categoryName": "UltraCloudDisk",
    "category": "cloud_efficiency",
    "description": "fff",
    "deleteWithInstance": "false",
    "attachments": [
      {
        "instanceName": "",
        "device": "",
        "instanceId": ""
      }
    ],
    "deleteAutoSnap": "true",
    "projectName": "TestProject",
    "diskId": "d-88051vfbu",
    "regionId": "cn-hangzhou-am24"
  },
  "errorMsg": "",
  "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```


1.5.3.5. attachCloudDisk

Description

Mounts a disk to a corresponding Elastic Compute Service (ECS) instance.

Name

attachCloudDisk

URL

```
{dtcenter_api_url}/gateway/api/cloudDisk/use/attachCloudDisk
```

Request type

POST message.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID
device	String	No	The mount point
deleteWithInstance	String	Yes	Whether the disk is released together with the instance
instanceId	String	Yes	The ECS instance ID
diskId	String	Yes	The disk ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
https://api.dtdream.com/gateway/api/cloudDisk/use/attachCloudDisk
?deleteWithInstance=true
&device=%2Fdev%2Fxvdb&diskId=d-25porvt32
&instanceId=i-25l93****
&regionId=cn-beijing
```

- Response example

```
{
   "result": "success",
   "data": {
      "requestId": "709F8092-EDC5-4E58-97C4-FFC1A48978DC"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.3.6. detachCloudDisk

Description

Unmounts a disk from a corresponding Elastic Compute Service (ECS) instance.

Name

detachCloudDisk

URL

```
{dtcenter_api_url}/gateway/api/cloudDisk/use/detachCloudDisk
```

Request type

POST message.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The ID of the region where the disk to be unmounted resides
instanceId	String	Yes	The ID of the ECS instance to which the disk to be unmounted is mounted
diskId	String	Yes	The ID of the disk to be unmounted

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudDisk/use/detachCloudDisk
? diskId=d-25porvt32
&instanceId=i-25l93****
&regionId=cn-beijing
```

- Response example

```
{
   "result": "success",
   "data": {
      "requestId": "E6768A19-DD33-47F1-ACCD-2D3807FB8E36"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
"requestId": null
}
```

1.5.4. Image-related APIs

1.5.4.1. getImageList

Description

Obtains the image list. You can filter images by region, department, image name, image ID, and image type and can have the results displayed on pages.

Currently, the image type only supports *self* (custom image) and *system* (public image).

Name

getImageList

URL

```
{dtcenter_api_url}/gateway/api/image/read/getImageList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	No	The region ID, which can be obtained by using the getRegionList API
departmentId	String	No	The department ID, which can be obtained by using the getDeptRootTree API
imageName	String	No	The image name
imageId	String	No	The image ID
imageOwnerAlias	String	No	The image type Values: • *self*: custom image • *system*: public image
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100
projectName	String	No	The name of the project where the image resides

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
architecture	String	The type of the image system
projectName	String	The name of the project where the image resides
imageId	String	The image ID
imageName	String	The image name
regionId	String	The ID of the region where the image resides
departmentId	String	The ID of the department where the image resides
creationTime	String	The created time of the image
creationTimeStamp	Long	The timestamp when the image is created
description	String	The image description
imageOwnerAlias	String	The image type Values: • *system*: public image • *self*: custom image
imageVersion	String	The image version
osName	String	The name of the operating system
size	String	The image size
diskSize	Integer	The size of the system disk required by the image
diskFormat	String	The image format
departmentName	String	The name of the department where the image resides
regionName	String	The name of the region where the image resides
regionType	String	The type of the region where the image resides Value: *regft* (Apsara Stack regions)
platform	String	The platform of the operating system
status	String	The status

Name	Type	Description
shareDepartmentIds	List<Long>	The ID list of departments that share the image
shareDepartmentNames	List<Long>	The name list of departments that share the image

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/image/read/getImageList?
departmentId=
&imageOwnerAlias=self
&pageNum=1
&pageSize=10
&regionId=
&projectName=
```

- Response example


```
{
  "return_subMsg":null,
  "errorDetail":"",
  "result":"success",
  "errorMsg":"",
  "requestId":null,
  "data":{
    "totalRows":1,
    "pageSize":10,
    "rows":[
      {
        "projectName":"",
        "imageId":"m-1ny05roi2leidyl5acoo",
        "imageName":"wlqde",
        "regionId":"cn-qingdao-apsara-d02",
        "departmentId":"3",
        "architecture":"x86_64",
        "creationTime":"2019-07-30 11:19:38",
        "description":"TestImageSharing",
        "imageOwnerAlias":"self",
        "imageVersion":"",
        "isSubscribed":false,
        "osName":"OthersLinux_64",
```

```
            "platform":"Others Linux",
            "productCode":"",
            "departmentName":"test0723",
            "regionType":"regft",
            "visibility":"",
            "diskSize":"",
            "diskFormat":"",
            "encrypted":"false",
            "creationTimeStamp":1564456778000,
            "status":"available",
            "shareDepartmentIds":[
              17,
              14
            ],
            "shareDepartmentNames":[
              "portal",
              "DTCenterDevelopmentDepartment"
            ],
            "size":"5G",
            "regionName":"cn-qingdao-apsara-d02"
          }
        ],
        "pageNum":1
    },
    "responseCode":"200",
    "return_subCode":null
}
```


1.6. RDS-related APIs

1.6.1. RDS instance-related APIs

1.6.1.1. createRdsInstance

Description

Creates an ApsaraDB for RDS instance on the cloud platform and for later use.

Name

createRdsInstance

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/createRdsInstance
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
zoneId	String	No	The zone ID
instanceName	String	Yes	The instance name
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API
engine	String	Yes	The database type Values: • MySQL • PostgreSQL • PPAS By default, all values are returned.
engineVersion	String	Yes	The database version number Value range: • MySQL: 5.6/5.7 • PostgreSQL: 9.4/10.0 • PPAS: 9.3
dBInstanceClass	String	Yes	The instance type

Name	Type	Required	Description
dBInstanceStorage	Integer	Yes	The custom storage space Value range: • MySQL: 5 to 1000 • PostgreSQL: 5 to 2000 • PPAS: 5 to 2000 The value is incremented every 5 GB. Unit: GB.
instanceNetworkType	String	No	The network type of the instance Values: • *VPC*: Creates a Virtual Private Cloud (VPC) instance. • *Classic*: Creates a classic network instance. By default, a classic network instance is created.
vpcId	String	No	The VPC ID
vSwitchId	String	No	The VSwitch ID, which can be obtained by using the getVswitchList API Note If the network type is set to *VPC*, this parameter is required.
securityIPList	String	No	IP addresses of all databases under this instance are allowed to access. Separate the IP addresses by commas (,). Duplicate IP addresses are not allowed and up to 1000 IP addresses can be accessed. Supported format: %, 0.0.0.0/0, 10.23.12.24 (IP), or 10.23.12.24/24 (Classless Inter-Domain Routing (CIDR) mode. /24 defines the length of the address prefix, whose value ranges from 1 to 32) 0.0.0.0/0 can be used to access all IP addresses.
privateIpAddress	String	No	Users can specify the vpcIp under VSwitchId. If not, the system automatically allocates the IP address. Note Apsara Stack V3 supports this field.

Name	Type	Required	Description
dBInstanceNetType	String	No	The network connection type of the instance. *Internet* indicates the public network. *Intranet* indicates the private network. The default value is *Intranet*.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
dBInstanceId	String	The instance ID
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/createRdsInstance?
instanceName=wuchen_dtce****
&regionId=cn-hangzhou-am24
&departmentId=8
&projectId=2
&dBInstanceClass=rds.mys2.small
&engine=Mysql
&engineVersion=5.6
&dBInstanceStorage=5
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
   "dBInstanceId":"rdsw9zoz00r74w57****",
   "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AA"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```


1.6.1.2. deleteRdsInstance

Description

Deletes a specified ApsaraDB for RDS instance.

- The instance status must be *running*.
- No read-only instances exist.

Name

deleteRdsInstance

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/deleteRdsInstance
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
departmentId	String	Yes	The department ID, which must be numbers and can be obtained by using the getDeptRootTree API

Name	Type	Required	Description
instanceId	String	Yes	The instance ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/deleteRdsInstance?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
     "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AA"
  }
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```

1.6.1.3. modifyRdsInstanceSpec

Description

Modifies the instance type or storage space of an ApsaraDB for RDS instance. Make sure that:

- The instance status must be *running*.
- The instance does not have a running backup task.
- You must specify the instance type and storage space.
- When you reduce the disk space configurations, the entered disk space must be equal to or larger than 1.1 times the actual used space.

- Currently, only regular and read-only instances can be modified. Temporary instances cannot be modified.

Name

modifyRdsInstanceSpec

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/modifyRdsInstanceSpec
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The primary instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API
dBInstanceClass	String	No	The instance type
dBInstanceStorage	Integer	No	The custom storage space Value range: • MySQL: 5 to 2000 • PostgreSQL: 5 to 2000 • PPAS: 5 to 2000 The value is incremented every 5 GB. Unit: GB.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/modifyRdsInstanceSpec?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
&dBInstanceClass=rds.mys2.mid
&dBInstanceStorage=5
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
    "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AA"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```

1.6.1.4. getRdsInstanceList

Description

Obtains the ApsaraDB for RDS instance list. You can filter ApsaraDB for RDS instances by region, department, and instance ID and have the results displayed on pages.

Name

getRdsInstanceList

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/getRdsInstanceList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	No	The instance ID
departmentId	String	No	The department ID, which can be obtained by using the getDeptRootTree API
engine	String	No	The database type Values: • *MySQL* • *PostgreSQL* • *PPAS* By default, all values are returned.
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
totalRows	Integer	The total number of rows
pageSize	Integer	The number of instances on each page
pageNum	Integer	The page number
rows	List<DBInstanceEntity>	A collection of ApsaraDB for RDS instances. For more information, see DBInstanceEntity.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/getRdsInstanceList?
regionId=cn-hangzhou-am24
&departmentId=8
```

- Response example

```
{
 "result":"success",
 "responseCode":"200",
 "data": {
     "totalRows":2,
     "pageSize":30,
     "pageNum":1,
     "rows":[{
          "dBInstanceId": "rds285f2uy060q83****",
         "dBInstanceName":"dc****",
         "departmentId": "8",
         "departmentName": "department001",
         "projectId": "3",
         "projectName": "project001",
         "dBInstanceType":"Primary",
         "regionId":"cn-hangzhou-am24",
         "dBInstanceStatus":"Running",
         "engine":"MySQL",
         "engineVersion":"5.6"
       },
       {
         "dBInstanceId": "rds7mbn48od0ghtb****",
         "dBInstanceName":"dtce****",
         "departmentId": "8",
         "departmentName": "department001",
         "projectId": "3",
         "projectName": "project001",
         "dBInstanceType":"Primary",
         "regionId":"cn-hangzhou-am24",
         "dBInstanceStatus":"Running",
         "engine":"MySQL",
         "engineVersion":"5.6"
       }
    ]
  }
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```

1.6.1.5. getRdsInstanceAttribute

Description

Views the details of a specified ApsaraDB for RDS instance.

Name

getRdsInstanceAttribute

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/getRdsInstanceAttribute
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
instanceName	String	No	The instance name

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
data	DBInstanceAttribute	The detailed attributes of the RDS instance. For more information, see DBInstanceAttribute.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/getRdsInstanceAttribute?
instanceId=rds7mbn48od0ghtb****
&instanceName=creat****
&regionId=cn-hangzhou-am24
&departmentId=8
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
   "dBInstanceId":"****",
   "dBInstanceName":"dtce****",
   "dBInstanceType":"Primary",
   "instanceNetworkType":"Classic",
   "regionId":"cn-hangzhou-am24",
   "zoneId":"cn-hangzhou-hsd-am24001-a",
   "projectId":"4",
   "connectionString":"xxxx.mysql.rds.example.com",
   "port":3306,
   "engine":"MySQL",
   "engineVersion":"5.6",
   "dBInstanceClass":"rds.mys2.large",
   "dBInstanceMemory":2400,
   "dBInstanceStorage":38,
   "dBInstanceStatus":"Running",
   "lockMode":"Unlock",
   "lockReason":"",
   "dBMaxQuantity":500,
   "accountMaxQuantity":500,
   "creationTime":"2016-06-07T19:48:30Z",
   "availabilityValue":"88.81%",
   "maxIOPS":1200,
   "maxConnections":600,
   "masterInstanceId":"",
   "tempDBInstanceId":"",
   "readOnlyDBInstanceIds":[{"readOnlyDBInstanceId": "****"}],
   "requestId":"848C2359-5339-4C17-8A9C-76B7146F543F",
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```


1.6.2. RDS database-related APIs

1.6.2.1. createRdsDatabase

Description

Creates a new database under an ApsaraDB for RDS instance. Make sure that:

- The instance status must be *running*.
- The instance is not locked.
- The maximum number of databases allowed for the instance is not exceeded.
- The instance must be a primary instance.

Name

createRdsDatabase

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/createRdsDatabase
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API
dBName	String	Yes	The database name, which must be unique and 2 to 64 characters in length and can contain lowercase letters, numbers, underscores (_), and hyphens (-). The name must start with a letter in lowercase and end with a number or letter in lowercase.

Name	Type	Required	Description
characterSetName	String	Yes	A character set. Values: MySQL • *utf8* • *gbk* • *latin1* • *utf8mb4* (5.5 and 5.6)
dBDescription	String	No	The database description, which must be 2 to 256 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). The name must start with a letter, but must not start with `http://` or `https://`.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/createRdsDatabase?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
&projectId=2
&dBName=db1
&characterSetName=utf8
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
    "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AA"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```


1.6.2.2. deleteRdsDatabase

Description

Deletes a specified database under an ApsaraDB for RDS instance. Make sure that:

- The instance status must be *running*.
- The instance must be a primary instance.

Name

deleteRdsDatabase

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/deleteRdsDatabase
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API

Name	Type	Required	Description
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API
dBName	String	Yes	The database name, which can be 64 characters at most in length and contain letters and numbers. It must start with a letter and can be obtained by using the getRdsDatabaseList API.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/deleteRdsDatabase?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
&projectId=2
&dBName=db1
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
    "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AA"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```

1.6.2.3. getRdsDatabaseList

Description

Queries the database list of a specified ApsaraDB for RDS instance and a specific database.

- If an error occurs when you query the parameter type, an error message is returned and the returned data is null.
- No requirement for the instance status.
- This API does not support ApsaraDB RDS for PostgreSQL and ApsaraDB RDS for PPAS.

Name

getRdsDatabaseList

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/getRdsDatabaseList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
dBName	String	No	The database name
dBStatus	String	No	The database status Values: • *Creating*: creating • *Running*: running • *Deleting*: deleting

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
totalRows	Integer	The total number of rows

Name	Type	Description
databases	List<DBDatabaseEntity>	The database list. For more information, see DBDatabaseEntity.
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/getRdsDatabaseList?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
```

- Response example

```
{
 "result":"success",
 "responseCode": "200",
 "data": {
     "totalRows": 1,
     "databases":[{
         "dBInstanceId": "rds285f2uy060q83****",
         "engine":"MySQL",
         "dBName":"db1",
         "dBStatus":"Runing",
         "characterSetName":"utf8",
         "dBDescription":"",
         "accounts":[{"account":"wu****","accountPrivilege":"ReadWrite"}]
         }
     ]
     "requestId": "FDEAD66A-F1CE-4848-9B06-DDA5B6869E82"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```

1.6.3. RDS account-related APIs

1.6.3.1. createRdsAccount

Description

Creates an account for ApsaraDB for RDS instances. For each ApsaraDB for RDS instance, an account can perform operations on multiple databases and have different permissions to each database.

Make sure that:

- The instance status must be *running*.
- The instance is not locked.
- The maximum number of accounts allowed for the instance is not exceeded.

Name

createRdsAccount

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/createRdsAccount
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API
accountName	String	Yes	The account name used for operations The name must be unique and have 2 to 16 characters in length. It must start with a lowercase letter and can contain lowercase letters, numbers, and underscores (_).

Name	Type	Required	Description
accountPassword	String	Yes	The account password used for operations The password must be 6 to 32 characters in length, start with a number or a letter, and can contain letters, numbers, and underscores (_).
accountDescription	String	No	The account description The description must be 2 to 256 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). It must start with a letter or a number.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/createRdsAccount?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
&projectId=2
&accountName=<youracountname>
&accountPassword=<youraccountPassword>
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
    "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AA"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```


1.6.3.2. deleteRdsAccount

Description

Deletes a database account under an ApsaraDB for RDS instance. Make sure that:

The instance status must be *running*.

Name

deleteRdsAccount

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/deleteRdsAccount
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API

Name	Type	Required	Description
accountName	String	Yes	The account name used for operations

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/deleteRdsAccount?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
&projectId=2
&accountName=wu****
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
    "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AA"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```

1.6.3.3. getRdsAccountList

Description

Queries the account list of a specified instance and database or the details of a specified account.

No requirement for the instance status.

Name

getRdsAccountList

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/getRdsAccountList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
accounts	List<DBAccountEntity>	DBAccountEntity
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/getRdsAccountList?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
```

- Response example

```
{
 "result":"success",
 "responseCode":"200",
 "data": {
     "accounts":[{
         "dBInstanceId": "rds285f2uy060q83****",
         "accountName":"wuchen",
         "accountStatus":"Available",
         "accountDescription":"rds_manage",
         "databasePrivileges":[{"dBName":"db1","accountPrivilege":"ReadWrite"}]
         }
     ]
     "requestId":"CF0B21D4-2CA0-4D35-BB83-2B4E07E81A3F"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```


1.6.3.4. grantRdsAccountPrivilege

Description

Grants database access permissions to accounts. Each account can be associated with one or more databases. If an account already has the access permission to a specified database, success is directly returned.

The instance status must be *running*.

Name

grantRdsAccountPrivilege

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/grantRdsAccountPrivilege
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can only contain numbers and be obtained by using the getDeptRootTree API
projectId	String	Yes	The project ID, which must be numbers and can be obtained by using the getProjectList API
accountName	String	Yes	The account name used for operations
dBName	String	Yes	The name of the database associated with the account
accountPrivilege	String	Yes	The account permission • *ReadOnly*: read only • *ReadWrite*: read and write

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/grantRdsAccountPrivilege?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
&projectId=2
&accountName=wu****
&dBName=db1
&accountPrivilege=ReadWrite
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
     "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AB"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```


1.6.3.5. revokeRdsAccountPrivilege

Description

Revokes database access permissions of an ApsaraDB for RDS instance account.

Make sure that:

- The database instance status must be *running*.
- The database status must be *running*.

Name

revokeRdsAccountPrivilege

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/revokeRdsAccountPrivilege
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API

Name	Type	Required	Description
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API
accountName	String	Yes	The account name used for operations
dBName	String	Yes	The name of the database associated with the account

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/revokeRdsAccountPrivilege?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
&projectId=2
&accountName=wu****
&dBName=db1
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
      "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AB"
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```

1.6.3.6. resetRdsAccountPassword

Description

Resets the account password.

Make sure that:

- The instance status must be *running*.
- The instance is not locked.

Name

resetRdsAccountPassword

URL

```
{dtcenter_api_url}/gateway/api/rds/instance/resetRdsAccountPassword
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
instanceId	String	Yes	The instance ID
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API
accountName	String	Yes	The account name used for operations
accountPassword	String	Yes	The new password The password must be 6 to 32 characters in length and can contain letters, numbers, and underscores (_). It must start with a letter or a number.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/rds/instance/resetRdsAccountPassword?
instanceId=rds7mbn48od0ghtb****
&regionId=cn-hangzhou-am24
&departmentId=8
&projectId=2
&accountName=wu****
&accountPassword=<youraccountPassword>
```

- Response example

```
{
  "result":"success",
  "responseCode":"200",
  "data": {
     "requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AA",
  },
  "errorMsg":"",
  "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```

1.7. SLB-related APIs

1.7.1. SLB instance-related APIs

1.7.1.1. createCloudSlbEntry

Description

Creates a Server Load Balancer (SLB) instance. An SLB instance is generated based on parameters, with the service address and SLB instance ID assigned.

Name

createCloudSlbEntry

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/manage/createCloudSlbEntry
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
loadBalancerName	String	Yes	The SLB instance name, which must be 1 to 63 characters in length, start with a letter, and can contain letters, numbers, hyphens (-), periods (.), and underscores (_) The displayed name depends on the number of created SLB instances. • If only one SLB instance is created, the displayed instance name is the configured one. • If more than one SLB instances are created, the displayed instance name is loadBalancerName + underscore (_) + instance serial number. For example, three instances are created in batches and the instance name is set to testSlb. The displayed names of these three instances are testSlb_1, testSlb_2, and testSlb_3.
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
departmentId	String	Yes	The department ID, which can only contain numbers and be obtained by using the getDeptRootTree API
projectId	String	Yes	The project ID, which can only contain numbers and be obtained by using the getProjectList API
addressType	String	Yes	The address type, which specifies whether the assigned service address is a public IP address or internal IP address Values: • *internet*: the public IP address • *intranet*: the internal IP address
networkType	String	Yes	The network type Values: • *classic*: classic network • *vpc*: Virtual Private Cloud

Name	Type	Required	Description
vSwitchId	String	No	The VSwitch ID, which can be obtained by using the getVswitchList API If the network type is set to *vpc*, this parameter is required.
createNum	Integer	Yes	The number of SLB instances to be created. The value ranges from 1 to 30.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
successNum	Integer	The number of SLB instances that are created
createResult	List	The information of SLB instances that are created
loadBalancerId	String	The SLB instance ID
operationDetail	String	The error message. If the operation result is *failed*, this parameter is valid.
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/manage/createCloudSlbEntry?
internetChargeType=
&bandWith=100
&createNum=1
&departmentId=2
&addressType=intranet
&loadBalancerName=ali-slb
&networkType=vpc
&projectId=1
&regionId=cn-beijing
&successNum=0
&vSwitchId=vsw-rvfac****
```

- Response example

```
{
"result": "success",
"data": {
"createResult": [
{
"operationDetail": "",
"operationResult": "success",
"requestId": "8A996BF0-07A0-4CCA-B053-DAF858AD242F",
"loadBalancerId": "1564a29f914-cn-hangzhou-****"
}
],
"successNum": 1
},
"errorMsg": "",
"errorDetail": "",
"responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
}
```


1.7.1.2. delCloudSlbEntry

Description

Deletes a Server Load Balancer (SLB) instance.

Name

delCloudSlbEntry

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/manage/delCloudSlbEntry
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
loadBalancerId	String	The SLB instance ID
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/manage/delCloudSlbEntry?
loadBalancerId=15595b1c546-cn-beijing-btc****
&region=cn-beijing
```

- Response example

```
{
"result": "success",
"data": {
"requestId": "4A3CA71B-11B9-4DF7-ADC9-7E4AE746B9AA",
"loadBalancerId": "1564a29f914-cn-hangzhou-****"
},
"errorMsg": "",
"errorDetail": "",
"responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
}
```

1.7.1.3. setCloudSlbEntry

Description

Modifies the Server Load Balancer (SLB) instance status, such as stopping and starting SLB instances.

- If you start an SLB instance, all its listeners are started.
- If you stop an SLB instance, all its listeners are stopped.

Name

setCloudSlbEntry

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/use/setCloudSlbEntry
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
slbStatus	String	Yes	The SLB instance status Values: • *active*: The SLB instance is running. • *inactive*: The SLB instance is stopped.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
loadBalancerId	String	The SLB instance ID
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/setCloudSlbEntry?
regionId=cn-hangzhou-am24
&loadBalancerId=1560b1b4f7f-cn-hangzhou-****
&slbStatus=active
```

- Response example

```
{
"result": "success",
"data": {
"requestId": "E119A327-65EE-4A0F-9914-3645C7BB2F6A",
"loadBalancerId": "1560b1b4f7f-cn-hangzhou-****"
},
"errorMsg": "",
"errorDetail": "",
"responseCode": "200",
"return_subCode": "",
"return_subMsg": ""
}
```

1.7.1.4. getCloudSlbEntryBaseInfoById

Description

Queries the details of a specified Server Load Balancer (SLB) instance.

Name

getCloudSlbEntryBaseInfoById

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/read/getCloudSlbEntryBaseInfoById
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
loadBalancerId	String	The SLB instance ID
loadBalancerName	String	The SLB instance name
regionId	String	The region ID
departmentId	String	The department ID
projectId	String	The project ID
projectName	String	The project name
slbIp	String	The IP address of the SLB instance
createTime	String	The created time of the SLB instance
vpcId	String	The Virtual Private Cloud (VPC) ID
vSwitchId	String	The VSwitch ID
slbStatus	String	The SLB instance status. Values: • *inactive*: stopped • *active*: running • *locked*: locked
addressType	String	The address type. Values: • *internet*: the public IP address • *intranet*: the internal IP address
networkType	String	The network type. Values: • *classic*: classic network • *vpc*: Virtual Private Cloud
slbBandwidth	Long	The bandwidth
testEndTime	String	The trial period

Name	Type	Description
projectCode	String	The resource application ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/read/getCloudSlbEntryBaseInfoById?
regionId=cn-hangzhou-am24
&loadBalancerId=155c93c1de4-cn-hangzhou-****
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {
"createTime": "2016-09-28 10:40:30",
"networkType": "classic",
"projectCode": "w201609280000000621",
"testEndTime": "",
"loadBalancerName": "yangzhentest104",
"loadBalancerId": "1576eaa3224-cn-hangzhou-****",
"vSwitchId": "",
"slbStatus": "inactive",
"addressType": "intranet",
"projectId": "33",
"slbBandwidth": "",
"departmentName": "CloudPlatformDevelopmentDepartment",
"vpcId": "",
"slbIp": "172.31.XX.XX",
"departmentId": "2",
"projectName": "yangzhentestadf",
"regionId": "cn-hangzhou-am24"
},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.7.1.5. getCloudSlbList

Description

Obtains the Server Load Balancer (SLB) instance list. You can filter SLB instances by region, department, project, status, SLB instance name, SLB instance ID, service address, Virtual Private Cloud (VPC) ID, and project name and have the results displayed on pages.

Name

getCloudSlbList

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/read/getCloudSlbList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	No	The region ID used to filter SLB instances, which is empty by default.
departmentId	String	No	The department ID used to filter SLB instances, which is empty by default.
projectId	String	No	The project ID used to filter SLB instances, which is empty by default.
querySlbCondition	String	No	The field used to filter SLB instances. Values: • *loadBalancerName*: The SLB instance name • *loadBalancerId*: The SLB instance ID • *slbIp*: The service address • *slbStatus*: The status • *vpcId*: The VPC ID • *projectName*: The project name
querySlbParam	String	No	The corresponding values of the field used to filter SLB instances

Name	Type	Required	Description
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
dt_rowId	String	Format: row_ + row number. For example, row_1
loadBalancerId	String	The SLB instance ID
loadBalancerName	String	The SLB instance name
regionId	String	The region ID
departmentId	String	The department ID
projectId	String	The project ID
projectName	String	The project name
startTime	String	The created time of the SLB instance
slbStatus	String	The SLB instance status. Values: • *inactive*: stopped • *active*: running • *locked*: locked
isMonitor	Boolean	Whether a listener port is configured. Values: • *true*: A listener port is configured for the SLB instance. • *false*: No listener port is configured for the SLB instance.
slbIp	String	The SLB instance IP address
addressType	String	The address type. Values: • *intranet*: the internal IP address • *internet*: the public IP address

Name	Type	Description
networkType	String	The network type. Values: • *classic*: classic network • *vpc*: Virtual Private Cloud

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/read/getCloudSlbList/
? regionId=cn-beijing
&departmentId=2
&querySlbCondition=%E8%B4%9F%E8%BD%BD%E5%9D%87%E8%A1%A1%E5%90%8D%E7%A7%B0
&querySlbParam=active
&pageNum=1
&pageSize=10
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {
"totalRows": 16,
"pageSize": 10,
"rows": [
{
"dt_rowId": "row_2",
"loadBalancerId": "157bcdd1eac-cn-hangzhou-****",
"projectId": "25",
"departmentName": "CloudPlatformDevelopmentDepartment",
"projectName": "TestCreate",
"loadBalancerName": "testzhuanyouyun",
"startTime": "2016-10-13 15:06:30",
"regionId": "cn-hangzhou-am24",
"slbStatus": "active",
"isMonitor": false,
"slbIp": "172.31.XX.XX",
"addressType": "intranet",
"networkType": "classic",
"expireDate": "",
```

```
"listenerList": "pending"
},
{
"dt_rowId": "row_3",
"loadBalancerId": "157bd08dd99-cn-hangzhou-****",
"projectId": "47",
"departmentName": "CloudPlatformDevelopmentDepartment",
"projectName": "qgh",
"loadBalancerName": "yangzhentest102_1",
"startTime": "2016-10-13 15:54:17",
"regionId": "cn-hangzhou-am24",
"slbStatus": "active",
"isMonitor": false,
"slbIp": "172.31.XX.XX",
"addressType": "intranet",
"networkType": "classic",
"expireDate": "",
"listenerList": "pending"
}
],
"pageNum": 2
},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```


1.7.2. SLB listener-related APIs

1.7.2.1. setHttpServiceListener

Description

Creates or modifies Hypertext Transfer Protocol (HTTP) listeners, that is, to create or modify HTTP-based listeners for Server Load Balancer (SLB) instances, namely the HTTP-based policies and health check configurations.

The listener is automatically started after being created.

Name

setHttpServiceListener

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/use/setHttpServiceListener
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
listenerPort	Long	Yes	The frontend port of the SLB instance. The value ranges from 1 to 65535.
backendServerPort	Long	Yes	The backend port of the SLB instance. The value ranges from 1 to 65535.
bandwidth	Long	Yes	The peak value of the listened bandwidth Values: -1 | 1 to 1000. Unit: Mbps. *-1* indicates that the peak value of the bandwidth is not limited.
xForwardedFor	String	No	Whether to obtain the visitor's real IP address in the X-Forwarded-For method Values: • *on* • *off* Default value: *on* We recommend that you set the value to *on* for security concerns.
scheduler	String	No	The scheduling algorithm Values: • *wrr* • *wlc* Default value: *wrr*

Name	Type	Required	Description
stickySession	String	Yes	Whether to enable session persistence Values: • *on* • *off*
stickySessionType	String	It depends.	The cookie processing method If the stickySession is set to *on*, this parameter is required. If the stickySession is set to *off*, this parameter is ignored. Values: • *insert*: inserted from SLB • *server*: SLB learns from the backend server.
cookieTimeout	Long	It depends.	Timeout period of the cookie. If the stickySession is set to *on* and stickySessionType is set to *insert*, this parameter is required. Otherwise, this parameter is ignored. Value range: 1 to 86400. Unit: second.
cookie	String	It depends.	The cookie configured on the backend server. If the stickySession is set to *on* and stickySessionType is set to *server*, this parameter is required. Otherwise, this parameter is ignored. Values: A string which conforms to the RFC 2965 and must be 1 to 200 characters in length. The value can only contain ASCII English letters and numbers, cannot contain commas (,), semicolons (;), or spaces. It must not start with a dollar sign ($).
healthCheck	String	Yes	Whether to enable the health check Values: • *on* • *off*

Name	Type	Required	Description
healthCheckDomain	String	No	The domain name used for health checks Values: • *$_ip* • User-defined string: The string must be 1 to 80 characters in length and can only contain letters, numbers, hyphens (-), and periods (.). • Null If this parameter is set to *$_ip* or null, SLB uses the private IP addresses of each backend server as the domain for health checks.
healthCheckURI	String	It depends.	The URI used for health checks If the healthCheck is set to *on*, this parameter is required. If the healthCheck is set to *off*, this parameter is ignored. Values: The value must be 1 to 80 characters in length, start with a forward slash (/), and can only contain letters, numbers, hyphens (-), forward slashes (/), periods (.), percent signs (%), question marks (?), number signs (#), and ampersands (&).
healthCheckConnectPort	Long	It depends.	The port used for health checks. If the healthCheck is set to *on*, this parameter is required. If the healthCheck is set to *off*, this parameter is ignored. Values: 1 to 65535 or -520 If this parameter is set to *-520*, the backend service port is used.
healthyThreshold	Long	It depends.	The threshold that determines the health check result as *success*. In other words, after the health check succeeds consecutively for a specific number of times, the health check result of the backend server changes from *failed* to *success*. If the healthCheck is set to *on*, this parameter is required. If the healthCheck is set to *off*, this parameter is ignored. Value range: 1 to 10. Unit: time.

Name	Type	Required	Description
unhealthyThreshold	Long	It depends.	The threshold that determines the health check result as *failed*. In other words, after the health check fails consecutively for a specific number of times, the health check result of the backend server changes from *success* to *failed*. If the healthCheck is set to *on*, this parameter is required. If the healthCheck is set to *off*, this parameter is ignored. Value range: 1 to 10. Unit: time.
healthCheckTimeout	Long	It depends.	The maximum timeout of each health check response If the healthCheck is set to *on*, this parameter is required. If the healthCheck is set to *off*, this parameter is ignored. Value range: 1 to 50. Unit: second. If the healthCheckTimeout < healthCheckInterval, healthCheckTimeout is invalid and the timeout is healthCheckInterval.
healthCheckInterval	Long	It depends.	The time interval between two consecutive health checks If the healthCheck is set to *on*, this parameter is required. If the healthCheck is set to *off*, this parameter is ignored. Value range: 1 to 5. Unit: second.
healthCheckHttpCode	String	It depends.	The HTTP status code for a normal health check. Use a comma (,) to separate HTTP status codes. If the healthCheck is set to *on*, this parameter is optional. If the healthCheck is set to *off*, this parameter is ignored. Values: • *http_2xx* • *http_3xx* • *http_4xx* • *http_5xx* Default value: *http_2xx*
actionType	String	Yes	The operation type • *add*: creates a listener port. • *edit*: modifies a listener port.
idleTimeout	Integer	No	The idle timeout Value range: 10 to 900. Unit: second.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/setHttpServiceListener?
actionType=add
&backendServerPort=8080
&bandwidth=-1
&cookie=
&cookieTimeout=3000
&healthCheck=on
&healthCheckConnectPort=8080
&healthCheckDomain= example.com
&healthCheckHttpCode=http_2xx
&healthCheckInterval=2
&healthCheckTimeout=5
&healthCheckURI=%2Fmanage%2Fview
&healthyThreshold=3
&listenerPort=8080
&loadBalancerId=155c93c1de4-cn-hangzhou-****
&regionId=cn-hangzhou-am24
&scheduler=wrr
&stickySession=on
&stickySessionType=insert
&unhealthyThreshold=3
&xForwardedFor=on
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {
"requestId": "951BB464-7738-491E-805D-1409886BA0DB"
},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```


1.7.2.2. setTcpServiceListener

Description

Creates or modifies Transmission Control Protocol (TCP) listeners, that is, to create or modify TCP-based listeners for Server Load Balancer (SLB) instances.

- The listener is automatically started after being created.
- The health check of a TCP listener is always enabled. You can configure the health check parameters, but cannot disable the health check.

Name

setTcpServiceListener

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/use/setTcpServiceListener
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API

Name	Type	Required	Description
listenerPort	Long	Yes	The frontend port of the SLB instance. The value ranges from 1 to 65535.
backendServerPort	Long	Yes	The backend port of the SLB instance. The value ranges from 1 to 65535.
bandwidth	Long	Yes	The peak value of the listened bandwidth Values: -1 | 1 to 1000. Unit: Mbps. *-1* indicates that the peak value of the bandwidth is not limited.
scheduler	String	No	The scheduling algorithm Values: • *wrr* • *wlc* Default value: *wrr*
persistenceTimeout	Long	No	The timeout for connection persistence Value range: 0 to 1000. Unit: second. Default value: *0*. *0* indicates off.
healthCheckType	String	No	The health check type Values: • *tcp*: Transmission Control Protocol (TCP) • *http*: Hypertext Transfer Protocol (HTTP) Default value: *tcp*
healthCheckConnectPort	Long	No	The port used for health checks. The value ranges from 1 to 65535. Default value: None If this parameter is not set, the backend service port is used.
healthyThreshold	Long	No	The threshold that determines the health check result as *success*. In other words, after the health check succeeds consecutively for a specific number of times, the health check result of the backend server changes from *failed* to *success*. Value range: 1 to 10. Unit: time. Default value: 3 times

Name	Type	Required	Description
unhealthyThreshold	Long	No	The threshold that determines the health check result as *failed*. In other words, after the health check fails consecutively for a specific number of times, the health check result of the backend server changes from *success* to *failed*. Value range: 1 to 10. Unit: time. Default value: 3 times
healthCheckTimeout	Long	No	The connection timeout of health check Value range: 1 to 50. Unit: second. Default value: 5 seconds
healthCheckInterval	Long	No	The time interval between two consecutive health checks. Value range: 1 to 5. Unit: second. Default value: 2 seconds
healthCheckHttpCode	String	No	The HTTP status code for a normal health check. Use a comma (,) to separate HTTP status codes. If the healthCheck is set to *on*, this parameter is optional. If the healthCheck is set to *off*, this parameter is ignored. Values: • *http_2xx* • *http_3xx* • *http_4xx* • *http_5xx* Default value: *http_2xx*
actionType	String	Yes	The operation type • *add*: create a listener port. • *edit*: modify a listener port.
establishedTimeout	Integer	No	The idle timeout Value range: 0 to 900. Unit: second.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Name	Type	Description

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/setTcpServiceListener?
establishedTimeout=900
&actionType=add
&backendServerPort=22
&bandwidth=-1
&healthCheck=on
&healthCheckConnectPort=22
&healthCheckHttpCode=
&healthCheckInterval=2
&healthCheckTimeout=5
&healthyThreshold=3
&listenerPort=22
&loadBalancerId=155c93c1de4-cn-hangzhou-****
&persistenceTimeout=1000
&regionId=cn-hangzhou-am24
&scheduler=wrr
&unhealthyThreshold=3
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {
"requestId": "E64E2032-E2C1-491D-B07B-946D08B58608"
},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.7.2.3. deleteServiceListener

Description

Deletes a specified listener.

If the Server Load Balancer (SLB) instance to which the listener belongs is in *locked* status, this API fails to be called.

Name

deleteServiceListener

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/use/deleteServiceListener
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
listenerPort	Long	Yes	The frontend port of the SLB instance. The value ranges from 1 to 65535.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/deleteServiceListener?
loadBalancerId=155c93c1de4-cn-hangzhou-****
&listenerPort=45
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "resquestId": "64D811C8-1A83-40EC-878C-0363E6F9F221"
   },
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.7.2.4. getServiceListener

Description

Obtains the Server Load Balancer (SLB) listener list.

Name

getServiceListener

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/read/getServiceListener
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
dt_rowId	String	The row name in the format of row_ + index. For example, row_1.
protocol	String	The listener protocol. Values: • *HTTPS*: Hyper Text Transfer Protocol over Secure Socket Layer • *HTTP*: HyperText Transfer Protocol • *TCP*: Transmission Control Protocol
listenerPort	Long	The frontend port of the SLB instance. The value ranges from 1 to 65535.
backendServerHealthStatus	String	The health status of the backend server. Values: • *normal*: normal • *abnormal*: abnormal • *unavailable*: The health check is not completed.
backendServerList	String	The ID of an abnormal server, such as "instance1, instance2, instance3"
backendProtocol	String	The backend protocol. Values: • *HTTPS*: Hyper Text Transfer Protocol over Secure Socket Layer • *HTTP*: HyperText Transfer Protocol • *TCP*: Transmission Control Protocol
backendServerPort	Long	The backend port of the SLB instance
serviceStatus	String	The listener status. Values: • *running*: running • *stopped*: stopped
scheduler	String	The scheduling algorithm. Values: • *wrr*: weighted round robin • *wlc*: weighted least connections
xForwardedFor	String	Whether to obtain the visitor's real IP address in the X-Forwarded-For method. Values: • *on*: enabled • *off*: disabled

Name	Type	Description
stickySession	String	Whether to enable session persistence. Values: • *on*: enabled • *off*: disabled
stickySessionType	String	The cookie processing method. If the stickySession is set to *on*, this parameter is valid. Values: • *insert*: SLB inserts cookies. • *server*: SLB rewrites cookies.
cookie	String	The cookie configured on the server If the stickySession is set to *on* and stickySessionType is set to *server*, this parameter is valid.
cookieTimeout	Long	The cookie timeout If the stickySession is set to *on* and stickySessionType is set to *insert*, this parameter is valid.
bandwidth	Long	The peak value of the listened bandwidth. The value ranges from -1 to 1000. *-1* indicates that the value of bandwidth is not limited. Unit: Mbps.
healthCheck	String	Whether to enable the health check. Values: • *on*: enabled • *off*: disabled
healthCheckDomain	String	The domain name used for health checks
healthCheckURI	String	The URI used for health checks
healthCheckConnectPort	Long	The port used for health checks If the healthCheck is set to *on*, this parameter is valid.
healthCheckTimeout	Long	The maximum timeout of each health check response If the healthCheck is set to *on*, this parameter is valid.
healthCheckInterval	Long	The time interval between two adjacent health checks If the healthCheck is set to *on*, this parameter is valid.

Name	Type	Description
unhealthyThreshold	Long	The threshold that determines the health check result as *failed*. In other words, after the health check fails consecutively for a specific number of times, the health check result of the backend server changes from *success* to *failed*. If the healthCheck is set to *on*, this parameter is valid.
healthyThreshold	Long	The threshold that determines the health check result as *success*. In other words, after the health check succeeds consecutively for a specific number of times, the health check result of the backend server changes from *failed* to *success*. If the healthCheck is set to *on*, this parameter is valid.
healthCheckHttpCode	Long	The HTTP status code for a normal health check. Use a comma (,) to separate HTTP status codes. If the healthCheck is set to *on*, this parameter is valid.
serverCertificateId	String	The server certificate ID If the frontend listener protocol is *HTTPS*, this parameter is valid.
persistenceTimeout	Integer	The timeout for connection persistence If the frontend listener protocol is set to *TCP*, this parameter is valid.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/read/getServiceListener?
loadBalancerId=1565490d1b2-cn-hangzhou-****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": [
    {
      "dt_rowId": "row_0",
      "protocol": "HTTP",
      "listenerPort": 8080,
      "backendServerHealthStatus": "abnormal"
```

```
    "backendServerHealthStatus": "abnormal",
    "backendServerList": "i-8892e905g, i-88i905gi2, i-88mepg4xy, i-881j7slsu",
    "backendProtocol": "HTTP",
    "backendServerPort": 8080,
    "serviceStatus": "running",
    "scheduler": "wrr",
    "xForwardedFor": "on",
    "stickySession": "off",
    "bandwidth": -1,
    "healthCheck": "on",
    "healthCheckDomain": null,
    "healthCheckURI": "/",
    "healthCheckConnectPort": 8080,
    "healthCheckTimeout": 5,
    "healthCheckInterval": 2,
    "unhealthyThreshold": 3,
    "healthyThreshold": 3,
    "healthCheckHttpCode": "http_2xx,http_3xx"
  },
  {
    "dt_rowId": "row_1",
    "protocol": "HTTP",
    "listenerPort": 22,
    "backendServerHealthStatus": "unavailable",
    "backendServerList": "",
    "backendProtocol": "HTTP",
    "backendServerPort": 22,
    "serviceStatus": "running",
    "scheduler": "wrr",
    "xForwardedFor": "on",
    "stickySession": "on",
    "stickySessionType": "insert",
    "cookie": "",
    "cookieTimeout": 3000,
    "bandwidth": -1,
    "healthCheck": "off"
  },
  {
    "dt_rowId": "row_2",
    "protocol": "HTTPS",
    "listenerPort": 9090,
    "backendServerHealthStatus": "unavailable",
```

```
    "backendServerList": "",
    "backendProtocol": "HTTPS",
    "backendServerPort": 9090,
    "serverCertificateId": "1240965701077932_156c0270d08",
    "serviceStatus": "running",
    "scheduler": "wrr",
    "xForwardedFor": "on",
    "stickySession": "on",
    "stickySessionType": "insert",
    "cookie": "",
    "cookieTimeout": 3000,
    "bandwidth": -1,
    "healthCheck": "off"
  },
  {
    "dt_rowId": "row_3",
    "protocol": "HTTPS",
    "listenerPort": 9091,
    "backendServerHealthStatus": "abnormal",
    "backendServerList": "i-8892e905g, i-88i905gi2, i-88mepg4xy, i-881j7slsu",
    "backendProtocol": "HTTPS",
    "backendServerPort": 9091,
    "serverCertificateId": "1240965701077932_156bbef80ab",
    "serviceStatus": "running",
    "scheduler": "wrr",
    "xForwardedFor": "on",
    "stickySession": "off",
    "bandwidth": -1,
    "healthCheck": "on",
    "healthCheckDomain": "",
    "healthCheckURI": "/",
    "healthCheckConnectPort": 9091,
    "healthCheckTimeout": 5,
    "healthCheckInterval": 2,
    "unhealthyThreshold": 3,
    "healthyThreshold": 3,
    "healthCheckHttpCode": "http_2xx,http_3xx"
  },
  {
    "dt_rowId": "row_4",
    "protocol": "TCP",
```

```
        "listenerPort": 33,
        "backendServerHealthStatus": "abnormal",
        "backendServerList": "i-8892e905g, i-88i905gi2, i-88mepg4xy, i-881j7slsu",
        "backendProtocol": "TCP",
        "backendServerPort": 33,
        "serviceStatus": "running",
        "scheduler": "wrr",
        "xForwardedFor": "",
        "persistenceTimeout": 1000,
        "stickySession": "on",
        "stickySessionType": "",
        "cookie": "",
        "cookieTimeout": 1000,
        "bandwidth": -1,
        "healthCheck": "on",
        "healthCheckDomain": null,
        "healthCheckURI": null,
        "healthCheckConnectPort": 33,
        "healthCheckTimeout": 5,
        "healthCheckInterval": 2,
        "unhealthyThreshold": 3,
        "healthyThreshold": 3,
        "healthCheckHttpCode": null,
        "healthCheckType": null
    },
    {
        "dt_rowId": "row_5",
        "protocol": "UDP",
        "listenerPort": 44,
        "backendServerHealthStatus": "abnormal",
        "backendServerList": "i-8892e905g, i-88i905gi2, i-88mepg4xy, i-881j7slsu",
        "backendProtocol": "UDP",
        "backendServerPort": 44,
        "serviceStatus": "running",
        "scheduler": "wlc",
        "xForwardedFor": "",
        "persistenceTimeout": 0,
        "stickySession": "off",
        "stickySessionType": "",
        "cookie": "-",
        "cookieTimeout": 0,
        "bandwidth": -1
```

```
            "bandwidth": -1,
            "healthCheck": "on",
            "healthCheckDomain": null,
            "healthCheckURI": null,
            "healthCheckConnectPort": 44,
            "healthCheckTimeout": 5,
            "healthCheckInterval": 2,
            "unhealthyThreshold": 3,
            "healthyThreshold": 3,
            "healthCheckHttpCode": null,
            "healthCheckType": null
        }
    ],
    "errorMsg": "",
    "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```


1.7.2.5. startServiceListener

Description

Starts a specified listener.

- After this API is called, the listener enters the *starting* status.
- This API can only be called when the listener is in *stopped* status.
- If the status of the Server Load Balancer (SLB) instance to which the listener belongs is in *locked* status, this API fails to be called.

Name

startServiceListener

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/use/startServiceListener
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
listenerPort	Long	Yes	The frontend port of the SLB instance. The value ranges from 1 to 65535.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/startServiceListener?
loadBalancerId=155c93c1de4-cn-hangzhou-****
&listenerPort=45
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "requestId": "CD88AD4F-602E-4E1A-93AC-F36FF598DDD5"
   },
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.7.2.6. stopServiceListener

Description

Stops a specified listener.

- After this API is called, the listener enters the *stopped* status.
- If the status of the Server Load Balancer (SLB) instance to which the listener belongs is in *locked* status, this API fails to be called.

Name

stopServiceListener

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/use/stopServiceListener
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
listenerPort	Long	Yes	The frontend port of the SLB instance. The value ranges from 1 to 65535.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/stopServiceListener?
loadBalancerId=155c93c1de4-cn-hangzhou-am24
&listenerPort=56
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "requestId": "A0C663AE-59F2-4D3F-8414-7257E0A09D0E"
   },
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```


1.7.3. SLB backend server-related APIs

1.7.3.1. addBackendServer

Description

Adds a backend server to a Server Load Balancer (SLB) instance.

- To add a backend server, the Elastic Compute Service (ECS) instance and the SLB instance must be in level-1 department.
- For an SLB instance of the classic network, you can add an ECS instance of the classic network or of the same Virtual Private Cloud (VPC) as that of the SLB instance.
- For an SLB instance of the VPC network type, you can add an ECS instance of the same VPC as that of the SLB instance.

Name

addBackendServer

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/use/addBackendServer
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Name	Type	Required	Description
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
backendServerId	String	Yes	The backend server ID, which can be obtained by using the getBackendServerList API
weight	Integer	Yes	The backend server weight Value range: 1 to 100 Default value: 100

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
backendServerId	String	The backend server ID
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/addBackendServer?
backendServerId=i-88ddgtspx
&loadBalancerId=1560b1aea46-cn-hangzhou-****
&regionId=cn-hangzhou-am24
&weight=100
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "requestId": "73A43867-90F9-4DC0-9E30-A2D758B1705B",
      "backendServerId": "i-88ddgtspx"
   },
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```


1.7.3.2. removeBackendServer

Description

Removes a backend server from a Server Load Balancer (SLB) instance.

If the backend server to be removed is not in the SLB instance, the request to remove it from the SLB instance is directly ignored and does not trigger an error message.

Name

removeBackendServer

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/use/removeBackendServer
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API

Name	Type	Required	Description
backendServerId	String	Yes	The backend server ID, which can be obtained by using the getBackendServerList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
backendServerId	String	The backend server ID
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/removeBackendServer?
backendServerId=i-88ddgtspx
&loadBalancerId=1560b1aea46-cn-hangzhou-am24
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "requestId": "3D2092D8-A1A4-4ABF-83C7-E4AD66F00C3E",
      "backendServerId": "i-88ddgtspx"
   },
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.7.3.3. setBackendServer

Description

Configures the weight values of backend servers (Elastic Compute Service (ECS) instances) for Server Load Balancer (SLB) instances.

Name

setBackendServer

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/use/setBackendServer
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
backendServerId	String	Yes	The backend server ID, which can be obtained by using the getBackendServerList API
weight	Integer	Yes	The backend server weight Value range: 1 to 100 Default value: 100

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
backendServerId	String	The backend server ID
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/setBackendServer
? backendServerId=i-88qv1rkpp
&loadBalancerId=1560b1aea46-cn-hangzhou-****
&regionId=cn-hangzhou-am24
&weight=90
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "requestId": "13C97436-3EEF-4FA5-BF85-A14058446FFB",
      "backendServerId": "i-88qv1rkpp"
   },
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.7.3.4. getBackendServerList

Description

Obtains the backend server list of a Server Load Balancer (SLB) instance.

Name

getBackendServerList

URL

```
{dtcenter_api_url}/gateway/api/cloudLoadBalancer/read/getBackendServerList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
dt_rowId	String	The row name in the format of row_ + index. For example, row_1.
backendServerId	String	The backend server ID
backendServerName	String	The backend server name
loadBalancerId	String	The SLB instance ID
regionId	String	The region ID
regionType	String	The region type
hostName	String	The hostname of the backend server
publicIpList	String	The public IP address
innerIpAddress	String	The internal IP address
privateIpAddress	String	The private IP address
eipAddress	String	Elastic IP Address (EIP)
vpcId	String	The Virtual Private Cloud (VPC) ID
instanceNetworkType	String	The backend server network type • *vpc*: Virtual Private Cloud • *classic*: classic network
status	String	The instance status. Values: • *deleted*: released • *running*: running • *stopped*: stopped • *stopping*: stopping • *starting*: starting
weight	Integer	The weight

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudSlb/read/cloudLoadBalancer/read/getBackendSe
rverList?
loadBalancerId=1560b1aea46-cn-hangzhou-****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": [
    {
      "dt_rowId": "row_0",
      "backendServerId": "i-88mepg4xy",
      "loadBalancerId": "157bcd67390-cn-hangzhou-****",
      "backendServerName": "slb-test_3",
      "regionId": "cn-hangzhou-am24",
      "regionType": "regft",
      "hostName": "iZ88mepg4xyZ",
      "vpcId": "vpc-88545****",
      "publicIpList": "",
      "innerIpAddress": "",
      "privateIpAddress": "192.168.XX.XX",
      "status": "running",
      "instanceNetworkType": "vpc",
      "health": "pending",
      "eipAddress": "",
      "weight": 100
    },
    {
      "dt_rowId": "row_1",
      "backendServerId": "i-88i905gi2",
      "loadBalancerId": "157bcd67390-cn-hangzhou-****",
      "backendServerName": "slb-test_1",
      "regionId": "cn-hangzhou-am24",
      "regionType": "regft",
      "hostName": "iZ88i905gi2Z",
      "vpcId": "vpc-88545****",
      "publicIpList": ""
```

```
        "publicIpList": "",
        "innerIpAddress": "",
        "privateIpAddress": "192.168.XX.XX",
        "status": "running",
        "instanceNetworkType": "vpc",
        "health": "pending",
        "eipAddress": "",
        "weight": 100
    },
    {
        "dt_rowId": "row_2",
        "backendServerId": "i-8892e905g",
        "loadBalancerId": "157bcd67390-cn-hangzhou-****",
        "backendServerName": "zhangjs",
        "regionId": "cn-hangzhou-am24",
        "regionType": "regft",
        "hostName": "yuanfang",
        "vpcId": "vpc-88545****",
        "publicIpList": "",
        "innerIpAddress": "",
        "privateIpAddress": "192.168.XX.XX",
        "status": "running",
        "instanceNetworkType": "vpc",
        "health": "pending",
        "eipAddress": "",
        "weight": 100
    },
    {
        "dt_rowId": "row_3",
        "backendServerId": "i-881j7slsu",
        "loadBalancerId": "157bcd67390-cn-hangzhou-****",
        "backendServerName": "slb-test_2",
        "regionId": "cn-hangzhou-am24",
        "regionType": "regft",
        "hostName": "iZ881j7slsuZ",
        "vpcId": "vpc-88545****",
        "publicIpList": "",
        "innerIpAddress": "",
        "privateIpAddress": "192.168.XX.XX",
        "status": "running",
        "instanceNetworkType": "vpc",
        "health": "pending",
```

```
        "eipAddress": "",
        "weight": 100
      }
   ],
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```


1.7.3.5. getBackendServerHealthStatus

Description

Queries the health status of the backend server of a Server Load Balancer (SLB) instance.

Name

getBackendServerHealthStatus

URL

{dtcenter_api_url}/gateway/api/cloudLoadBalancer/read/getBackendServerHealthStatus

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
loadBalancerId	String	Yes	The SLB instance ID, which can be obtained by using the getCloudSlbList API
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
listenerPort	Long	The listener port number, such as 8080 and 8443
protocol	String	The listener protocol. Values: • *TCP* • *UDP* • *HTTP* • *HTTPS*
status	String	The health status • *normal*: normal • *abnormal*: abnormal • *unavailable*: The health check is not completed.
backendServerId	String	The backend server ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/cloudLoadBalancer/use/getBackendServerHealthStatus?
loadBalancerIds=1580e5c7c9c-cn-hangzhou-****
regionId=cn-hangzhou-am24
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": [
    {
      "backendServerId": "i-88l5kyck0",
      "status": "abnormal",
      "protocol": "tcp",
      "listenerPort": 22
    },
    {
      "backendServerId": "i-88ru3532m",
      "status": "abnormal",
      "protocol": "tcp",
      "listenerPort": 22
    }
```

```
    },
    {
      "backendServerId": "i-88yxlfn04",
      "status": "abnormal",
      "protocol": "tcp",
      "listenerPort": 22
    },
    {
      "backendServerId": "i-88l5kyck0",
      "status": "abnormal",
      "protocol": "https",
      "listenerPort": 443
    },
    {
      "backendServerId": "i-88ru3532m",
      "status": "abnormal",
      "protocol": "https",
      "listenerPort": 443
    },
    {
      "backendServerId": "i-88yxlfn04",
      "status": "abnormal",
      "protocol": "https",
      "listenerPort": 443
    },
    {
      "backendServerId": "i-88l5kyck0",
      "status": "abnormal",
      "protocol": "http",
      "listenerPort": 80
    },
    {
      "backendServerId": "i-88ru3532m",
      "status": "abnormal",
      "protocol": "http",
      "listenerPort": 80
    },
    {
      "backendServerId": "i-88yxlfn04",
      "status": "abnormal",
      "protocol": "http",
      "listenerPort": 80
```

```
    }
  ],
  "errorMsg": "",
  "errorDetail": "",
"return_subCode": "",
"return_subMsg": ""
}
```

1.8. OSS-related APIs

1.8.1. Bucket attribute-related APIs

1.8.1.1. setBucketWebsite

Description

Configures the homepage of a specified Object Storage Service (OSS) bucket.

Name

setBucketWebsite

URL

```
gateway/api/cloudOss/use/setBucketWebsite
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
indexHtml	String	No	The default homepage name, which can only end with .html. Leave it null or blank to cancel the settings.
errorHtml	String	No	The 404 page name, which can only end with .html, .jpg, .webp, .png, and .bmp. Leave it null or blank to cancel the settings.
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
https://api.dtdream.com/gateway/api/cloudOss/use/SetBucketWebsite?
bucketName=bucket-wine****
&errorHtml=2.html
&indexHtml=1.html
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "data": {},
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.8.1.2. getBucketWebsite

Description

Obtains the homepage settings of a specified Object Storage Service (OSS) bucket.

- Users can configure the default homepage and the 404 page.
- With the default homepage configured, the homepage directly appears when users access the corresponding service address of the bucket.
- With the 404 page configured, the 404 page directly appears when users access an incorrect bucket path or the corresponding file does not exist.

Name

getBucketWebsite

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/read/getBucketWebsite
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
errorHtml	String	The 404 page name. If not configured, the value is "".
indexHtml	String	The homepage name. If not configured, the value is "".

Examples

- Request example

```
https://api.dtdream.com/gateway/api/cloudOss/read/getBucketWebsite?
bucketName=bucket-wine****
&region=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "data": {
      "errorHtml": "",
      "indexHtml": ""
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```


1.8.1.3. setBucketACL

Description

Configures the read-write permissions of a specified Object Storage Service (OSS) bucket.

Currently, the bucket has three kinds of read-write permissions:

Value	Business meaning
public-read-write	Public read-write, indicating everyone can read from and write to the bucket without authorization
public-read	Public read, indicating everyone can obtain bucket files without authorization, but needs authentication for uploading files
private	Private, indicating authentication is required for both uploading and acquisition

Name

setBucketACL

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/use/setBucketACL
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
privilege	String	Yes	The permission Values: • *public-read-write*: public read-write, indicating everyone can read from and write to the bucket without authorization • *public-read*: public read, indicating everyone can obtain bucket files without authorization, but needs authentication for uploading files • *private*: private, indicating authentication is required for both uploading and acquisition
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/use/setBucketACL?
bucketName=bucket-wine****
&privilege=public-read
&region=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "data": {},
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.8.1.4. getBucketACL

Description

Obtains the read-write permissions of a specified Object Storage Service (OSS) bucket.

Currently, the bucket has three kinds of read-write permissions:

Value	Business meaning
public-read-write	Public read-write, indicating everyone can read from and write to the bucket without authorization
public-read	Public read, indicating everyone can obtain bucket files without authorization, but needs authentication for uploading files
private	Private, indicating authentication is required for both uploading and acquisition

Name

getBucketACL

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/read/getBucketACL
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
bucketAcl	String	The permission to read from and write to the bucket

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/read/getBucketACL?
bucketName=bucket-wine****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
"result": "success",
"data": {
"bucketAcl": "public-read-write"
},
"errorMsg": "",
"errorDetail": "",
"responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.8.2. Bucket-related APIs

1.8.2.1. getBucketList

Description

Obtains all of the Object Storage Service (OSS) bucket lists in the cloud platform.

This API returns all bucket lists in the cloud platform based on users' access permissions. If no parameter is specified, all visible buckets are returned.

Name

getBucketList

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/read/getBucketList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
departmentId	String	No	The department ID, which can be obtained by using the getDeptRootTree API
projectId	String	No	The project ID, which can be obtained by using the getProjectList API
bucketName	String	No	The bucket name, which supports fuzzy query based on partial match
regionId	String	No	The region ID, which can be obtained by using the getRegionList API
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time to obtain the queried data in a paged way. The value ranges from 1 to 65535.
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time to obtain the queried data in a paged way. The value ranges from 1 to 100.
orderBy	String	No	The keyword used to sort the data. You must specify orderBy and orderAsc at the same time.
orderAsc	Boolean	No	The sort order of data. You must specify orderBy and orderAsc at the same time. Values: • *true*: ascending order • *false*: descending order

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
rows	BucketEntity	A collection of bucket instances. For more information, see BucketEntity.
requestId	String	The request ID

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/read/getBucketList?
bucketName=bu****
&orderAsc=false
&orderBy=createTimeStamp
&departmentId=542
&pageNum=1
&pageSize=10
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
"responseCode": "200",
   "data": {
      "rows": [
         {
            "instanceName": "bucke****",
            "projectName": "p5",
            "projectId": "14",
            "createDate": "2016-07-18 19:32:43",
             "createTimeStamp": "1539084441000",
            "storeSpace": "1",
            "newStoreSpace": "1024",
            "regionId": "cn-shanghai",
            "expireDate": "",
            "departmentId": "542",
            "departmentName": "dtboost2",
            "userId": "9",
            "creator": "admin",
            "isAliType": true
         }
      ],
      "totalRows": "1"
   },
   "errorMsg": "",
   "errorDetail": "",
   "requestId": null,
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```


1.8.2.2. deleteBucket

Description

Deletes a specified Object Storage Service (OSS) bucket in the cloud platform.

Before deleting a bucket, you must clear all objects in the bucket. Otherwise, the bucket fails to be deleted.

Name

deleteBucket

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/manage/deleteBucket
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
bucketName	String	Yes	The bucket name

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/manage/deleteBucket?
bucketName=bucket-wine****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "errorMsg":"",
   "return_subCode":"",
   "responseCode":"200",
   "result":"success",
   "requestId":null,
   "data":{
      "requestId":""
   },
   "return_subMsg":"",
   "errorDetail":""
}
```

1.8.2.3. createBucket

Description

Creates an Object Storage Service (OSS) bucket in the cloud platform.

- The root department ID cannot be used as a department ID.
- Users must have permissions to the department and the project, which are specified by the department ID and project ID respectively.
- The project, which is specified by the project ID, must belong to the department, which is specified by the department ID.
- A maximum capacity can be set for a bucket. No limitation mode is also available.

Name

createBucket

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/manage/createBucket
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
bucketName	String	Yes	The bucket name, which must be 3 to 35 characters in length, start and end with a lowercase letter or a number, and can only contain lowercase letters, numbers, and hyphens (-)
privilege	String	Yes	The bucket access permission. Values: • *public-read-write*: public read-write, indicating everyone can read from and write to the bucket without authorization • *public-read*: public read, indicating everyone can obtain bucket files without authorization, but needs authentication for uploading files • *private*: private, indicating authentication is required for both uploading and acquisition
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
spaceStorage	Long	Yes	The maximum capacity of the bucket. The value must be an integer. 0 indicates no limitation.
projectId	String	Yes	The project ID, which can be obtained by using the getProjectList API
createOssNum	Integer	No	The number of buckets to be created in batches. The default value is 1. At most 10 buckets can be created at a time.
capacityUnit	String	No	The unit of the bucket capacity. The default value is TB. If the value of spaceStorage is *0*, this parameter is not required. Values: • *GB* • *TB*
description	String	No	The description of the bucket

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
successNum	String	The number of instances created
instanceId	String	The instance ID returned after the creation.

Name	Type	Description
regionId	String	The region ID returned after the creation.
requestId	String	The request ID

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/manage/createBucket?
bucketName=bucket-wine****
&departmentId=2
&privilege=public-read-write
&projectId=13
&regionId=cn-hangzhou-am24
&spaceStorage=5
```

- Response example

```
{
  "errorMsg":"",
  "return_subCode":"",
  "responseCode":"200",
  "result":"success",
  "requestId":null,
  "data":{
    "successNum":1,
    "instanceId":"[bucket-wine****]",
    "regionId":"cn-hangzhou-am24",
    "requestId":""
  },
  "return_subMsg":"",
  "errorDetail":""
}
```

1.8.2.4. getBucketInfo

Description

Obtains the details of a specified Object Storage Service (OSS) bucket in the cloud platform.

Name

getBucketInfo

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/read/getBucketInfo
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
bucketName	String	Yes	The bucket name

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
data	BucketInfo	A collection of bucket instances. For more information, see BucketInfo.

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/read/getBucketInfo?
regionId=cn-hangzhou-am24
&bucketName=bucket-wine****
```

- Response example

```
{
   "result": "success",
   "data": {
      "createTime": "2016-07-07 20:07:52",
      "bucketName": "bucket-wine****",
      "projectName": "OSSPermissionTestProject2",
      "projectId": "13",
      "expireDate": "",
      "regionId": "cn-hangzhou-am24",
      "departmentId": "2",
      "departmentName": "CloudPlatformDevelopmentDepartment",
      "testEndTime": "",
      "isAliPublic": false,
      "host": "oss-cn-hangzhou-am24-a.dtdream.lab.com"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```


1.8.2.5. checkBucketName

Description

Checks if the bucket name is the same as that of an existing bucket in the cloud platform. Generally, this API is used to check the name before you create a bucket.

Name

checkBucketName

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/manage/checkBucketName
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
departmentId	String	Yes	The department ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
isExist	Boolean	Whether the bucket already exists in the cloud platform

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/manage/checkBucketName?
bucketName=bucket-wine****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "isExist": true
   },
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.8.3. Object-related APIs

1.8.3.1. addNewFolder

Description

Creates a folder in a specified Object Storage Service (OSS) bucket.

If you create a folder, you can classify and archive objects in a more systematic way.

Name

addNewFolder

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/use/addNewFolder
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
folderName	String	Yes	The folder name • The folder path. To create a folder in the root directory, you are only required to enter the folder name. • To create a folder in a sub-directory, you must add its parent directory names of each level before the sub-folder name, starting from the root directory. Parent directory names are separated by forward slashes (/). • The folder name must be 1 to 254 characters in length and can only contain letters, numbers, underscores (_), hyphens (-), and periods (.). It must start with a letter or a number.

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/use/addNewFolder?
bucketName=bucket-wine****
&folderName=hahaha%2Fhehehe
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "errorMsg":"",
   "return_subCode":"",
   "responseCode":"200",
   "result":"success",
   "requestId":null,
   "data":{
      "requestId":""
   },
   "return_subMsg":"",
   "errorDetail":""
}
```

1.8.3.2. deleteObject

Description

Deletes a specified object.

The object cannot be restored after being deleted, so proceed with caution.

Name

deleteObject

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/use/deleteObject
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
key	String	Yes	The file path

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/use/deleteObject?
bucketName=bucket-wine****
&key=Hash.exe
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "data": {},
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.8.3.3. GetObjectList

Description

Obtains the object list in a specified bucket in the cloud platform.

Name

GetObjectList

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/read/GetObjectList
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
filterPrefix	String	No	The path prefix. If it is left empty, the root directory is queried.
netMarker	String	No	The object name. The returned result is an object name list after this object name. See the returned results when you last time requsted this parameter as a reference. For example, the returned result of your last request is a name list from the first to 20th object. This time, when you request this parameter and enters the 10th object name of the last returned result, then the returned result of this request is a name list from the 11th to 30th object.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
netMarker	String	The starting point of the next list
bNextMarker	Boolean	Whether the starting point for the next list exists
rows	ObjectInfo	A collection of objects. For more information, see ObjectInfo.
totalRows	String	The total number of rows in the current query results. At most 20 results are returned for each query.

Examples

- Request example

```
https://api.dtdream.com/gateway/api/cloudOss/read/GetObjectList?
bucketName=bucket-wine****
&filterPrefix=abc%2F
&netMarker=
&regionId=cn-hangzhou-am24
```

- Response example

```
{
"result": "success",
"responseCode": "200",
"data": {
"netMarker": "",
"rows": [
{
"fileName": "abc/",
"fileSize": "0",
"lastModifedDate": "2016-07-08 17:22:43",
"fileType": "Folder"
},
{
"fileName": "abc/WorkOrderProductController.java",
"fileSize": "28026",
"lastModifedDate": "2016-07-08 17:23:35",
"fileType": "java"
},
{
"fileName": "abc/bcd/",
"fileSize": "0",
"fileType": "Folder"
}
],
"totalRows": "3",
"bNextMarker": false
},
"errorMsg": "",
"errorDetail": "",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```


1.8.3.4. getObjectAddress

Description

Obtains the external link address of a specified object.

- The address can be used directly for downloading objects.
- The address is unavailable after the timeout.

Name

getObjectAddress

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/read/getObjectAddress
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
key	String	Yes	The file path
timeOut	String	Yes	The timeout. Value range: 1 to 3600. Unit: second.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
address	String	The external link address of a specific object

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/read/getObjectAddress?
bucketName=bucket-wine****
&key=abc%2FWorkOrderProductController.java
&regionId=cn-hangzhou-am24
&timeOut=3600
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "address": "http://oss-cn-hangzhou-am24-a.dtdream.lab.com/bucket-wine0201/abc/WorkOrderProductController.java?Expires=1470139065&OSSAccessKeyId=FiRP8gpQAQKN****&Signature=LveFx4t/lnlrpU3aV9k4ZoFDp8****"
   },
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```


1.8.3.5. getOssAccessKey

Description

Obtains available AccessKeys in the current Object Storage Service (OSS) bucket.

You can use the obtained AccessKey to manage buckets on the GUI of the third-party OSS client software.

Name

getOssAccessKey

URL

```
{dtcenter_api_url}/gateway/api/cloudOss/use/getOssAccessKey
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
keyId	String	The AccessKey ID
keySecret	String	The AccessKey Secret

Examples

- Request example

```
http://api.dtdream.com/gateway/api/cloudOss/use/getOssAccessKey?
bucketName=bucket-wine****
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "data": {
      "keySecret": "vLPf5Vy5BMKzNSNwZ5*******",
      "keyId": "0INX89xm*********"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.9. VPC-related APIs

1.9.1. createVpc

Description

Creates Virtual Private Cloud (VPC) in the cloud platform.

If the region type is *regft*, the Classless Inter-Domain Routing (CIDR) block is required. To obtain the CIDR block parameters, use the getVpcNetworkSegment API.

Name

createVpc

URL

```
{dtcenter_api_url}/gateway/api/vpcs/
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
vpcName	String	Yes	The VPC name, which must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). It must start with a letter in uppercase or lowercase.
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API
description	String	No	The description. If it is left empty, the VPC does not have a description. By default, the value is empty. The description must be 2 to 256 characters in length and contain letters, but must not start with `http://` or `https://`.
cidrBlock	String	No	The CIDR block
reservedType	String	No	The reserved type, which can be left empty. The default value is *normal*.
externalGateway	Boolean	No	Whether an external gateway exists

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID
vpcId	String	The ID of the newly created VPC
vrouterId	String	The VRouter ID of VPC
routerTableId	String	The route table ID of VPC

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vpcs/?
cidrBlock=192.168.0.0%2F16
&departmentId=10
&description=
&externalGateway=false
&regionId=cn-hangzhou-am24
&userName=
&vpcName=zy-test
```

- Response example

```
{
   "result": "success",
   "data": {
      "requestId": "6A8CC56A-4E8A-4FEB-B81C-25D076B3D68A",
      "vpcId": "vpc-883m4****"
      "vrouterId ": "vrt-883m4****",
      "routerTableId": "vtb-883m4y1de"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.9.2. deleteVpc

Description

Deletes a specified Virtual Private Cloud (VPC) in the cloud platform.

VPC must exist in the cloud platform.

Name

deleteVpc

URL

```
{dtcenter_api_url}/gateway/api/vpcs/{vpcId}
```

Request type

DELETE method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
vpcId	String	Yes	The ID of VPC to be deleted

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vpcs/vpc-88mnxzmyo
```

- Response example

```
{
   "result": "success",
   "data": {
      "requestId": "0176DE9E-6B17-430D-89C9-F63A1462C13E"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.9.3. modifyVpc

Description

Modifies the attributes of a specified Virtual Private Cloud (VPC).

The region must be the one where VPC resides, which can be obtained by using the getVpcs API.

Name

modifyVpc

URL

```
{dtcenter_api_url}/gateway/api/vpcs/{vpcId}/
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
vpcId	String	Yes	The VPC ID
vpcName	String	Yes	The modified VPC name, which must be 2 to 128 characters in length and start with a letter in uppercase or lowercase. The name can contain letters, numbers, underscores (_), and hyphens (-). The system displays the modified VPC name in the console.
regionId	String	Yes	The region ID
description	String	No	The modified description, which must be 2 to 256 characters in length and can contain letters, but must not start with `http://` or `https://`

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vpcs/vpc-88f3j7a0j/?
description=dsadsa
&regionId=cn-hangzhou-am24
&vpcName=wqd-test
```

- Response example

```
{
   "result": "success",
   "data": {
      "requestId": "3F2E77CB-6CCD-4253-A840-1176CAEEDD56"
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.9.4. getVpcs

Description

Obtains the Virtual Private Cloud (VPC) list. You can filter VPCs by region, department, status, VPC ID, and VPC name, have the results displayed on pages, and sort the results.

- The status only supports *Available* (available) and *Invailable* (unavailable).
- This API supports sorting VPCs by regionId (region ID), vpcId (VPC ID), vpcName (VPC name), cidrBlock (Classless Inter-Domain Routing (CIDR) block), and creationTime (created time).
- The sorting order is controlled by the field orderAsc.
- Select whether to synchronize the VPC status when obtaining the VPC list.

Name

getVpcs

URL

```
{dtcenter_api_url}/gateway/api/vpcs/read/getVpcs
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
departmentId	String	No	The department ID used to filter VPCs, which can be obtained by using the getDeptRootTree API. The default value is empty.
regionId	String	No	The region ID used to filter VPCs, which can be obtained by using the getRegionList API. The default value is empty.
vpcStatus	String	No	The VPC status, which is empty by default Values: • *Available*: available • *Invailable*: unavailable
vpcId	String	No	The VPC ID used to filter VPCs, which is empty by default
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100
orderBy	String	No	Obtains the keyword of sorting order Values: • *vpcId*: the VPC ID • *regionId*: the region ID • *vpcName*: the VPC name • *creationTime*: the created time • *cidrBlock*: the CIDR block
orderAsc	Boolean	No	Obtains the sorting order of data Values: • *true*: ascending order • *false*: descending order
vpcName	String	No	The VPC name used to filter VPCs
needSync	Boolean	No	Whether to trigger synchronization when obtaining data Values: • *true*: Trigger the synchronization (default value). • *false*: Do not trigger the synchronization.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
total	Long	The total number of rows
data	string	A collection of VPC instances. For more information, see VpcEntity.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vpcs/read/getVpcs?
departmentId=2
&pageNum=1
&pageSize=10
&regionId=
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": {
    "result": [
      {
        "vpcId": "vpc-884ln****",
        "status": "Available",
        "vpcName": "zy-test1",
        "creationTime": "2016-07-22 09:34:13",
        "cidrBlock": "10.0.XX.XX/8",
        "vRouterId": "vrt-88wva****",
        "departmentName": "DoNotUseThisDepartment",
        "departmentId": "2",
        "description": "ggg",
        "vSwitchCount": 5,
        "extNetworkId": "",
        "extNetworkName": "",
        "defaultSGId": "",
        "regionId": "cn-hangzhou-am24",
        "regionType": "regft",
        "regionName": "ApsaraStack",
        "reservedType": "",
        "externalGateway": false
      }
    ],
    "total": 23
  },
  "errorMsg": "",
  "errorDetail": "",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```


1.9.5. getVpcById

Description

Obtains the details of a specified Virtual Private Cloud (VPC).

VPC must exist in the cloud platform.

Name

getVpcById

URL

```
{dtcenter_api_url}/gateway/api/vpcs/read/{vpcId}
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
vpcId	String	Yes	The VPC ID, which can be obtained by using the getVpcs API

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
result	VpcDetailInfo	A collection of VPC details. For more information, see VpcDetailInfo.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vpcs/read/vpc-88f3j7a0j
```

- Response example

```
{
  "result": "success",
  "data": {
    "result": {
      "vpcId": "vpc-88f3j****",
      "departmentId": 2,
      "departmentName": "CloudPlatformDevelopmentDepartment",
      "cidrBlock": "192.168.XX.XX/16",
      "creationTime": "2016-06-15 15:58:57",
      "description": "",
      "vpcName": "wqd-test",
      "regionId": "cn-hangzhou-am24",
      "status": "Available",
      "vSwitchCount": 1,
      "vRouterId": "vrt-88tsz****"
    }
  },
  "errorMsg": "",
  "errorDetail": "",
  "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```


1.9.6. getVpcNetworkSegment

Description

Obtains the available Classless Inter-Domain Routing (CIDR) blocks of a specified region.

Use the getRegionList API to obtain the region information.

Name

getVpcNetworkSegment

URL

```
{dtcenter_api_url}/gateway/api/vpcs/getVpcNetworkSegment
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The ID of the region where Virtual Private Cloud (VPC) resides

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
cidrBlocks	JSONArray	A collection of available CIDR blocks
total	Integer	The total number of rows

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vpcs/getVpcNetworkSegment?
regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result": "success",
   "data": {
      "total": 4,
      "cidrBlocks": [
         "100.64.XX.XX/10",
         "192.168.XX.XX/16",
         "10.0.XX.XX/8",
         "172.16.XX.XX/13"
      ]
   },
   "errorMsg": "",
   "errorDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```


1.9.7. VSwitch-related APIs

1.9.7.1. createVswitch

Description

Creates a VSwitch in a specified Virtual Private Cloud (VPC).

- The region must be the one where VPC resides, which can be obtained by using the getVpcs API.
- The zone must be in the selected region, which can be obtained by using the getZoneList API.
- The VSwitch Classless Inter-Domain Routing (CIDR) block must belong to the CIDR block of VPC where the VSwitch resides.
- The VSwitch CIDR block can be the same as the CIDR block of VPC where the VSwitch resides, but this indicates that VPC can only have one VSwitch.
- The VSwitch CIDR block cannot be the same as the DestCIDRBlock of the current RouteEntry of VPC where VSwitch resides.
- The VSwitch CIDR block cannot include the DestCIDRBlock of the current RouteEntry of VPC where VSwitch resides, but can be the subset of this DestCIDRBlock.

Name

createVswitch

URL

```
{dtcenter_api_url}/gateway/api/vswitchs
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
vpcId	String	Yes	The VPC ID
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
zoneId	String	Yes	The zone ID
cidrBlock	String	Yes	The CIDR block
vSwitchName	String	Yes	The VSwitch name, which must be 2 to 128 characters in length and start with a letter in uppercase or lowercase. It can contain letters, numbers, underscores (_), and hyphens (-). The system displays the name in the console.
description	String	No	The VSwitch description, which must be 2 to 256 characters in length. If it is left empty, the VSwitch does not have a description. By default, the value is empty.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID
vSwitchId	String	The ID of the newly created VSwitch

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vswitchs?
cidrBlock=10.213.XX.XX%2F24
&description=
&regionId=cn-hangzhou-am24
&vSwitchName=fdajgh
&vpcId=vpc-884l****
&zoneId=cn-hangzhou-hsd-am24001-a
```

- Response example

```
{
   "result": "success",
   "data": {
      "requestId": "99075267-8F57-48F5-A857-9FBC5AC69B3E",
      "vSwitchId": "vsw-8805x****"
   },
   "errorMsg": "",
   "errDetail": "",
   "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.9.7.2. deleteVswitch

Description

Deletes a specified VSwitch.

The region must be the one where the VSwitch resides.

Name

deleteVswitch

URL

```
{dtcenter_api_url}/gateway/api/vswitchs/{vSwitchId}
```

Request type

DELETE method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
vSwitchId	String	Yes	The VSwitch ID
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
vSwitchName	String	Yes	The VSwitch name
departmentId	String	Yes	The department ID, which can be obtained by using the getDeptRootTree API. The department must be the one that has the Virtual Private Cloud (VPC) where the VSwitch resides.

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vswitchs/vsw-88wd6x9p8?
regionId=cn-hangzhou-am24
&vSwitchName=fdajgh
&departmentId=2
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "requestId": "E1E56256-032E-4251-8D2A-241EC1999635"
   },
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```


1.9.7.3. modifyVswitch

Description

Modifies the attributes of a specified VSwitch.

The region must be the one where the VSwitch resides.

Name

modifyVswitch

URL

```
{dtcenter_api_url}/gateway/api/vswitchs/{vSwitchId}
```

Request type

POST method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
vSwitchId	String	Yes	The VSwitch ID
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API

Name	Type	Required	Description
vSwitch Name	String	Yes	The VSwitch name. If it is left empty, the VSwitch does not have a name. By default, the value is empty. The name, which must be 2 to 128 characters in length and start with a letter in uppercase or lowercase, can contain letters, numbers, underscores (_), and hyphens (-). The system displays the name in the console.
description	String	Yes	The modified VSwitch description. If it is left empty, the VSwitch does not have a description. By default, the value is empty. The description must be 2 to 256 characters in length.
departmentId	String	Yes	The ID of the department where the VSwitch to be modified resides

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
requestId	String	The request ID

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vswitchs/vsw-8805xdpqn
? departmentId=2
&description=fdsgds
&regionId=cn-hangzhou-am24
&vSwitchName=hghfh
```

- Response example

```
{
   "result": "success",
   "responseCode": "200",
   "data": {
      "requestId": "CB8990AC-1F68-40CA-BF20-55953B1456AC"
   },
   "errorMsg": "",
   "errorDetail": "",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.9.7.4. getVswitchList

Description

Obtains the VSwitch list in a specified Virtual Private Cloud (VPC).

The region must be the one where VPC resides, which can be obtained by using the getZoneList API.

Name

getVswitchList

URL

```
{dtcenter_api_url}/gateway/api/vswitchs/read/vpcs/{vpcId}
```

Request type

GET method.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID, which can be obtained by using the getRegionList API
vpcId	String	Yes	The VPC ID
zoneId	String	No	The zone ID
departmentId	String	Yes	The department ID

Response parameters

For more information about the common response values, see Response structure.

Name	Type	Description
result	String	A collection of VSwitch instances. For more information, see VswitchEntity - Alibaba Cloud regions.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/vswitchs/read/vpcs/vpc-884lnnm4w?
regionId=cn-hangzhou-am24
&departmentId=2
```

- Response example

```
{
  "result": "success",
  "data": {
    "result": [
      {
        "zoneId": "cn-hangzhou-hsd-am24001-a",
        "zoneName": "cn-hangzhou-hsd-am24001-a",
        "vpcId": "vpc-88f3j****",
        "vSwitchId": "vsw-88wbq****",
        "vSwitchName": "wqd_test",
        "status": "Available",
        "cidrBlock": "192.168.XX.XX/16",
        "description": "",
        "createTime": "2016-06-15 15:59:43"
      }
    ]
  },
  "errorMsg": "",
  "errorDetail": "",
  "responseCode": "200",
"return_subCode": "",
"return_subMsg": "",
"requestId": null
}
```

1.10. Monitoring center-related APIs

1.10.1. ECS monitoring-related APIs

1.10.1.1. InstallEcsCmsAgent

Description

Installs the Elastic Compute Service (ECS) monitoring plug-in.

Name

InstallEcsCmsAgent

URL

{dtcenter_api_url}/gateway/api/monitor/use/installEcsCmsAgent

Request type

POST message.

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
instanceIdList	List<String>	Yes	A collection of IDs for instances where plug-in installation is required

Response parameters

For more information about the common response values, see Response structure.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/monitor/use/installEcsCmsAgent? instanceIdList=i-88hmgk15o,i-885ngupv
```

- Response example

```
{
"result":"success",
"responseCode":"200",
"data":"",
"errorMsg":"",
"errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```

1.10.1.2. getMonitorHistory

Description

Obtains the historical monitoring data of an Elastic Compute Service (ECS) instance.

Name

getMonitorHistory

URL

{dtcenter_api_url}/gateway/api/monitorecs/history/monitor

Request type

GET message.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID
instanceId	String	Yes	The instance ID
monitorItem	String	Yes	The monitoring item. For more information about the details, see the description of monitoring items in Apsara CloudMonitor.
monitorTime	String	Yes	The sampling interval of the history monitoring data, which is valued as numbers. Unit: hour.

Response parameters

Name	Type	Description
monitorData	Map<String,Array>	The monitoring data of the monitoring item, such as the monitoring data of CPU utilization at each time point

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/monitorecs/history/monitor?
regionId=424f5a39-ec0b-441f-8f71-26b12ba496ea
&instanceId=0adbdd81-2aa2-497c-b943-955a131e****
&monitorItem=CPUUtilization
&monitorTime=2
```

- Response example

```
{
"result":"success",
"responseCode":"200",
"data":{
"monitorData":{ "CPU":[ [1480049851000, 0.11], [1480050151000, 0.112], [1480050451000, 0.112], [14800507
51000, 0.111] ]}
},
"errorMsg":"",
"errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```


1.10.1.3. getMonitorCurrent

Description

Obtains the real-time monitoring data of Elastic Compute Service (ECS).

Name

getMonitorCurrent

URL

`{dtcenter_api_url}/gateway/api/monitorecs/current/monitor`

Request type

GET

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	No	The region ID
departmentId	String	No	The department ID
instanceId	String	No	The instance ID
instanceName	String	No	The instance name

Name	Type	Required	Description
instanceStatus	String	No	The instance status Values: • *Running*: running • *Stopped*: stopped • *starting*: starting • *stopping*: stopping • *taskCreating*: creating the task • *taskDeleting*: deleting the task • *Pending*: pending
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not specified, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not specified, all data is obtained. Value range: 1 to 100

Response parameters

Name	Type	Discription
regionId	String	The region ID
regionName	String	The region name
instanceId	String	The instance ID
departmentId	String	The department ID
departmentName	String	The department name
instanceName	String	The instance name

Name	Type	Discription
instanceStatus	String	The instance status Values: • *Running*: running • *Stopped*: stopped • *starting*: starting • *stopping*: stopping • *taskCreating*: creating the task • *taskDeleting*: deleting the tsak • *Pending*: Pending
cpuUtilization	double	The CPU utilization (%)
memoryUtilization	double	The memory utilization (%)
diskUtilization	double	The disk utilization (%)
internetRx	double	The inbound traffic (Kbps)
InternetTx	double	The outbound traffic (Kbps)
bpsRead	double	The disk read bandwidth (KB/s)
bpsWrite	double	The disk write bandwidth (KB/s)
regionType	String	The region type
projectId	String	The project ID
projectName	String	The project name
agentStatus	String	The plug-in status Value: *running*: running **Note** This field is only supported by CDU.

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/monitorecs/current/monitor?
departmentId=4
&regionId=cn-hangzhou-am24
&instanceName=aaaa
&pageNum=1
&pageSize=10
```

- Response example

```
{
    "result": "success",
    "responseCode": "200",
    "data": {
      "pageSize": 10,
      "totalRows": 1,
      "rows":[
            {
              "agentStatus":"Running",
              "bpsRead":0,
              "bpsWrite":0,
              "cpuUtilization":0.125,
              "departmentId":"2",
              "departmentName":"Department",
              "diskUtilization":0,
              "instanceId":"0adbdd81-2aa2-497c-b943-955a131e****",
              "instanceName":"sswResource****",
              "internetRx":0,
              "internetTx":0,
              "memoryUtilization":0,
              "projectId":"78",
              "projectName":"wangyaochong",
              "regionId":"cn-hangzhou-am24",
              "regionName":"cn-hangzhou-am24",
              "regionType":"regft",
              "instanceStatus":"Running"

      }
       ],
       "pageNum": 1
    },
    "errorMsg": "",
    "errorDetail": ""
}
```


1.10.2. OSS monitoring-related APIs

1.10.2.1. GetMonitorHistory

Description

Obtains the historical monitoring data of Object Storage Service (OSS).

Name

GetMonitorHistory

URL

{dtcenter_api_url}/gateway/api/monitoross/history/monitor

Request type

GET

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
bucketName	String	Yes	The bucket name
monitorItem	String	Yes	The monitoring item. For more information about the details, see the description of monitoring items in Apsara CloudMonitor.
monitorTime	String	Yes	The sampling interval of the history monitoring data, which is valued as numbers. Unit: hour.
regionId	String	Yes	The region ID

Response parameters

Name	Type	Description
monitorData	Map<String,Array>	The monitoring data of the monitoring item, such as the monitoring data of internal errors at each time point

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/monitoross/history/monitor?
bucketName=aaaa1
&monitorItem=InternalError
&monitorTime=6
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result":"success",
   "responseCode":"200",
   "data":{
         "monitorData":{ "InternalError":[ [1480049851000, 3], [1480050151000, 4], [1480050451000, 1], [148
0050751000, 0] ]}
        },
   "errorMsg":"",
   "errorDetail":"",
"return_subCode" : "",
"return_subMsg" : ""
}
```

1.10.2.2. getMonitorCurrent

Description

Obtains the real-time monitoring data of Object Storage Service (OSS).

Name

getMonitorCurrent

URL

`{dtcenter_api_url}/gateway/api/monitoross/current/monitor`

Request type

GET

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
departmentId	String	No	The department ID

Name	Type	Required	Description
bucketName	String	No	The bucket name
regionId	String	No	The region ID
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100
orderBy	String	No	The keyword used to sort the data. For example, if the value orderBy is bucketName, data is sorted by OSS bucket name.
orderAsc	Boolean	No	Whether the result is sorted in ascending order: • *true*: ascending order • *false*: descending order

Response parameters

Name	Type	Description
bucketName	String	The bucket name
regionId	String	The region ID
projectId	String	The project ID
projectName	String	The project name
departmentName	String	The department name

Name	Type	Description
departmentId	String	The department ID
getRequest	Integer	The number of reads (time)
internalError	Integer	The number of internal errors
internetTX	double	The outbound traffic of Internet (byte)
internetRX	double	The inbound traffic of Internet (byte)
intranetRX	double	The inbound traffic of intranet (byte)
intranetTX	double	The outbound traffic of intranet (byte)
putRequest	Integer	The number of writes (time)
storageUtilization	double	The used storage space (byte)

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/monitoross/read/oss?bucketName =a****
&departmentId=1
&regionId=cn-hangzhou-am24
&pageNum=1
&pageSize=25
&orderBy=bucketName
&orderAsc=true
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": {
    "pageSize": 10,
    "totalRows": 1,
    "rows": [
          {
            "bucketName":"a****",
            "departmentName":"DoNotUseThisDepartment",
            "departmentId":2,
            "getRequest":0,
            "internalError":0,
            "internetRX":0,
            "internetTX":0,
            "intranetRX":0,
            "intranetTX":0,
            "projectId":"2",
            "projectName":"test",
            "putRequest":0,
            "regionId":"cn-hangzhou-am24",
            "storageUtilization":0
          }
    ],
    "pageNum": 1
  },
  "errorMsg": "",
  "errorDetail": ""
}
```


1.10.3. RDS monitoring-related APIs

1.10.3.1. getMonitorHistory

Description

Obtains the historical monitoring data of an ApsaraDB for RDS instance.

Name

getMonitorHistory

URL

{dtcenter_api_url}/gateway/api/monitorrds/history/monitor

Request type

GET

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	Yes	The region ID
instanceName	String	Yes	The instance name
monitorItem	String	Yes	The monitoring item. For more information about the details, see the description of monitoring items in Apsara CloudMonitor.
monitorTime	String	Yes	The sampling interval of the history monitoring data, which is valued as numbers. Unit: hour.
departmenId	String	No	The department ID

Response parameters

Name	Type	Description
monitorData	Map<String,Array>	The monitoring data of the monitoring item, such as the monitoring data of disk usage at each time point

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/monitorrds/history/monitor?
instanceName=rdsx35i180uyq726****
&monitorItem=DiskUsage
&monitorTime=2
&regionId=cn-hangzhou-am24
```

- Response example

```
{
   "result":"success",
   "responseCode":"200",
   "data":{
         "monitorData":{ "DiskUsage":[ [1480056000000, 10.1], [1480056300000, 10.1], [1480056600000, 10.
1], [1480056900000, 10.1] ]}
        },
   "errorMsg":"",
   "errorDetail":"",
"return_subCode": "",
"return_subMsg": ""
}
```


1.10.3.2. getMonitorCurrent

Description

Obtains the real-time monitoring data of an ApsaraDB for RDS instance.

Name

getMonitorCurrent

URL

`{dtcenter_api_url}/gateway/api/monitorrds/current/monitor`

Request type

GET

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	No	The region ID
departmentId	String	No	The department ID
instanceId	String	No	The ID of the ApsaraDB for RDS instance
instanceName	String	No	The name of the ApsaraDB for RDS instance

Name	Type	Required	Description
projectName	String	No	The project name

Name	Type	Required	Description
instanceStatus	String	No	The status of the ApsaraDB for RDS instance, which is empty by default Values: • *Creating*: creating • *Running*: running • *Stopped*: stopped • *Deleting*: deleting • *Rebooting*: rebooting • *DBInstanceClassChanging*: upgrading and degrading • *TRANSING*: migrating • *EngineVersionUpgrading*: migrating the version • *TransingToOthers*: migrating data to other ApsaraDB for RDS instances • *GuardDBInstanceCreating*: creating the disaster recovery instance • *Restoring*: restoring • *Importing*: importing data • *ImportingFromOthers*: importing data from other ApsaraDB for RDS instances • *DBInstanceNetTypeChanging*: swtiching internal and public network • *GuardSwitching*: switching the disaster recovery • *TempDBInstance_Creating*: creating temporary instances • *LingSwitching*: switching access mode

Name	Type	Required	Description
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100
orderBy	String	No	The keyword used to sort the data. For example, if the value is instanceName, data is sorted by the name of the ApsaraDB for RDS instance.
orderAsc	Boolean	No	Whether the results are sorted in an ascending order: • *true*: ascending order • *false*: descending order

Response parameters

Name	Type	Description
cpuUtilization	double	The CPU utilization
departmentId	String	The department ID
departmentName	String	The department name
databaseType	String	The database type
instanceId	String	The ID of the ApsaraDB for RDS instance
instanceName	String	The name of the ApsaraDB for RDS instance

Name	Type	Description
iopsUtilization	double	The IOPS utilization
memoryUtilization	double	The memory utilization
projectId	String	The project ID
projectName	String	The project name
regionId	String	The region ID
regionName	String	The region name
regionType	String	The region type
sessions	Integer	The number of sessions
spaceUsage	double	The space usage

Name	Type	Description
instanceStatus	String	The status of the ApsaraDB for RDS instance Values: • *Creating*: creating • *Running*: running • *Stopped*: stopped • *Deleting*: deleting • *Rebooting*: rebooting • *DBInstanceClassChanging*: upgrading and degrading • *TRANSING*: migrating • *EngineVersionUpgrading*: upgrading the version • *TransingToOthers*: migrating data to other ApsaraDB for RDS instances • *GuardDBInstanceCreating*: creating the disaster recovery instance • *Restoring*: restoring • *Importing*: importing data • *ImportingFromOthers*: importing data from other ApsaraDB for RDS instances • *DBInstanceNetTypeChanging* : swtiching internal and public network • *GuardSwitching*: switching the disaster recovery • *TempDBInstance_Creating*: creating temporary instances • *LingSwitching*: switching access mode

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/monitorrds/current/monitor?departmentId=1
&regionId=cn-hangzhou-am24
&pageIndex=1
&pageSize=10
&orderBy=instanceName
&orderAsc=true
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": {
    "pageSize": 10,
    "totalRows": 1,
    "rows": [
          {
           "cpuUtilization":0,
           "departmentId":"25",
           "departmentName":"asdf",
           "databaseType":"MySQL",
           "instanceId":"rds1ws99139t1n3k****",
           "instanceName":"t***",
           "iopsUtilization":0,
           "memoryUtilization":26.7,
           "netTraffic":0,
           "projectId":"35",
           "projectName":"tt",
           "regionId":"cn-hangzhou-am24",
           "regionName":"ApsaraStack",
           "regionType":"",
           "sessions":0,
           "spaceUsage":10.1,
           "instanceStatus":"Running"
          }
    ],
    "pageNum": 1
  },
  "errorMsg": "",
  "errorDetail": ""
}
```


1.10.4. SLB monitoring-related APIs

1.10.4.1. getMonitorHistory

Description

Obtains the historical monitoring data of Server Load Balancer (SLB).

Name

getMonitorHistory

URL

{dtcenter_api_url}/gateway/api/monitorslb/history/monitor

Request type

GET

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
instanceId	String	Yes	The SLB instance ID
port	String	No	The monitoring port
monitorItem	String	Yes	The monitoring item. For more information about the details, see the description of monitoring items in Apsara CloudMonitor.
monitorTime	String	Yes	The sampling interval of the history monitoring data, which is valued as numbers. Unit: hour.
regionId	String	Yes	The region ID
regionType	String	Yes	The region type Value: *regft*(Apsara Stack regions)
departmentId	String	No	The department ID

Response parameters

Name	Type	Description
monitorData	Map<String,Array>	The monitoring data of the monitoring item, such as the monitoring data of the number of outbound data packages at each time point

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/monitorslb/history/monitor?
instanceId=1580e5c7c9c-cn-hangzhou-****
&monitorItem=PacketTX
&monitorTime=2
&port=100
&regionId=cn-hangzhou-am24
&regionType=regft
```

- Response example

```
{
   "result":"success",
   "responseCode":"200",
   "data":{
         "monitorData":{ "PacketTX":[ [1480057500000, 0], [1480057560000, 0], [1480057620000, 0], [148005
7680000, 0], [1480057740000, 0] ]}
        },
   "errorMsg":"",
   "errorDetail":"",
"return_subCode” : "",
"return_subMsg” : ""
}
```

1.10.4.2. getMonitorCurrent

Description

Obtains the real-time monitoring data of a Server Load Balancer (SLB) instance.

Name

getMonitorCurrent

URL

```
{dtcenter_api_url}/gateway/api/monitorslb/current/monitor
```

Request type

GET

Request headers

For more information about the common headers, see Common parameters.

Request parameters

Name	Type	Required	Description
regionId	String	No	The region ID
departmentId	String	No	The department ID
slbId	String	No	The SLB instance ID
slbName	String	No	The SLB instance name
projectName	String	No	The project name
slbStatus	String	No	The SLB instance status, which is empty by default Values: • *Running*: running • *Stopped*: stopped
pageNum	Integer	No	The page number in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 65535
pageSize	Integer	No	The number of rows on each page in a paged query. You must specify pageSize and pageNum at the same time. If not, all data is obtained. Value range: 1 to 100
orderBy	String	No	The keyword used to sort the data. For example, if the value orderBy is slbName, data is sorted by SLB instance name.
orderAsc	Boolean	No	Whether the result is sorted in ascending order: • *true*: ascending order • *false*: descending order
instanceIpAddress	String	No	The service address

Response parameters

Name	Type	Description
activeConnectNum	Double	The number of active connections
departmentId	String	The department ID
inActiveConnectNum	Double	The number of inactive connections
inFlowRate	Double	The inbound data volume per second (kbps)
inPacketRate	Double	The number of inbound data packages per second
newConnectNum	Double	The number of newly created connections
outFlowRate	Double	The outbound data volume per second (kbps)
outPacketRate	Double	The number of outbound data packages per second
projectId	String	The project ID
projectName	String	The project name
regionId	String	The region ID
regionName	String	The region name
serviceIpAddress	String	The service address
slbId	String	The SLB instance ID
slbName	String	The SLB instance name
slbStatus	String	The SLB instance status Values: • *Running*: running • *Stopped*: stopped
port	String	The monitoring port
protocol	String	The monitoring protocol

Examples

- Request example

```
http://apigateway.dtdream.com/gateway/api/monitorslb/current/monitor?
&pageNum=1
&pageSize=10
&orderBy=slbName
&orderAsc=true
```

- Response example

```
{
  "result": "success",
  "responseCode": "200",
  "data": {
    "pageSize": 10,
    "totalRows": 1,
    "rows": [
          {
            "activeConnectNum":0,
            "departmentName":"EastDawning1",
            "departmentId":"510",
            "inActiveConnectNum":0,
            "inFlowRate":0,
            "inPacketRate":0,
            "instanceId":"1580e5c7c9c-cn-hangzhou-****",
            "instanceName":"loadBala****",
            "newConnectNum":0,
            "outFlowRate":0,
            "outPacketRate":0,
            "projectId":"58",
            "projectName":"dongfangjiabai",
            "regionId":"cn-hangzhou-am24",
            "serviceIpAddress":"172.31.XX.XX",
            "slbId":"1580e5c7c9c-cn-hangzhou-am24",
            "slbStatus":"Running",
            "port":"100",
            "protocol":"http"
          }
    ],
    "pageNum": 1
  },
  "errorMsg": "",
  "errorDetail": ""
}
```


1.11. Data type

1.11.1. RDS data types

1.11.1.1. DBInstanceAttribute

The attribute information of an ApsaraDB for RDS instance.

Name	Type	Description
dBInstanceId	String	The instance ID
dBInstanceName	String	The instance name
dBInstanceType	String	The instance type • *Primary*: primary instance • *Readonly*: read-only instance • *Temp*: temporary instance
instanceNetworkType	String	The network type • *Classic*: classic network • *VPC*: Virtual Private Cloud
regionId	String	The region ID
zoneId	String	The zone ID
departmentId	Long	The department ID
projectId	Long	The project ID
connectionString	String	The connection address
port	Integer	The connection port
engine	String	The database type
engineVersion	String	The database version
dBInstanceClass	String	The instance type
dBInstanceMemory	Integer	The instance memory. Unit: MB.
dBInstanceStorage	Integer	The instance storage. Unit: GB.
dBInstanceStatus	String	The instance status. For more information, see DBInstanceStatus.
lockMode	String	• *Unlock*: normal • *LockByDiskQuota*: If the storage space of an instance is used up, the instance is automatically locked.
lockReason	String	The reason why an instance is locked
dBMaxQuantity	Integer	The maximum number of databases that can be created in an instance

Name	Type	Description
accountMaxQuantity	Integer	The maximum number of accounts that can be created
creationTime	String	The created time Format: YYYY-MMDD'T'hh:mm:ssZ. For example, 2011-05-30T12:11:4Z.
availabilityValue	String	Query the availability status of available instances in the current year Unit: percentage
maxIOPS	Integer	The maximum number of I/O requests, that is, IOPS
maxConnections	Integer	The maximum number of concurrent connections of an instance
masterInstanceId	String	The primary instance ID. If this parameter is not returned (that is, the value is null), this instance is the primary instance.
tempDBInstanceId	String	The ID of temporary instances
readOnlyDBInstanceIds	List<ReadOnlyDBInstanceId>	The ID list of read-only instances that are mounted under the master instance
connectionMode	String	The access mode *Performance*is the standard access mode. *Safety* is the highly secure access mode.
vpcid	String	The VPC ID
vip	String	The IP address and port number
testTime	String	The test deadline
diskUsed	Long	The space used by an ApsaraDB for RDS instance
backupSize	Long	The space used by the backup of an ApsaraDB for RDS instance
dataDiskSize	Long	The space used by data files of an ApsaraDB for RDS instance
logDiskSize	Long	The space used by logs of an ApsaraDB for RDS instance

1.11.1.2. DBInstanceEntity

The basic information of an ApsaraDB for RDS instance.

Name	Type	Description
dBInstanceId	String	The instance ID
dBInstanceName	String	The instance name
departmentId	String	The department ID
departmentName	String	The department name
projectId	String	The project ID
projectName	String	The project name
dBInstanceType	String	The instance type *Primary*: the primary instance *ReadOnly*: the read-only instance *Temp*: the temporary instance
regionId	String	The region ID
regionName	Sring	The region name
regionType	String	The region type
dBInstanceStatus	String	The instance status. For more information, see DBInstanceStatus.
engine	String	The database type
engineVersion	String	The database version
maxIOPS	Integer	The maximum number of I/O requests, that is, IOPS
dBInstanceStorage	Integer	The instance storage Unit: GB
dBInstanceMemory	Integer	The instance memory Unit: MB
maxConnections	Integer	The maximum number of concurrent connections of an instance
expireDate	String	The expiry date of an instance
zoneId	String	The zone ID

Name	Type	Description
lockMode	String	*Unlock*: normal *LockByDiskQuota*: If the storage space of an instance is used up, the instance is automatically locked.
dBInstanceCreateTime	String	The created time of the instance
networkType	String	The network type of the instance Values: • *Classic*: classic network • *VPC*: Virtual Private Cloud

1.11.1.3. DBInstanceNetInfo

The network information of an ApsaraDB for RDS instance.

Name	Type	Description
ConnectionString	String	The Domain Name System (DNS) connection string
IPAddress	String	The IP address
Port	Integer	The port information
VPCId	String	The Virtual Private Cloud (VPC) ID
VSwitchId	String	The VSwitch ID

1.11.1.4. DBInstanceStatus

The status list of an ApsaraDB for RDS instance.

Status	Description
Creating	Creating
Running	Running
Deleting	Deleting
Rebooting	Restarting
DBInstanceClassChanging	Upgrading/downgrading
TRANSING	Migrating
Restoring	Restoring the backup

Status	Description
TransingToOthers	Migrating data to other RDS databases

1.11.1.5. ReadOnlyDBInstanceId

The read-only instance ID.

Name	Type	Description
dBInstanceId	String	The read-only instance ID

1.11.1.6. DBDatabaseEntity

The ApsaraDB for RDS database information.

Name	Type	Description
dBInstanceId	String	The ID of the instance to which the database belongs
engine	String	The database instance type
dBName	String	The database name
dBStatus	String	The database status *Creating*: creating *Running*: running *Deleting*: deleting
characterSetName	String	The character set
dBDescription	String	The database description
accounts	List<DBAccountPrivilegeInfo>	A list of accounts

1.11.1.7. DBAccountPrivilegeInfo

The permission information of an ApsaraDB for RDS database.

Name	Type	Description
Account	String	The account name
AccountPrivilege	String	The permissions that the account has to the database

1.11.1.8. DBAccountEntity

The ApsaraDB for RDS account information.

Name	Type	Description
dBInstanceId	String	The ID of the instance to which the database belongs
accountName	String	The account name
accountStatus	String	The account status *Unavailable*: unavailable *Available*: available
accountDescription	String	The account description
databasePrivileges	List<DatabasePrivilege>	An array composed of DatabasePrivileges

1.11.1.9. DBDatabasePrivilege

The permission information of an ApsaraDB for RDS account.

Name	Type	Description
DBName	String	The database name
AccountPrivilege	String	The permissions that the account has

1.11.1.10. DatabasePrivilege

The database permission information of an ApsaraDB for RDS account.

Name	Type	Description
DBName	String	The database name
AccountPrivilege	String	The permissions that the account has to the database

1.11.2. OSS data types

1.11.2.1. BucketEntity

The attribute information of a bucket.

Name	Type	Description
createDate	String	The created time
createTimeStamp	Long	The timestamp of the created time
departmentId	String	The department ID

Name	Type	Description
departmentName	String	The department name
instanceName	String	The bucket name
projectId	String	The project ID
projectName	String	The project name
regionId	String	The region ID
storeSpace	Long	The bucket capacity. 0 indicates no limitation. Unit: TB.
newStoreSpace	Long	The bucket capacity. 0 indicates no limitation. Unit: GB.
expireDate	String	The expiry date of the resource
isAliType	Boolean	Whether the bucket is in an Apsara Stack regionV alues: • *true*: The bucket is in an Apsara Stack region. • *false*: The bucket is not in an Apsara Stack region.
userId	Long	The user ID
creator	String	The name of the user who creates the bucket

1.11.2.2. BucketInfo

The attribute information of a bucket.

Name	Type	Description
bucketName	String	The bucket name
createTime	String	The created time
departmentId	String	The department ID
departmentName	String	The department name
host	String	The service address
projectId	String	The project ID
projectName	String	The project name
regionId	String	The region ID
testEndTime	String	The test deadline
expireDate	String	The expiry date of the resource

1.11.2.3. ObjectInfo

The attribute information of an object.

Name	Type	Description
fileName	String	The file name
fileType	String	The file type
lastModifedDate	String	The last modified time
fileSize	String	The file size Unit: B

1.11.3. VPC data types

1.11.3.1. NetworkEntity

The attribute information of the instance.

Name	Type	Description
bExtNetwork	Boolean	Whether it is the external network
department	String	The department ID
description	String	The description
dnsServer	String	The DNS server
gateway	String	The gateway
networkId	String	The virtual subnet ID
networkName	String	The virtual subnet name
networkType	String	The virtual subnet type
password	String	The password
regionId	String	The region ID
reservedType	String	The reserved type
routerId	String	The VRouter ID
status	String	The status
subnetId	String	The subnet ID
subnetIp	String	The subnet IP address

Name	Type	Description
userName	String	The username
vlanId	String	The VLAN ID
vpcId	String	The Virtual Private Cloud (VPC) ID
zoneId	String	The zone ID
zoneName	String	The zone name

1.11.3.2. VpcDetailInfo

The attribute information of a Virtual Private Cloud (VPC) instance.

Name	Type	Description
cidrBlock	String	The Classless Inter-Domain Routing (CIDR) block
creationTime	String	The created time
departmentId	String	The ID of the department to which the instance belongs
departmentName	String	The name of the department where the instance resides
description	String	The description
regionId	String	The ID of the region in which the instance resides
status	String	The status
vRouterId	String	The VRouter ID
vSwitchCount	Integer	The number of VSwitches
vpcId	String	The VPC ID
vpcName	String	The VPC name

1.11.3.3. VpcEntity

The attribute information of a Virtual Private Cloud (VPC) instance.

Name	Type	Description
cidrBlock	String	The Classless Inter-Domain Routing (CIDR) block
creationTime	String	The created time
defaultSGId	String	The default security group ID

Name	Type	Description
departmentId	String	The ID of the department to which the instance belongs
departmentName	String	The name of the department to which the instance belongs
description	String	The description
extNetworkId	String	The ID of the external network
extNetworkName	String	The name of the external network
externalGateway	Boolean	Whether it is the external gateway
regionId	String	The ID of the region in which the instance resides
regionName	String	The name of the region in which the instance resides
regionType	String	The type of the region in which the instance resides
reservedType	String	The reserved type
status	String	The status
vRouterId	String	The VRouter ID
vSwitchCount	Integer	The number of VSwitches
vpcId	String	The VPC ID
vpcName	String	The VPC name

1.11.3.4. VrouterDetailInfo

The attribute information of a Virtual Private Cloud (VPC) instance.

Name	Type	Description
regionId	String	The region ID
vpcId	String	The VPC ID
vRouterId	String	The VRouter ID
vRouterName	String	The VRouter name
description	String	The VRouter description
creationTime	String	The created time

1.11.3.5. vrouterRule

The attribute information of a Virtual Private Cloud (VPC) instance.

Name	Type	Description
destinationCidrBlock	String	The destination Classless Inter-Domain Routing (CIDR) block
instanceId	String	The Elastic Compute Service (ECS) instance ID for the next hop
routeTableId	String	The route table ID
status	String	The status
type	String	The route type

1.11.3.6. VswitchEntity - Alibaba Cloud regions

The attribute information of a Virtual Private Cloud (VPC) instance.

Name	Type	Description
zoneId	Boolean	The zone ID
vpcId	String	The VPC ID
vSwitchId	String	The VSwitch ID
vSwitchName	String	The VSwitch name
status	String	The status
cidrBlock	String	The Classless Inter-Domain Routing (CIDR) block
description	String	The description
createTime	String	The created time

1.11.4. User center data types

1.11.4.1. AuthorizationDetail

The attribute information of user authorization.

Name	Type	Description
authId	Long	The AuthorizationDetail ID corresponding to the user
serviceId	Long	The platform ID
serviceName	String	The platform name
loginName	String	The logon name of the user

Name	Type	Description
userId	Long	The user ID
roles	Set<RoleDetail>	A collection of roles. For more information, see RoleDetail.

1.11.4.2. PrivilegeEntity

The attribute information of permissions.

Name	Type	Description
id	Long	The permission ID
name	String	The name of the permission string
cnName	String	The permission name
comment	String	The description of the permission
addTime	Timestamp	The created time
updateTime	Timestamp	The updated time

1.11.4.3. RoleDetail

The attribute information of roles.

Name	Type	Description
roleId	String	The role ID
roleName	String	The role name
privilege	String	The string of permissions that the role has. This API does not provide this parameter value.
service	String	The platform name. This API does not provide this parameter value.
userNum	Integer	The number of users under the role. This API does not provide this parameter value.
level	Integer	The role priority. The smaller the number, the higher the priority. This API does not provide this parameter value.

Name	Type	Description
serviceId	Long	The platform ID. This API does not provide this parameter value.
comment	String	The description of the role. This API does not provide this parameter value.
privilegeList	List<PrivilegeEntity>	An array collection composed of PrivilegeEntity. This API does not provide this parameter value.
isActive	boolean	Whether the role is active
isDefault	boolean	Whether the role is the default role

1.12. Appendix

1.12.1. Apsara resource table

Instance series one

Non-I/O optimized instances

- Non-I/O optimized instances support the following disk types:

  Basic cloud disk

Type classification	instanceType	CPU (Core)	Memory (G)
Tiny	ecs.t1.small	1	1
Standard	ecs.s1.small	1	2
	ecs.s1.medium	1	4
	ecs.s1.large	1	8
	ecs.s2.small	2	2
	ecs.s2.large	2	4
	ecs.s2.xlarge	2	8
	ecs.s2.2xlarge	2	16
	ecs.s3.medium	4	4
	ecs.s3.large	4	8

Type classification	instanceType	CPU (Core)	Memory (G)
High Memory	ecs.m1.medium	4	16
	ecs.m2.medium	4	32
	ecs.m1.xlarge	8	32
High CPU	ecs.c1.small	8	8
	ecs.c1.large	8	16
	ecs.c2.medium	16	16
	ecs.c2.large	16	32
	ecs.c2.xlarge	16	64

- I/O optimized instances: SSD cloud disk and ultra cloud disk.

Type classification	instanceType	CPU (Core)	Memory (G)
Standard	ecs.s2.large	2	4
	ecs.s2.xlarge	2	8
	ecs.s2.2xlarge	2	16
	ecs.s3.medium	4	4
	ecs.s3.large	4	8
High Memory	ecs.m1.medium	4	16
	ecs.m2.medium	4	32
	ecs.m1.xlarge	8	32
High CPU	ecs.c1.small	8	8
	ecs.c1.large	8	16
	ecs.c2.medium	16	16
	ecs.c2.large	16	32
	ecs.c2.xlarge	16	64

Instance series two

Instance series II are all I/O optimized instances that support the following disk types:

- SSD cloud disk
- Ultra cloud disk

Instance type family	instanceType	CPU (Core)	Memory (G)
ecs.n1 (general n1)	ecs.n1.tiny	1	1
	ecs.n1.small	1	2
	ecs.n1.medium	2	4
	ecs.n1.large	4	8
	ecs.n1.xlarge	8	16
	ecs.n1.3xlarge	16	32
	ecs.n1.7xlarge	32	64
ecs.n2 (general n2)	ecs.n2.small	1	4
	ecs.n2.medium	2	8
	ecs.n2.large	4	16
	ecs.n2.xlarge	8	32
	ecs.n2.3xlarge	16	64
	ecs.n2.7xlarge	32	128
ecs.e3 (memory e3)	ecs.e3.small	1	8
	ecs.e3.medium	2	16
	ecs.e3.large	4	32
	ecs.e3.xlarge	8	64
	ecs.e3.3xlarge	16	128

1.12.2. Monitoring metrics in CoudMonitor

ECS monitoring metrics

Metric name	monitorItem	Description	Unit	Remarks
CPU Utilization	CPUUtilization	This metric is used to measure the CPU utilization of a measured object.	%	None

Metric name	monitorItem	Description	Unit	Remarks
Memory Utilization	MemoryUtilization	This metric is used to measure the memory utilization of a measured object.	%	None
Disk I/O Read	DiskIORead	This metric is used to measure the volume of data read from a measured object per second.	KBps	None
Disk I/O Write	DiskIOWrite	This metric is used to measure the volume of data written to a measured object per second.	KBps	None
Disk Utilization	DiskUtilization	This metric is used to measure the disk utilization of a measured object.	%	None
Inbound Traffic	InternetNetworkRX	This metric is used to measure the inbound network traffic of a measured object per second.	Kbps	None
Outbound Traffic	InternetNetworkTX	This metric is used to measure the outbound network traffic of the measurement object per second.	Kbps	None
TCP Connections	TcpCount	The number of TCP connections in various statuses set up by the server.	None	None
Processes	ProcessCount	This metric is used to measure the number of processes of a measured object.	None	None

Metric name	monitorItem	Description	Unit	Remarks
Average Load	LoadAverage	A concept in Linux, the average load value of the server.	None	Not supported by Windows operating systems

RDS monitoring metrics

Metric name	monitorItem	Description	Unit
CPU Utilization	CpuUsage	This metric is used to measure the CPU utilization of a measured object.	%
Memory Utilization	MemoryUsage	This metric is used to measure the memory utilization of a measured object.	%
Disk Utilization	DiskUsage	This metric is used to measure the disk utilization of a measured object.	%
IOPS Usage	IOPSUsage	This metric is used to measure the number of I/O requests of a measured object per second.	%
Connection Utilization	ConnectionUsage	This metric is used to measure the number of connections between the application and the measured object per second.	%

SLB monitoring metrics

Metric name	monitorItem	Description	Unit	Remarks
Outbound Packets per Second	PacketTX	This metric is used to measure the outbound packets of a measured object per second.	None	None

Metric name	monitorItem	Description	Unit	Remarks
Inbound Packets per Second	PacketRX	This metric is used to measure the inbound packets of a measured object per second.	None	None
Inbound Data	TrafficRX	This metric is used to measure the inbound network traffic of a measured object per second.	Kbps	None
Outbound Data	TrafficTX	This metric is used to measure the outbound network traffic of a measured object per second.	Kbps	None
Active Port Connections	ActiveConnection	This metric is used to measure the number of connections generated when the client accesses an SLB instance.	None	None
Inactive Port Connections	InactiveConnection	This metric is used to measure the number of idle connections that are not broken after the client accesses an SLB instance.	None	None
New Port Connections	NewConnection	This metric is used to measure the number of new connections of a measured object.	None	None

OSS monitoring metrics

Metric name]	monitorItem	Description	Unit

Metric name]	monitorItem	Description	Unit
Storage Space Used	StorageUtilization	This metric is used to measure the used storage space of a measured object.	Bytes
Reads	GetRequest	This metric is used to measure the number of reads of a measured object.	Times
Writes	PutRequest	This metric is used to measure the number of writes of a measured object.	Times
Public Network Inbound Traffic	InternetRX	This metric is used to measure the inbound Internet network traffic of a measured object per second.	Bytes
Public Network Outbound Traffic	InternetTX	This metric is used to measure the outbound Internet network traffic of a measured object per second.	Bytes
Classic Network Inbound Traffic	IntranetRX	This metric is used to measure the inbound intranet network traffic of a measured object per second.	Bytes
Classic Network Outbound Traffic	IntranetTX	This metric is used to measure the outbound intranet network traffic of a measured object per second.	Bytes
Internal Server Errors	InternalError	This metric is used to measure the number of errors of a measured object.	None

2.Cloud products

2.1. Elastic Compute Service (ECS)

2.1.1. API reference

2.1.1.1. List of operations

This topic introduces all of the ECS operations that you can call.

Instance operations

Operation	Description
RunInstances	Creates one or more ECS instances.
CreateInstance	Creates an ECS instance.
StartInstance	Starts an instance.
StopInstance	Stops an instance.
RebootInstance	Restarts an instance.
DeleteInstance	Releases instance resources.
AttachInstanceRamRole	Attaches an instance RAM role to your ECS instance.
DetachInstanceRamRole	Detaches a RAM role from an instance.
DescribeInstanceStatus	Obtains a list of all instances for a current user and their status information.
DescribeInstances	Queries the details of all instances.
DescribeInstanceVncUrl	Queries the Web management terminal address of an ECS instance.
DescribeUserdata	Queries the custom data of an ECS instance.
DescribeInstanceRamRole	Queries information about the instance RAM role for one or more ECS instances.
DescribeInstanceTypeFamilies	Queries the instance type families provided by ECS.
DescribeInstanceTypes	Queries the instance types provided by ECS.
ModifyInstanceAttribute	Modifies the attributes of an instance, such as the password, name, and security group.
ModifyInstanceVpcAttribute	Modifies the VPC attributes of an ECS instance.
ModifyInstanceVncPasswd	Modifies the VNC password of an ECS instance.

Deployment set operations

Operation	Description
CreateDeploymentSet	Creates a deployment set.
DeleteDeploymentSet	Deletes a deployment set.
ModifyDeploymentSetAttribute	Modifies the attributes of a deployment set.
DescribeDeploymentSets	Queries deployment sets.
DescribeDeploymentSetTopology	Obtains the physical topology of a deployment set.

Disk operations

Operation	Description
CreateDisk	Creates a disk.
DescribeDisks	Queries disks.
AttachDisk	Attaches a disk to an instance.
DetachDisk	Detaches a disk from an instance.
ModifyDiskAttribute	Modifies the attributes of a disk.
DeleteDisk	Releases a disk that is no longer in use. Only independent cloud disks can be released.
ReInitDisk	Reinitializes a disk.
ResetDisk	Restore the content of a disk using its snapshot.
ReplaceSystemDisk	Replaces a system disk.
ResizeDisk	Scales up a disk.
migrate_disk	Migrates a disk online.
query_load_progress	Queries the progress of a migration operation for a disk.

Snapshot operations

Operation	Description
CreateSnapshot	Creates a snapshot for a disk storage device.
DeleteSnapshot	Deletes the snapshot of an instance or disk.
DescribeSnapshots	Queries all snapshots of a disk device in ECS.

Operation	Description
DescribeSnapshotLinks	Queries the snapshot links of one or more disks.
CreateAutoSnapshotPolicy	Creates an automatic snapshot policy.
DeleteAutoSnapshotPolicy	Deletes an automatic snapshot policy.
ModifyAutoSnapshotPolicyEx	Modifies an automatic snapshot policy.
DescribeAutoSnapshotPolicyEx	Queries automatic snapshot policies.
ApplyAutoSnapshotPolicy	Applies an automatic snapshot policy to one or more disks.
CancelAutoSnapshotPolicy	Cancels the automatic snapshot policy of one or more disks.

Image operations

Operation	Description
DescribeImages	Queries available images.
CreateImage	Creates a custom image. The created custom image can be used to create an ECS instance.
ModifyImageAttribute	Modifies the name and description of a custom image.
DeleteImage	Deletes a custom image.
CopyImage	Copies a custom image from one region to another for consistent deployment.
CancelCopyImage	Cancels an image copy task.
ModifyImageSharePermission	Manages what accounts a custom image is shared to.
DescribeImageSharePermission	Queries the accounts to which a custom image is shared.
ImportImage	Imports an offline image file to ECS to create a custom image.
ExportImage	Exports a custom image to an OSS bucket in the same region as the custom image.

Network operations

Operation	Description
AllocatePublicIpAddress	Assigns an available public IP address to a specific instance.
ModifyInstanceNetworkSpec	Modifies the bandwidth configurations of an ECS instance.

Security group operations

Operation	Description
CreateSecurityGroup	Creates a security group. You can configure the firewall rules for a group of instances.
AuthorizeSecurityGroup	Sets the inbound access permissions of a security group.
AuthorizeSecurityGroupEgress	Sets the outbound access permissions of a security group.
RevokeSecurityGroup	Lifts the security group rules on inbound traffic.
RevokeSecurityGroupEgress	Lifts the security group rules on outbound traffic.
JoinSecurityGroup	Adds an instance to a security group.
LeaveSecurityGroup	Removes an instance from a security group.
DeleteSecurityGroup	Deletes a security group.
DescribeSecurityGroupAttribute	Queries details about a security group, including its permission rules.
DescribeSecurityGroups	Queries the basic information about all user-defined security groups.
DescribeSecurityGroupReferences	Queries whether a security group is referenced by other security groups.
ModifySecurityGroupAttribute	Modifies the attribute of a security group, including its name and description.
ModifySecurityGroupPolicy	Modifies the intranet communication policy of a security group.
ModifySecurityGroupRule	Modify the inbound rules of a security group.

SSH key pair operations

Operation	Description
CreateKeyPair	Creates an SSH key pair.
ImportKeyPair	Imports the public key of an RSA-encrypted key pair that was created by other key pair generators.
AttachKeyPair	Attaches attach an SSH key pair to one or more Linux instances.
DetachKeyPair	Detaches an SSH key pair from one or more Linux instances.
DeleteKeyPairs	Deletes one or more SSH key pairs.
DescribeKeyPairs	Queries one or more SSH key pairs.

ENI operations

Operation	Description
CreateNetworkInterface	Creates an Elastic Network Interface (ENI).
AttachNetworkInterface	Attaches an ENI to an ECS instance in a VPC.
DescribeNetworkInterfaces	Queries available ENIs.
DetachNetworkInterface	Detaches an ENI from an ECS instance.
DeleteNetworkInterface	Deletes an ENI.
ModifyNetworkInterfaceAttribute	Modifies the attributes of an ENI.

Region operations

Operation	Description
DescribeRegions	Queries available regions.
DescribeZones	Queries available zones.

Tag operations

Operation	Description
AddTags	Binds tags to an instance, disk, snapshot, image, or security group.
RemoveTags	Unbinds tags from an instance, disk, snapshot, image, or security group.
DescribeTags	Queries tags.

Other operations

Operation	Description
DescribeTasks	Queries existing tasks.
DescribeTaskAttribute	Queries the details of a task.
CancelTask	Cancels a running task.

2.1.1.2. Make API requests

2.1.1.2.1. Overview

You can call an operation by sending an HTTP GET request to the ECS endpoint. You must specify the relevant request parameters in the request based on the operation descriptions. The system returns the processing result of the request. Requests and responses are encoded using UTF-8.

2.1.1.2.2. Request structure

Endpoints

The endpoint for ECS APIs is tjv3ecs.example.com. For more information about how to obtain a service endpoint, see Obtain an endpoint.

Methods

You can call an API operation by sending an HTTP GET request. If you use this method, the request parameters must be included in the request URL.

Protocols

You can send requests over HTTP or HTTPS. For security considerations, we recommend that you use HTTPS.

Parameters

For each request, you must specify the Action parameter (such as StartInstance), common request parameters, and API-specific parameters.

Encoding

Requests and responses are encoded using UTF-8.

2.1.1.2.3. API authorization

To ensure the security of your account, we recommend that you call ECS APIs as a RAM user. Before you can call an ECS API as a RAM user, you must create and assign corresponding permissions for your RAM user account. In RAM, you can grant permissions on ECS resources to carry out the following operations:

- AllocatePublicIpAddress
- AttachDisk
- AuthorizeSecurityGroup
- CreateDisk
- CreateImage
- CreateInstance
- CreateSecurityGroup
- CreateSnapshot
- DeleteDisk
- DeleteImage
- DeleteInstance
- DeleteSecurityGroup
- DeleteSnapshot
- DescribeAutoSnapshotPolicy
- DescribeDisks
- DescribeImages
- DescribeInstances

- DescribeInstanceStatus
- DescribeInstanceTypes
- DescribeRegions
- DescribeSecurityGroupAttribute
- DescribeSecurityGroups
- DescribeSnapshots
- DescribeZones
- DetachDisk
- JoinSecurityGroup
- LeaveSecurityGroup
- ModifyAutoSnapshotPolicy
- ModifyDiskAttribute
- ModifyInstanceAttribute
- ModifyInstanceVpcAttribute
- ModifyInstanceNetworkSpec
- RebootInstance
- ReplaceSystemDisk
- ReInitDisk
- ResetDisk
- RevokeSecurityGroup
- StartInstance
- StopInstance

2.1.1.2.4. Signature mechanism

To ensure the security of your API, you must sign the API request with signature information. ECS uses this signature to verify the identity of the caller.

ECS implements symmetric encryption through AccessKey ID and AccessKey Secret to authenticate the request sender. AccessKey ID and AccessKey Secret are issued to Apsara Stack tenant accounts and RAM users. The AccessKey ID is used to identify the user, while the AccessKey Secret is used to encrypt the signature string on the client side and to verify the signature string on the server side. The AccessKey Secret must be kept strictly confidential. For more information about how to obtain an AccessKey, see Obtain an AccessKey pair.

Perform the following steps to sign an access request:

1. Use request parameters to construct a canonicalized query string.
    i. Sort parameters. To construct a canonicalized query string, sort all request parameters by name in alphabetic order. These parameters include common request parameters and customized API request parameters, but do not include the Signature parameter in common request parameters.

    > **Note** If a request is submitted using the GET method, these parameters are placed in the request section after a question mark (?) in the request URI and connected with ampersands (&).

ii. Encode parameters. Parameter names and values must be encoded using UTF-8. The URL encoding rules are described as follows:

- Uppercase and lowercase letters, digits, hyphens (-), underscores (_), periods (.), and tildes (~) are not required to be encoded.
- Other characters are encoded as %XY, where XY is the hexadecimal representation of the character in ASCII. For example, double quotation marks (") are encoded as %22.
- Extended UTF-8 characters are encoded in the %XY%ZA... format.
- A space is encoded as %20, rather than the plus sign (+).

> **Note**
>
> This encoding method is similar to but different from the application/x-www-form-urlencoded MIME encoding algorithm (such as the implementation of the java.net.URLEncoder class provided by the Java standard library). If this encoding method is used, replace the plus signs (+) in the encoded strings with %20, the asterisks (*) with %2A, and %7E with a tilde (~) to conform to the encoding rules. This algorithm can be implemented using the following percentEncode() method:

```
private static final String ENCODING = "UTF-8";

private static String percentEncode(String value) throws UnsupportedEncodingException {
  return value != null ? URLEncoder.encode(value, ENCODING).replace("+", "%20").replace("*", "%2A").replace("%7E", "~") : null;
}
```

iii. Connect the encoded parameter names and values with equal signs (=).

iv. Sort the equal sign-connected strings by their parameter names alphabetically and connect them with ampersands (&).

2. Use the created canonicalized query string to construct a string for signature calculation based on the following rule:

```
StringToSign=
  HTTPMethod + “&” +
  percentEncode( “/” ) + ” &” +
   percentEncode(CanonicalizedQueryString)
```

- In the preceding example, HTTPMethod indicates that an HTTP-style request such as GET is submitted.
- percentEncode("/") is the encoded value (%2F) of a forward slash (/). The encoding follows the URL encoding rules described in the previous step.
  percentEncode(CanonicalizedQueryString) is the string constructed using the canonicalized query string. The encoding follows the URL encoding rules described in the previous step.

3. Use the signature string to calculate the HMAC value of the signature as defined by RFC 2104.

> **Note** The key used for signature calculation is your AccessKey Secret. An ampersand (*&*) is added to the end of the key (ASCII: 38). The SHA-1 hashing algorithm is used.

4. Encode the HMAC value into a string based on the Base64 encoding rules. This encoded string is the signature value.
5. Add this signature value as the value of the Signature parameter to the request parameters. You have now completed the request signing process.

> **Note** The obtained signature value must be URL encoded as specified in RFC 3986, like other parameters, before it can be submitted to the ECS server as the final request parameter value.

Taking DescribeRegions as an example, if the AccessKey ID is *testid* and the AccessKey Secret is *testsecret*, the request URL placed before the signature is as follows:

```
http://ecs.example.com/?TimeStamp=2016-02-23T12:46:24Z&Format=XML&AccessKeyId=testid&Action=DescribeRegions&SignatureMethod=HMAC-SHA1&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82f****&Version=2014-05-26&SignatureVersion=1.0
```

The StringToSign placed after the signature is as follows:

```
GET&%2F&AccessKeyId%3Dtestid%26Action%3DDescribeRegions%26Format%3DXML%26SignatureMethod%3DHMAC-SHA1%26SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82f****%26SignatureVersion%3D1.0%26TimeStamp%3D2016-02-23T12%253A46%253A24Z%26Version%3D2014-05-26
```

Because the value of AccessKey Secret is *testsecret*, the key used for HMAC calculation is *testsecret&*. The calculated signature is *CT9X0VtwR86fNWSnsc6v8YG*****.

Add this signature value as the value of the Signature parameter to the URL request parameters, and the signed request URL will be as follows: `http://ecs.example.com/?SignatureVersion=1.0&Action=DescribeRegions&Format=XML&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82f****&Version=2014-05-26&AccessKeyId=testid&Signature=CT9X0VtwR86fNWSnsc6v8YGO****&SignatureMethod=HMAC-SHA1&TimeStamp=2016-02-23T12%3A46%3A24Z` .

2.1.1.2.5. Responses

API responses use a unified format. 2xx HTTP status codes indicate successful calls. 4xx or 5xx HTTP status codes indicate failed calls. Responses can be returned in XML or JSON format. By default, responses are returned in XML format. You can specify the response format in the request of an API call.

> **Note** To improve readability, the sample responses in this topic are formatted. The actual responses are not formatted with line breaks or indentation.

Successful response examples

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<! --Result root node-->
<API name+Response>
   <! --Returned request tag-->
   <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
   <! --Returned results-->
</API name+Response>
```

- JSON format

```
{
   "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
   /*Returned results*/
}
```

Error response examples

If an error occurs when you call an operation, the requested data will not be returned. You can troubleshoot the error based on the error code specific to the operation and the common errors. If the operation fails to be called, a 4xx or 5xx HTTP status code will be returned. The response body contains the error code, the error message, a unique request ID, and the ID of the site accessed by the request.

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<Error>
  <RequestId>8906582E-6722-409A-A6C4-0E7863B733A5</RequestId>
  <HostId>ecs.example.com</HostId>
  <Code>InvalidOwnerId</Code>
  <Message>The specified OwnerId is not valid. </Message>
</Error>
```

- JSON format

```
{
   "RequestId": "8906582E-6722-409A-A6C4-0E7863B733A5",
   "HostId": "ecs.example.com",
   "Code": "InvalidOwnerId",
   "Message": "The specified OwnerId is not valid."
}
```

2.1.1.3. RAM authentication

When a RAM user requests access to the ECS resources of an Apsara Stack tenant account through ECS APIs, the ECS backend sends a request to RAM to check the access levels and ensure that the caller has been granted access to these resources.

ECS determines which resource permission to check based on the resources specified in the ECS operation request and the syntax. Authentication rules for APIs lists the API authentication rules.

Authentication rules for APIs

Operation name	Authentication rule
AllocatePublicIpAddress	acs:ecs: $regionid:$accountid:instance/$instanceid
AttachDisk	acs:ecs:$regionid:$accountid:disk/$diskid acs:ecs:$regionid:$accountid:instance/$instanceid
AuthorizeSecurityGroup	acs:ecs:$regionid:$accountid:securitygroup/$securitygroupid[and acs:ecs:$regionid:$accountid:securitygroup/$sourcegroupid (if the SourceGroupId parameter is specified)]
CreateDisk	acs:ecs:$regionid:$accountid:disk/*[and acs:ecs:$regionid:$accountid:snapshot/$snapshotid (if the SnapshotId parameter is specified)]
CreateImage	acs:ecs:$regionid:$accountid:image/*acs:ecs:$regionid:$accountid:snapshot/$snapshotid
CreateInstance	acs:ecs:$regionid:$accountid:instance/*acs:ecs:$regionid:$accountid:securitygroup/$securitygroupidacs:ecs:$regionid:$accountid:image/$imageid[and acs:ecs:$regionid:$accountid:snapshot/$snapshotid (if the DataDisk.n.SnapshotId parameter is specified)]
CreateSecurityGroup	acs:ecs:$regionid:$accountid:securitygroup/*
CreateSnapshot	acs:ecs:$regionid:$accountid:disk/$diskid acs:ecs:$regionid:$accountid:snapshot/*
DeleteDisk	acs:ecs:$regionid:$accountid:disk/$diskid
DeleteImage	acs:ecs:$regionid:$accountid:image/$imageid
DeleteInstance	acs:ecs:$regionid:$accountid:instance/$instanceid
DeleteSecurityGroup	acs:ecs:$regionid:$accountid:securitygroup/$securitygroupid
DeleteSnapshot	acs:ecs:$regionid:$accountid:snapshot/$snapshotid
DescribeAutoSnapshotPolicy	acs:ecs:*:$accountid:snapshot/*
DescribeDisks	acs:ecs:$regionid:$accountid:disk/*
DescribeImages	acs:ecs:$regionid:$accountid:image/*
DescribeInstanceStatus	acs:ecs:$regionid:$accountid:instance/*
DescribeInstanceTypes	acs:ecs:*:$accountid:*
DescribeRegions	acs:ecs:*:$accountid:*

Operation name	Authentication rule
DescribeSecurityGroupAttribute	acs:ecs:$regionid:$accountid:securitygroup/$securitygroupid
DescribeSecurityGroups	acs:ecs:$regionid:$accountid:securitygroup/*
DescribeSnapshots	acs:ecs:$regionid:$accountid:snapshot/*
DescribeZones	acs:ecs:*:$accountid:*
DetachDisk	acs:ecs:$regionid:$accountid:disk/$diskid acs:ecs:$regionid:$accountid:instance/$instanceid
JoinSecurityGroup	acs:ecs:$regionid:$accountid:instance/$instanceid acs:ecs:$regionid:$accountid:securitygroup/$securitygroupid
LeaveSecurityGroup	acs:ecs:$regionid:$accountid:instance/$instanceid acs:ecs:$regionid:$accountid:securitygroup/$securitygroupid
ModifyAutoSnapshotPolicy	acs:ecs:*:$accountid:snapshot/*
ModifyDiskAttribute	acs:ecs:$regionid:$accountid:disk/$diskid
ModifyInstanceAttribute	acs:ecs:$regionid:$accountid:instance/$instanceid
ModifyInstanceNetworkSpec	acs:ecs:$regionid:$accountid:instance/$instanceid
RebootInstance	acs:ecs:$regionid:$accountid:instance/$instanceid
ReplaceSystemDisk	acs:ecs:$regionid:$accountid:instance/$instanceid [and acs:ecs:$regionid:$accountid:image/$imageid (if a custom image is used)]
ReInitDisk	acs:ecs:$regionid:$accountid:disk/$diskid
ResetDisk	acs:ecs:$regionid:$accountid:snapshot/$snapshotid acs:ecs:$regionid:$accountid:disk/$diskid
RevokeSecurityGroup	acs:ecs:$regionid:$accountid:securitygroup/$securitygroupid [and acs:ecs:$regionid:$accountid:securitygroup/$sourcegroupid (if the SourceGroupId parameter is specified)]
StartInstance	acs:ecs:$regionid:$accountid:instance/$instanceid
StopInstance	acs:ecs:$regionid:$accountid:instance/$instanceid
DescribeInstances	acs:ecs:$regionid:$accountid:instance/*
CreateVpc	acs:ecs:$regionid:$accountid:vpc/*
ModifyVpcAttribute	acs:ecs:$regionid:$accountid:vpc/$vpcid

Operation name	Authentication rule
DescribeVRouters	acs:ecs:$regionid:$accountid:vrouter/*
CreateVSwitch	acs:ecs:$regionid:$accountid:vswitch/*
CreateRouteTable	acs:ecs:$regionid:$accountid:routetable/*
CreateRouteEntry	acs:ecs:$regionid:$accountid:routetable/$routetableid
AllocateEipAddress	acs:ecs:$regionid:$accountid:eip/*
AssociateEipAddress	acs:ecs:$regionid:$accountid:eip/$allocationid acs:ecs:$regionid:$accountid:instance/$instanceid
ReleaseEipAddress	acs:ecs:$regionid:$accountid:eip/$allocationid
DescribeVpcs	acs:ecs:$regionid:$accountid:vpc/*
DeleteVpc	acs:ecs:$regionid:$accountid:vpc/$vpcid
ModifyVRouterAttribute	acs:ecs:$regionid:$accountid:vrouter/$vrouterid
DescribeVSwitches	acs:ecs:$regionid:$accountid:vswitch/*
DeleteVSwitch	acs:ecs:$regionid:$accountid:vswitch/$vswitchid
DescribeRouteTables	acs:ecs:$regionid:$accountid:routetable/*
DeleteRouteEntry	acs:ecs:$regionid:$accountid:routetable/$routetableid
DescribeEipAddresses	acs:ecs:$regionid:$accountid:eip/*
UnassociateEipAddresses	acs:ecs:$regionid:$accountid:eip/$eipid acs:ecs:$regionid:$accountid:instance/$instanceid
ModifySecurityGroupAttribute	acs:ecs:$regionid:$accountid:securitygroup/$securitygroupid
DescribeEipMonitorData	acs:ecs:$regionid:$accountid:eip/$allocationid
ModifyVSwitchAttribute	acs:ecs:$regionid:$accountid:vswitch/$vswitchid
DescribeInstanceVncUrl	acs:ecs:$regionid:$accountid:instance/$instanceid
ModifySnapshotAttribute	acs:ecs:$regionid:$accountid:snapshot/$snapshotid
ModifyInstanceVpcAttribute	acs:ecs:$regionid:$accountid:instance/$instanceid
ModifyEipAddressAttribute	acs:ecs:$regionid:$accountid:eip/$allocationid

2.1.1.4. Common parameters

Common parameters include the common request parameters and the common response parameters.

Common request parameters

Common request parameters are request parameters that you must use when you call each API.

Common request parameter description

Name	Type	Required	Description
Format	String	No	The format of the response. Valid values: JSON and XML. Default value: XML.
Version	String	Yes	The API version in the format of YYYY-MM-DD. Note Access *http://gitlab.alibaba-inc.com/apsara_stack/APIVersionController/blob/v3.5*, locate a specific service, open the API under the OpenAPI folder of the service, and view the corresponding API version. The current version is 2014-05-26.
AccessKeyId	String	Yes	The AccessKey ID provided by Apsara Stack for you to access services.
Signature	String	Yes	The calculated signature string. For more information about how to calculate the signature value, see Request signatures.
SignatureMethod	String	Yes	The algorithm used to create the request signature. Valid value: HMAC-SHA1.
Timestamp	String	Yes	The timestamp of the request. The timestamp uses UTC and it complies with the ISO 8601 standard. The timestamp format is YYYY-MM-DDThh:mm:ssZ.
SignatureVersion	String	Yes	The version of the signature algorithm.
SignatureNonce	String	Yes	A unique random number that is used to prevent network replay attacks. You must use different random numbers for different requests.
ResourceOwnerAccount	String	No	The account of the owner of the requested resource. Set the value to the logon username. You must use this parameter in operations where ECS resources can be authozied in the RAM console. Otherwise, the request is rejected.

Examples

```
https://ecs.example.com/?Format=xml&Version=2014-05-26&Signature=Pc5WB8gokVn0xfeu%2FZV%2BiNM1****&SignatureMethod=HMAC-SHA1&SignatureNonce=1521552885****&SignatureVersion=1.0&AccessKeyId=key-test&Timestamp=2012-06-01T12:00:00Z...
```

Common response parameters

Each time you send a request to call an API, the system returns a unique identifier RequestId, regardless of whether the call is successful.

Examples

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<! --Result root node-->
<API name+Response>
  <! --Returned request tag-->
  <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
  <! --Returned results-->
</API name+Response>
```

- JSON format

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
  /*Returned results*/
}
```

2.1.1.5. Instances

2.1.1.5.1. RunInstances

You can call this operation to create one or more ECS instances.

When you call this operation, note that:

- You can create a maximum of 100 instances each time.
- You can specify a time for the instances to be automatically released by specifying the `AutoReleaseTime` parameter in your request.
- The operation returns the IDs of created instances. You can call DescribeInstances to check the status of the instances.
- You must have available security groups before instances can be created. For more information, see **Create a security group** in *ECS User Guide* and CreateSecurityGroup.
- After a successful request, the created instances start automatically. An instance is ready for use when it is in the `Running` state.
- Before creating a VPC-type instance, you must create a VPC and VSwitch in the corresponding

region. For more information, see **Create a VPC** and **Create a VSwitch** in *ECS User Guide* . You can also call APIs to create a VPC and VSwitch. For more information, see **CreateVPC** and **CreateVSwitch** in *VPC API Reference* .

- In comparison to the CreateInstance operation, the `RunInstances` operation assigns a public IP address to the newly created instance if the value of the `InternetMaxBandwidthOut` parameter is set to greater than 0.
- After the operation is called, if request parameters are invalid or no resources are available in the specified region, errors will be returned. For more information, see Error codes.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RunInstances.
RegionId	String	Yes	The ID of the region to which the instance belongs. You can call DescribeRegions to view latest regions.
ImageId	String	No	The ID of the image file to be used to create the instances. You can call DescribeImages to query available images. If neither `LaunchTemplateId` nor `LaunchTemplateName` is specified to determine a launch template, you must specify the `ImageId` parameter.
InstanceType	String	No	The instance type. For more information, see Instance type families. You can call DescribeInstanceTypes to query latest instance types. If neither `LaunchTemplateId` nor `LaunchTemplateName` is specified to determine a launch template, you must specify the `InstanceType` parameter.
SecurityGroupId	String	No	The ID of the security group to which the instances belong. Instances within the same security group can access one another. A security group can contain up to 1,000 instances. If neither `LaunchTemplateId` nor `LaunchTemplateName` is specified to determine a launch template, you must specify the `SecurityGroupId` parameter.
ZoneId	String	No	The ID of the zone to which the instance belongs. You can call DescribeZones to obtain latest zones. If this parameter is not specified, the system will assign a zone for you. Default value: null.

Name	Type	Required	Description
IoOptimized	String	No	Indicates whether the instance is I/O optimized. Valid values: • none: The instance is non-I/O optimized. • optimized: The instance is I/O optimized. • If the value of the `InstanceType` parameter indicates a Generation I type, the instance is non-I/O optimized by default. • If the value of the `InstanceType` parameter does not indicate a Generation I type, the instance is I/O optimized by default.
SystemDisk.Category	String	No	The category of the system disk. Valid values: • cloud: basic disk • cloud_efficiency: ultra disk • cloud_ssd: SSD disk • ephemeral_ssd: local SSD disk If the value of the `InstanceType` parameter indicates a Generation I type and the value of the `IoOptimized` parameter is `none`, the default value of the SystemDisk.Category parameter is cloud. In other cases, the default value is cloud_efficiency.
SystemDisk.Size	String	No	The size of the system disk. Unit: GiB. Valid values: [40, 500]. The value of this parameter must be at least 40 GiB, or greater than or equal to the value of ImageSize. By default, the size is 40 GiB or the value of ImageSize.
SystemDisk.DiskName	String	No	The name of the system disk. • The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, colons (:), underscores (_), and hyphens (-). • It cannot start with http:// or https://. • If not specified, this parameter is null. Default value: null.
SystemDisk.Description	String	No	The description of the system disk. • The description must be 2 to 256 characters in length. • It cannot start with http:// or https://. • If not specified, this parameter is null. Default value: null.

Name	Type	Required	Description
DataDisk.N.Category	String	No	The category of data disk n. Value range of `n`: [1, 16]. Valid values: • cloud: basic disk • cloud_efficiency: ultra disk • cloud_ssd: SSD disk • ephemeral_ssd: local SSD disk Default value: cloud.
DataDisk.N.Size	Integer	No	The size of data disk n. Value range of n: [1, 16]. Unit: GiB. Valid values: • cloud: [5, 2000] • cloud_efficiency: [20, 32768] • cloud_ssd: [20, 32768] • ephemeral_ssd: [5, 800] The value of this parameter must be greater than or equal to the size specified by the `SnapshotId` parameter.
DataDisk.N.SnapshotId	String	No	The ID of the snapshot used to create data disk n. Value range of n: [1, 16]. If the `DataDisk.n.SnapshotId` parameter is specified, the `DataDisk.n.Size` parameter will be ignored, and the size of the created disk will be the size of the specified snapshot.
DataDisk.n.Encrypted	String	No	Indicates whether data disk n is encrypted. Value range of `n`: [1, 16]. Valid values: • true • false Default value: false.
DataDisk.n.DiskName	String	No	The name of data disk n. Value range of `n`: [1, 16]. • The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, colons (:), underscores (_), and hyphens (-). • It cannot start with http:// or https://. • If not specified, this parameter is null. Default value: null.

Name	Type	Required	Description
DataDisk.n.Description	String	No	The description of data disk n. Value range of `n`: [1, 16]. • The description must be 2 to 256 characters in length. • It cannot start with http:// or https://. • If not specified, this parameter is null. Default value: null.
DataDisk.n.DeleteWithInstance	Boolean	No	Indicates whether data disk n is released together when the attached instance is released. Value range of `n`: [1, 16]. Valid values: • true: The disk is released with the instance. • false: The disk is not released with the instance. Default value: true. This parameter is valid only when the `DataDisk.n.Category` parameter is set to `cloud`, `cloud_efficiency`, or `cloud_ssd`. Otherwise, an error will be returned.
HpcClusterId	String	No	The ID of the HPC cluster to which the instance belongs.
VSwitchId	String	No	The ID of the VSwitch. If you are creating VPC-type instances, you must specify this parameter.
InternetMaxBandwidthIn	Integer	No	The maximum inbound bandwidth from the Internet. Unit: Mbit/s. Valid values: [1, 200]. Default value: 200.
InternetMaxBandwidthOut	Integer	No	The maximum outbound bandwidth to the Internet. Unit: Mbit/s. Valid values: [0, 100]. Default value: 0. You can submit a ticket to set the bandwidth range to [0, 200].
InstanceName	String	No	The name of the instance. • The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), colons (:), underscores (_), and hyphens (-). • If this parameter is not specified, the value of the InstanceId parameter is used as the instance name by default. • It cannot start with http:// or https://.

Name	Type	Required	Description
HostName	String	No	The name of the host that will contain the created ECS instances. • It cannot start or end with a period (.) or a hyphen (-). It cannot contain consecutive periods (.) or hyphens (-). • On Windows, the hostname must be 2 to 15 characters in length and can be a combination of letters, digits, and hyphens (-). The hostname cannot contain periods (.) or contain only digits. • On other OSs such as Linux, the hostname must be 2 to 128 characters in length. It can be segments separated with periods (.). Each segment can contain uppercase or lowercase letters, digits, and hyphens (-).
Description	String	No	The description of the instance. • The description must be 2 to 256 characters in length. • If not specified, this parameter is null. Default value: null. • It cannot start with http:// or https://.
PasswordInherit	Boolean	No	Indicates whether to use the preconfigured password of the specified image. When the PasswordInherit parameter is specified, the Password parameter must be null. For secure access, make sure that the selected image has password configured.
Amount	String	No	The number of instances to be created. Valid values: [1, 100]. Default value: 1.
AutoReleaseTime	String	No	The time when the instance is automatically released. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDTHH:mm:ssZ. • If the value of the seconds place is not 00, the time will automatically be set to the start of the specified minute. • It must be at least half an hour later than the current time. • It must be less than three years from the current time.
UserData	String	No	The custom data of the instance. It is encoded by using Base64. The maximum size of the raw data is 16 KB.

Name	Type	Required	Description
KeyPairName	String	No	The name of the key pair. • **For a Windows ECS instance**, this parameter is ignored. Default value: null. The Password parameter is still effective even the KeyPairName parameter is specified. • For a **Linux ECS instance**, the username and password authentication method is disabled by default if the KeyPairName parameter is specified.
RamRoleName	String	No	The RAM role name of the instance. You can call the RAM operation `ListRoles` to query the RAM roles that you have created. For more information, see `CreateRole` and `ListRoles`.
SecurityEnhancementStrategy	String	No	Indicates whether to enable security hardening. Valid values: • Active: Enables security hardening for system images. • Deactive: Disables security hardening for all image types.
Tag.n.Key	String	No	The key of the tag. Value range of n: [1, 5]. It cannot be a null string. It can be a maximum of 64 characters in length. It cannot start with aliyun, http://, or https://.
Tag.n.Value	String	No	The value of the tag. Value range of n: [1, 5]. It can be a null string. It can be a maximum of 128 characters in length. It cannot start with aliyun, http://, or https://.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency.

Response parameters

Name	Type	Description
InstanceIdSets	InstanceIdSet	The list of instance IDs.

Data type

Name	Type	Description
InstanceId	String	The ID of the instance. The ID is automatically generated by the system and acts as a unique identifier.

Examples

Sample requests

```
https://ecs.example.com/?Action=RunInstances
&RegionId=cn-hangzhou
&InstanceType=ecs.cm4.6xlarge
&SecurityGroupId=sg-securitygro****
&Amount=3
&<Common request parameters>
```

Sample responses

XML format

```
<RunInstancesResponse>
  <RequestId>04F0F334-1335-436C-A1D7-6C044FE73368</RequestId>
  <InstanceIdSets>
    <InstanceIdSet>
      <InstanceId>i-instanc****</InstanceId>
      <InstanceId>i-instanc****</InstanceId>
      <InstanceId>i-instanc****</InstanceId>
    </InstanceIdSet>
  </InstanceIdSets>
</RunInstancesResponse>
```

JSON format

```
{
  "InstanceIdSets": {
    "InstanceIdSet": [
      "i-instanc****",
      "i-instanc****",
      "i-instanc****"
    ]
  },
  "RequestId": "04F0F334-1335-436C-A1D7-6C044FE73368"
}
```

Error codes

Error code	Error message	HTTP status code	Description
EncryptedOption.Conflict	Encryption value of disk and snapshot conflict.	400	The error message returned when the encryption attributes of the specified disk and snapshot are not the same.
IncorrectVSwitchStatus	The current status of virtual switch does not support this operation.	400	The error message returned when the specified VSwitch is in a state that does not support this operation.
InstanceDiskCategoryLimitExceed	The specified DataDisk.n.Size beyond the permitted range, or the capacity of snapshot exceeds the size limit of the specified disk category.	400	The error message returned when the specified disk size has reached the upper limit for the disk category.
InstanceDiskNumber . LimitExceed	The total number of specified disk in an instance exceeds.	400	The error message returned when the number of data disks attached to the instance has reached the upper limit.
InvalidDataDiskSize. ValueNotSupported	The specified DataDisk.n.Size beyond the permitted range, or the exceeds the size limit of the specified disk category.	400	The error message returned when the specified DataDisk.n.Size parameter is invalid or exceeds the permitted range.
InvalidDescription.Malformed	The specified parameter Description is not valid.	400	The error message returned when the specified Description parameter is invalid.
InvalidDiskCategory. ValueNotSupported	The specified parameter DiskCategory is not valid.	400	The error message returned when the specified disk category is invalid.
InvalidDiskDescripti on. Malformed	The specified parameter SystemDisk.DiskDescription or DataDisk.n.Description is not valid.	400	The error message returned when the specified SystemDisk.DiskDescription or DataDisk.n.Description parameter is invalid.

Error code	Error message	HTTP status code	Description
InvalidDiskName.Malformed	The specified parameter SystemDisk.DiskName or DataDisk.n.DiskName is not valid.	400	The error message returned when the specified SystemDisk.DiskName or DataDisk.n.DiskName parameter is invalid.
InvalidHostName.Malformed	The specified parameter HostName is not valid.	400	The error message returned when the format of the HostName parameter is invalid.
InvalidInstanceName.Malformed	The specified parameter InstanceName is not valid.	400	The error message returned when the format of the InstanceName parameter is invalid.
InvalidInstanceType.ValueNotSupported	The specified InstanceType beyond the permitted range.	400	The error message returned when the specified InstanceType parameter is invalid or exceeds the permitted range.
InvalidInstanceType.ValueUnauthorized	The specified InstanceType is not authorized.	400	The error message returned when you are not authorized to use the specified instance type.
InvalidIoOptimizedValue.ValueNotSupported	IoOptimized value not supported.	400	The error message returned when the specified IoOptimized parameter is not supported.
InvalidNetworkType.Mismatch	Specified parameter InternetMaxBandwidthIn or InternetMaxBandwidthOut conflict with instance network type.	400	The error message returned when the specified InternetMaxBandwidthIn or InternetMaxBandwidthOut parameter does not comply with the instance network type.
InvalidParameter	The specified parameterInternetMaxBandwidthOut is not valid.	400	The error message returned when the specified InternetMaxBandwidthOut parameter is invalid.
InvalidParameter	The specified parameter bandwidth is not valid.	400	The error message returned when the specified instance bandwidth is invalid.

Error code	Error message	HTTP status code	Description
InvalidParameter	The specified parameter Amount is not valid.	400	The error message returned when the specified number of instances has reached 100.
InvalidParameter.Bandwidth	The specified parameter Bandwidth is not valid.	400	The error message returned when the specified instance bandwidth is invalid.
InvalidParameter.Conflict	The specified image does not support the specified instance type.	400	The error message returned when the specified instance type does not support the specified image.
InvalidParameter.EncryptedIllegal	The value of parameter Encrypted is illegal.	400	The error message returned when the specified DataDisk.n.Encrypted parameter is invalid.
InvalidParameter.EncryptedNotSupported	Encrypted disk is not support in this region.	400	The error message returned when disk encryption is not supported in the specified region.
InvalidParameter.EncryptedNotSupported	Corresponding data disk category does not support encryption.	400	The error message returned when disk encryption is not supported by the specified disk category.
InvalidParameter.Mismatch	Specified security group and virtual switch are not in the same VPC.	400	The error message returned when the specified security group does not belong to the same VPC as the specified VSwitch.
InvalidParameter.Mismatch	Specified virtual switch is not in the specified zone.	400	The error message returned when the specified VSwitch does not belong to the specified zone.
InvalidPassword.Malformed	The specified parameter Password is not valid.	400	The error message returned when the format of the specified password is invalid.
InvalidPasswordParam.Mismatch	The input password should be null when passwdInherit is true.	400	The error message returned when the PasswdInherit parameter is specified but the Password parameter is not left null.

Error code	Error message	HTTP status code	Description
InvalidSystemDiskCategory.ValueNotSupported	The specified parameter SystemDisk.Category is not valid.	400	The error message returned when the specified SystemDisk.Category parameter is invalid.
InvalidUserData.NotSupported	The specified parameter UserData only support the vpc and IoOptimized Instance.	400	The error message returned when the UserData parameter is not specified for a VPC-type or I/O optimized instance.
InvalidUserData. Size Exceeded	The specified parameter UserData exceeds the size.	400	The error message returned when the volume of custom data before being encoded based on Base64 is more than 16 KB.
InvalidHpcClusterId. NotFound	The specified HpcClusterId is not found.	400	The error message returned when the specified HPC cluster does not exist.
InvalidHpcClusterId. Creating	The specified HpcClusterId is creating.	400	The error message returned when the specified HPC cluster is still being created and cannot be used.
InvalidHpcClusterId. Unnecessary	The specified HpcClusterId is unnecessary.	400	The error message returned when the HpcClusterId parameter is not supported by the current instance type.
InvalidVSwitchId.Necessary	The HpcClusterId is necessary.	400	The error message returned when the HpcClusterId parameter is not specified for the instance type.
MissingParameter	The input parameter VSwitchId that is mandatory for processing this request is not supplied.	400	The error message returned when the required parameter VSwitchId is not specified.
QuotaExceeded	Living instances quota exceeded in this VPC.	400	The error message returned when the number of instances in the specified VPC has reached the upper limit.

Error code	Error message	HTTP status code	Description
ResourceNotAvailable	Resource you requested is not available in this region or zone.	400	The error message returned when the resource you requested is unavailable in the specified region or zone.
CategoryNotSupported	The specified zone does not offer the specified disk category.	403	The error message returned when the specified disk category is unavailable in the specified zone.
DeleteWithInstance. Conflict	The specified disk is not a portable disk and cannot be set to DeleteWithInstanc e attribute.	403	The error message returned when the specified disk category does not support setting the DeleteWithInstance attribute.
DependencyViolation.Window sInstance	The instance creating is window, cannot use ssh key pair to login.	403	The error message returned when you are trying to create a Windows instance that does not support SSH key pairs.
Forbidden	User not authorized to operate on the specified resource.	403	The error message returned when you do not have permissions on the specified resource.
ImageNotSupportInstanceTyp e	The specified image don't support the InstanceType instance.	403	The error message returned when the specified image does not support the instance type.
InstanceDiskCategoryLimitExc eed	The total size of specified disk category in an instance exceeds.	403	The error message returned when the specified disk category exceeds the maximum capacity of a single instance.
InstanceDiskNumLimitExceed	The number of specified disk in an instance exceeds.	403	The error message returned when the number of disks has reached the upper limit supported by the specified instance.
InvalidDiskCategory. Mismatch	The specified disk categories combination is not supported.	403	The error message returned when the combination of specified disk categories is not supported.

Error code	Error message	HTTP status code	Description
InvalidDiskCategory.NotSupported	The specified disk category does not support the specified instance type.	403	The error message returned when the specified disk category does not support the specified instance type.
InvalidDiskSize.TooSmall	Specified disk size is less than the size of snapshot.	403	The error message returned when the specified disk size is smaller than the specified snapshot size.
InvalidInstanceType.ZoneNotSupported	The specified zone does not support this InstanceType.	403	The error message returned when the specified instance type cannot be created in the specified zone.
InvalidResourceType.NotSupported	This resource type is not supported; please try other resource types.	403	The error message returned when the resource type is not supported in the current zone. You can select a different resource type.
InnerServiceFailed	The request processing has failed due to some unknown error.	403	The error message returned when an unknown internal error occurs.
InvalidSnapshotId.NotDataDiskSnapshot	The specified snapshot is system disk snapshot.	403	The error message returned when the specified snapshot is a system disk snapshot and cannot be used to create a data disk.
InvalidSnapshotId.NotReady	The specified snapshot has not completed yet.	403	The error message returned when the snapshot is being created. You can try again later.
InvalidSystemDiskCategory.ValueUnauthorized	The disk category is not authorized.	403	The error message returned when you are not authorized to create a disk of the specified category.
InvalidUserData.Forbidden	User not authorized to input the parameter UserData, please apply for permission UserData.	403	The error message returned when you are not authorized to configure custom data for the instance.

Error code	Error message	HTTP status code	Description
InvalidVSwitchId.NotFound	The VSwitchId provided does not exist in our records.	403	The error message returned when the specified VSwitch does not exist.
IoOptimized.NotSupported	The specified image is not support IoOptimized Instance.	403	The error message returned when the specified image does not support I/O optimized instances.
IoOptimized.NotSupported	Vpc is not support IoOptimized instance.	403	The error message returned when I/O optimized instances are not supported in VPC.
OperationDenied	The specified snapshot is not allowed to create disk.	403	The error message returned when the specified snapshot cannot be used to create a disk.
OperationDenied	The creation of Instance to the specified Zone is not allowed.	403	The error message returned when the instance cannot be created in the specified zone, or the specified zone and region do not match.
OperationDenied	The specified Image is disabled or is deleted.	403	The error message returned when the specified image does not exist.
OperationDenied	The capacity of snapshot exceeds the size limit of the specified disk category or the specified category is not authorized.	403	The error message returned when the specified DataDisk.n.Size parameter is invalid or exceeds the permitted range, or when you are not authorized to create disks of the specified category.
OperationDenied	The type of the disk does not support the operation.	403	The error message returned when the specified disk type does not support the current operation.
OperationDenied.NoStock	Sales of this resource are temporarily suspended in the specified region; please try again later.	403	The error message returned when the inventory of the specified instance type is insufficient. You can try other instance types or try other zones.

Error code	Error message	HTTP status code	Description
QuotaExceed.BuyImage	The specified image is from the image market. You have not bought it or your quota has been exceeded.	403	The error message returned when you have not purchased the specified image or the image quota has been exhausted.
QuotaExceed.PortableCloudDisk	The quota of portable cloud disk exceeds.	403	The error message returned when the number of disks attached to the instance has reached 16.
RegionUnauthorized	There is no authority to create instance in the specified region.	403	The error message returned when you are not authorized to access resources in the specified zone.
SecurityGroupInstanceLimitExceed	The maximum number of instances in a security group is exceeded.	403	The error message returned when the number of instances in the security group has reached 1,000.
Zone.NotOnSale	The specified zone is not available for purchase.	403	The error message returned when you are not authorized to create instances in the specified zone. You can try again in other regions or zones. The error message may also be returned when you are creating VPC-type instances but the specified VSwitch cannot be used in the specified zone.
Zone.NotOpen	The specified zone is not granted to you to buy resources yet.	403	The error message returned when you are not authorized to create instances in the specified zone.
ZoneId.NotFound	The specified zone does not exists.	403	The error message returned when the specified zone does not exist.
DependencyViolation.IoOptimized	The specified InstanceType must be IoOptimized instance.	404	The error message returned when the specified instances are not I/O optimized.
HOSTNAME_ILLEGAL	hostname is not valid.	404	The error message returned when the specified HostName parameter is invalid.

Error code	Error message	HTTP status code	Description
InvalidDataDiskSnapshotId.NotFound	The specified parameter DataDisk.n.SnapshotId is not valid.	404	The error message returned when the specified DataDisk.n.SnapshotId parameter does not exist.
InvalidImageId.NotFound	The specified ImageId does not exist.	404	The error message returned when the specified image does not exist.
InvalidKeyPairName.NotFound	The specified KeyPairName does not exist in our records.	404	The error message returned when the specified key pair name does not exist.
InvalidLaunchTemplate.NotFound	The specified LaunchTemplateId "{0}" LaunchTemplateName "{1}" is not found.	404	The error message returned when the specified LaunchTemplateId or LaunchTemplateName parameter does not exist.
InvalidLaunchTemplateVersion.NotFound	The specified LaunchTemplateId "{0}" Version "{1}" is not found.	404	The error message returned when the specified LaunchTemplateVersion parameter does not exist.
InvalidRamRole.NotFound	The specified RamRoleName does not exist.	404	The error message returned when the specified RAM role name does not exist.
InvalidRegionId.NotFound	The specified RegionId does not exist.	404	The error message returned when the specified region does not exist.
InvalidSecurityGroupId	The specified SecurityGroupId is invalid or does not exist.	404	The error message returned when the specified SecurityGroupId parameter is invalid or does not exist, or you are not authorized to use the specified security group.
InvalidSystemDiskSize	The specified parameter SystemDisk.Size is invalid.	404	The error message returned when the specified SystemDisk.Size parameter is invalid.
InvalidSystemDiskSize.LessThanImageSize	The specified parameter SystemDisk.Size is less than the image size.	404	The error message returned when the specified SystemDisk.Size value is smaller than the image size.

Error code	Error message	HTTP status code	Description
InvalidSystemDiskSize.LessThanMinSize	The specified parameter SystemDisk.Size is less than the min size.	404	The error message returned when the specified SystemDisk.Size value is smaller than 20 GiB.
InvalidSystemDiskSize.MoreThanMaxSize	The specified parameter SystemDisk.Size is more than the max size.	404	The error message returned when the specified SystemDisk.Size value is greater than 500 GiB.
InvalidVSwitchId.NotFound	Specified virtual switch does not exist.	404	The error message returned when the specified VSwitch does not exist.
InvalidZoneId.NotFound	The specified ZoneId does not exist.	404	The error message returned when the specified zone does not exist.
IoOptimized.NotSupported	The specified InstanceType is not support IoOptimized instance.	404	The error message returned when the specified instance type does not support I/O optimization.
OperationDenied	Another Instance is being created.	404	The error message returned when other instances are being created. You can try again later.
InternalError	The request processing has failed due to some unknown error, exception or failure.	500	The error message returned when an unknown internal error occurs. You can try again later.

2.1.1.5.2. CreateInstance

You can call this operation to create an instance.

When you call this operation, note that:

- When creating an instance, you must select an image to determine the system disk configuration of the new instance. The image contains OS and application configurations. The system disk of an instance is a clone of the image that was used to create the instance.
- When creating an instance, you must specify a security group for the instance. The security group must be created in advance. You can create a security group by calling CreateSecurityGroup. You can specify the security group when creating the instance, or change the security group to which the instance belongs by calling ModifyInstanceAttribute.

Instances that belong to the same security group can access each other. Security groups are isolated by firewalls by default, and instances in different security groups cannot access each other. However, you can configure the firewall permissions of a security group by calling AuthorizeSecurityGroup or AuthorizeSecurityGroupEgress. A security group can contain a maximum of 1,000 instances. If you specify a security group that already contains 1,000 instances, a failure prompt will be displayed.

- When creating an instance, you can specify whether it is an I/O optimized instance.
- During instance creation, the system allocates a system disk with an appropriate size for the instance based on the specified image. You can also specify the system disk capacity by using the SystemDisk.size parameter. The system disk capacity must be at least 40 GiB, or greater than or equal to the ImageSize value. You can set the system disk type to ultra disk (cloud_efficiency) or SSD disk (cloud_ssd).
- The capacity of a basic disk cannot exceed 2,000 GiB, the capacity of an ultra disk cannot exceed 32 TB (32,768 GiB), and the capacity of an SSD disk cannot exceed 32 TB (32,768 GiB).
- For the system disk created with an instance, the value of the Portable attribute is false. This indicates that the system disk cannot be attached or detached from the instance and that the system disk is to be released together when the instance is released. Therefore, the value of the DeleteWithInstance attribute of the system disk is true.
- If a data disk is created with an instance and its type is set to ultra disk (cloud_efficiency) or SSD disk (cloud_ssd), the value of the Portable attribute of the data disk is set to true. This indicates that the data disk can be attached or detached to from instances. If the data disk is to be released together when its attached instance is released, the default value of the DeleteWithInstance attribute is true. Otherwise, the default value of the DeleteWithInstance attribute is false.
- A 32-bit Windows operating system supports a maximum of 4 CPU cores. For ECS instances with 4 GiB or larger memory, select a 64-bit operating system. The maximum amount of addressable memory for a 32-bit operating system is 4 GiB.
- To create a VPC-type instance, you must specify network type of the instance as VPC when creating the instance. The VPC-type instance must belong and only belong to one VSwitch.
- If the VSwitchId parameter is specified to create an instance, the specified VSwitch and security group must belong to the same VPC.
- When you specify both the VSwitchId and PrivateIpAddress parameters, the specified private IP address must be within the range of the VSwitch CIDR block.
- The PrivateIpAddress parameter is dependent on the VSwitch and cannot be specified separately.
- After an instance is created, it is in the Stopped state.
- You can use the UserData parameter to specify custom data for the instance. The custom data is encoded in Base64. The custom data is not encrypted. Do not enter confidential information such as passwords and private keys in plaintext. If such information must be transmitted, we recommend that you first encrypt the information and encode it in Base64 before transmitting it. You can decrypt the information in the same mode after it is transmitted within your ECS instance.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateInstance.
RegionId	String	Yes	The ID of the region that the created instance will belong to.
ZoneId	String	No	The ID of the zone that the created instance will belong to. If this parameter is not specified, the system will automatically allocate the instance to a zone. Default value: null.
ImageId	String	Yes	The ID of the image file to create the instance from.
InstanceType	String	Yes	The instance type. For more information, see Instance types. You can call DescribeInstanceTypes to query the instance types provided by ECS.
SecurityGroupId	String	Yes	The ID of the security group that the created instance will belong to. Instances within the same security group can access one another.
UserData	String	No	The custom data of the instance. It is encoded in Base64. The maximum size of the raw data is 16 KB.
DataDisk.n.Encrypted	Boolean	No	Indicates whether data disk n is to be encrypted. Valid values: • true • false Default value: false.
InstanceName	String	No	The name of the instance. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). The instance name is displayed in Apsara Stack console. If this parameter is not specified, the value of the InstanceId parameter is used as the instance name by default. The instance name cannot start with http:// or https://.

Name	Type	Required	Description
Description	String	No	The description of the instance. The description must be 2 to 256 characters in length. It is displayed in Apsara Stack console. If not specified, this parameter is null. Default value: null. It cannot start with http:// or https://.
InternetMaxBandwidthIn	String	No	The maximum inbound bandwidth from the Internet. Unit: Mbit/s. Valid values: [1, 200]. If this parameter is not specified, the maximum inbound bandwidth will be set to 200 Mbit/s.
InternetMaxBandwidthOut	String	No	The maximum outbound bandwidth to the Internet. Unit: Mbit/s. Valid values: • Measured by bandwidth: [0, 100]. If this parameter is not specified, the maximum outbound bandwidth will be set to 0 Mbit/s. • Measured by traffic: [1, 100]. If this parameter is not specified, an error will be returned.
HostName	String	No	The hostname of the ECS. It must contain at least two characters. It cannot start or end with a period (.) or a hyphen (-). It cannot contain consecutive periods (.) or hyphens (-). On Windows, the hostname can contain a maximum of 15 characters, which can be a combination of uppercase or lowercase letters, digits, and hyphens (-). The hostname cannot contain periods (.) or contain only digits. On other OSs such as Linux, the hostname can contain a maximum of 30 characters, which can be segments separated with periods (.). Each segment can contain uppercase or lowercase letters, digits, and hyphens (-).

Name	Type	Required	Description
Password	String	No	The password of the instance. The password is a string of 8 to 30 characters and must contain uppercase or lowercase letters, digits, and special characters. The password can contain any of the following special characters: ( ) ` ~ ! @# $ % ^ & * - + = | { }[ ] : ; ' < > , . ? / If the Password parameter is specified, use HTTPS to call the operation to avoid password leakage.
IoOptimized	String	No	Indicates whether the created instance is I/O optimized. Valid values: • none: The instance is not I/O optimized. • optimized: The instance is I/O optimized. Default value: none.
SystemDisk.Category	String	No	The category of the system disk. Valid values: • cloud_efficiency: ultra disk • cloud_ssd: SSD disk Default value: cloud.
SystemDisk.Size	Integer	No	The size of the system disk. Unit: GiB. Valid values: • cloud_efficiency: 40 to 500 • cloud_ssd: 40 to 500 Default value: max{40, ImageSize}. The value of this parameter must be at least 40 GiB, or greater than or equal to the value of ImageSize.

Name	Type	Required	Description
SystemDisk.DiskName	String	No	The name of the system disk. If not specified, this parameter is null. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, underscores (_), and hyphens (-). The disk name is displayed in Apsara Stack console. It cannot start with `http://` or `https://`.
SystemDisk.Description	String	No	The description of the system disk. If not specified, this parameter is null. Default value: null. The description must be 2 to 256 characters in length. It is displayed in Apsara Stack console. It cannot start with http:// or https://.
DataDisk.N.Size	Integer	No	The allocated size of data disk n. n is an integer count that begins at 1. Unit: GiB. Valid values: • cloud_efficiency: 20 to 32768 • cloud_ssd: 20 to 32768 The value of this parameter must be greater than or equal to that of the specified snapshot file used to create the disk.
DataDisk.N.Category	String	No	The category of data disk n. Valid values: • cloud_efficiency: ultra disk • cloud_ssd: SSD disk Default value: cloud.
DataDisk.N.SnapshotId	String	No	The ID of the snapshot used to create the data disk. If this parameter is specified, the DataDisk.n.Size parameter will be ignored, and the size of the created disk will be the size of the specified snapshot.

Name	Type	Required	Description
DataDisk.n.DiskName	String	No	The name of the data disk. If not specified, this parameter is null. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, underscores (_), and hyphens (-). The disk name is displayed in Apsara Stack console. It cannot start with http:// or https://.
DataDisk.n.Description	String	No	The description of the data disk. If not specified, this parameter is null. Default value: null. The description must be 2 to 256 characters in length. It is displayed in Apsara Stack console. It cannot start with http:// or https://.
DataDisk.N.Device	String	No	If the parameter value is null, the value will be automatically allocated starting from /dev/xvdb to /dev/xvdz. Default value: null.
DataDisk.n.DeleteWithInstance	String	No	Indicates whether the data disk is released together with the instance. • true: When the instance is released, the disk will be released together with it. • false: When the instance is released, the disk will be retained. Default value: true. This parameter is valid only when the DataDisk.n.Category parameter is set to cloud, cloud_efficiency, or cloud_ssd. Otherwise, an error will be returned.
VSwitchId	String	No	The ID of the VSwitch used by the VPC. This parameter must be specified if you are creating a VPC-type instance.
PrivateIpAddress	String	No	The private IP address of the instance. This parameter cannot be specified separately.

Name	Type	Required	Description
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters.

Response parameters

Response parameter description

Name	Type	Required
InstanceId	String	The ID of the instance. The ID is automatically generated by the system and acts as a unique identifier.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required RegionId parameter is not specified or when you do not have access to this region.
InvalidInstanceType.ValueUnauthorized	The specified InstanceType is not authorized.	400	The error message returned when you are not authorized to use the specified instance type.

Error code	Error message	HTTP status code	Description
InvalidSystemDiskSize.LessThanImageSize	The specified parameter SystemDisk.Size is less than the image size.	404	The error message returned when the value of the SystemDisk.Size parameter is smaller than the size of the specified image.
InvalidSystemDiskSize.MoreThanMaxSize	The specified parameter SystemDisk.Size is more than the max size	404	The error message returned when the value of the SystemDisk.Size parameter is greater than the maximum capacity.
InvalidSystemDiskSize.LessThanMinimumSize	The specified parameter SystemDisk.Size is less than the minimum size	404	The error message returned when the value of the SystemDisk.Size parameter is smaller than the minimum capacity.
InvalidZoneId.NotFound	The ZoneId provided does not exist in our records.	404	The error message returned when the specified zone ID does not exist or when you are not authorized to access this zone.
MissingParameter	The input parameter ImageId that is mandatory for processing this request is not supplied.	400	The error message returned when the required ImageId parameter is not specified.

Error code	Error message	HTTP status code	Description
InvalidInstanceType.ValueNotSupported	The specified InstanceType beyond the permitted range.	400	The error message returned when the value of the InstanceType parameter is not within the valid range.
MissingParameter	The input parameter InstanceType that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceType parameter is not specified.
InvalidSecurityGroupId.NotFound	The SecurityGroupId provided does not exist in our records.	404	The error message returned when the specified security group does not exist or when you are not authorized to access this security group.
MissingParameter	The input parameter SecurityGroupId that is mandatory for processing this request is not supplied.	400	The error message returned when the required SecurityGroupId parameter is not specified.
InvalidDescription.Malformed	The specified parameter Description is not valid.	400	The error message returned when the specified Description parameter is invalid.
InvalidInternetChargeType.ValueNotSupported	The specified InternetChargeType is not valid.	400	The error message returned when the specified InternetChargeType parameter does not exist.

Error code	Error message	HTTP status code	Description
InvalidParameter	The specified parameter InternetMaxBandwidthIn is not valid.	400	The error message returned when the value of the InternetMaxBandwidthIn parameter is not a numeric value or is not within the valid range.
InvalidParameter	The specified parameter InternetMaxBandwidthOut is not valid.	400	The error message returned when the value of the InternetMaxBandwidthOut parameter is not a numeric value or is not within the valid range.
InvalidHostName.Malformed	The specified parameter HostName is not valid.	400	The error message returned when the HostName parameter is invalid.
InvalidPassword.Malformed	The specified parameter Password is not valid.	400	The error message returned when the Password parameter is invalid.
InvalidUserData.NotSupported	The specified parameter UserData only support the vpc and IoOptimized Instance.	400	The error message returned when the UserData parameter is not specified for a VPC-type or I/O optimized instance.

Error code	Error message	HTTP status code	Description
InvalidUserData.SizeExceeded	The specified parameter UserData exceeds the size.	400	The error message returned when the size of the specified custom data exceeds 16 KB.
InvalidSystemDiskCategory.ValueNotSupported	The specified parameter SystemDisk.Category is not valid.	400	The error message returned when the SystemDisk.Category parameter is invalid.
InvalidDiskName.Malformed	The specified parameter SystemDisk.DiskName or DataDisk.n.DiskName is not valid.	400	The error message returned when the SystemDisk.DiskName or DataDisk.n.DiskName parameter is invalid.
InvalidDiskDescription.Malformed	The specified parameter SystemDisk.DiskDescription or DataDisk.n.Description is not valid.	400	The error message returned when the SystemDisk.DiskDescription or DataDisk.n.Description parameter is invalid.
InvalidParameter	The specified parameter DataDisk.n.Size is not valid.	400	The error message returned when the value of the DataDisk.n.Size parameter is not a numeric value.

Error code	Error message	HTTP status code	Description
InvalidDataDiskSize.ValueNotSupported	The specified DataDisk.n.Size beyond the permitted range, or the capacity of snapshot exceeds the size limit of the specified disk category.	400	The error message returned when the value of the DataDisk.n.Size parameter is not within the valid range.
InvalidDataDiskCategory.ValueNotSupported	The specified parameter DataDisk.n.Category is not valid.	400	The error message returned when the DataDisk.n.Category parameter is invalid.
InvalidDataDiskSnapshotId.NotFound	The specified parameter DataDisk.n.SnapshotId is not valid.	404	The error message returned when the specified DataDisk.n.SnapshotId parameter does not exist.
InvalidDataDevice.Malformed	The specified parameter DataDisk.n.Device is not valid.	400	The error message returned when the DataDisk.n.Device parameter is invalid.
OperationDenied	The specified parameter VlanId is not valid or vlan has not enough IP address.	400	The error message returned when the VlanId parameter is invalid.
InvalidParameter.Conflict	The specified image does not support the specified instance type.	400	The error message returned when the specified image cannot be used with the specified instance type.

Error code	Error message	HTTP status code	Description
InvalidSnapshotId.BasedSnapshotTooOld	The specified snapshot is created before 2013-07-15.	400	The error message returned when the specified snapshot was created before July 15, 2013.
OperationDenied	The specified Image is disabled or is deleted.	403	The error message returned when the specified image is unavailable or does not exist.
InvalidSystemDiskCategory.ValueUnauthorized	The system disk category is not authorized.	403	The error message returned when you are not authorized to use the specified disk category.
InvalidParameter.Mismatch	The data disk must be cloud disk when system disk category is cloud.	403	The error message returned when the system disk category is cloud but the specified data disk is not a basic cloud disk.
InvalidSnapshotId.NotReady	The specified snapshot has not completed yet.	403	The error message returned when the snapshot is being created.
OperationDenied	The specified snapshot is not allowed to create disk.	403	The error message returned when the specified snapshot cannot be used to create a disk.

Error code	Error message	HTTP status code	Description
InstanceDiskCategoryLimitExceed	The total size of specified disk category in an instance exceeds.	403	The error message returned when the specified disk category exceeds the maximum capacity of a single instance.
InvalidDevice.InUse	The specified device has been occupied.	403	The error message returned when the mount point is already occupied.
InvalidClusterId.NotFound	The ClusterId provided does not exist in our records.	404	The error message returned when the specified cluster ID does not exist.
OperationDenied	The creation of Instance to the specified Zone is not allowed.	403	The error message returned when the instance cannot be created in the specified zone, or the specified zone and region do not match.
CategoryNotSupported	The specified zone does not offer the specified disk category.	403	The error message returned when disks of the specified category cannot be created in the specified zone.

Error code	Error message	HTTP status code	Description
OperationDenied	The specified Zone or cluster does not offer the specified disk category or the specified zone and cluster do not match.	403	The error message returned when the specified zone or cluster does not support the specified disk category, or the specified zone and cluster do not match.
InvalidInstanceName.Malformed	The specified parameter InstanceName is not valid.	400	The error message returned when the InstanceName parameter is invalid.
InvalidInstanceDescription.Malformed	The specified parameter Description is not valid.	400	The error message returned when the Description parameter is invalid.
OperationDenied	The specified Image is disabled or is deleted.	404	The error message returned when the specified image does not exist.
OperationDenied	The resource is out of usage.	403	The error message returned when the zone and cluster resources are insufficient to create the instance.
InternalError	The request processing has failed due to some unknown error.	500	The error message returned when you have no available zones.

Error code	Error message	HTTP status code	Description
InvalidParameter.Conflict	The specified region and cluster do not match.	400	The error message returned when the specified region and cluster do not match.
SecurityGroupInstanceLimitExceed	Exceeding the allowed amount of instances of a security group.	403	The error message returned when the number of instances in the security group has reached the upper limit.
RegionUnauthorized	There is no authority to create instance in the specified region.	403	The error message returned when you are not authorized to access the specified region.
CategoryNotSupported	The specified Zone or cluster does not offer the specified disk category.	403	The error message returned when the specified zone or cluster does not support the specified disk category.
InvalidSnapshotId.NotDataDiskSnapshot	The specified snapshot is system disk snapshot.	403	The error message returned when the snapshot specified to create a data disk is a system disk snapshot and cannot be used.

Error code	Error message	HTTP status code	Description
OperationDenied	The capacity of snapshot exceeds the size limit of the specified disk category or the specified category is not authorized.	403	The error message returned when the value of the DataDisk.n.Size parameter is not within the valid range, or when you are not authorized to use the specified disk category.
CategoryNotSupported	The specified cluster does not offer the specified disk category.	403	The error message returned when the specified cluster does not support the specified disk category.
InvalidDiskCategory.Mismatch	The specified disk categories' combination is not supported.	403	The error message returned when the specified combination of disk categories is not allowed.
QuotaExceed.PortableCloudDisk	The quota of portable cloud disk exceeds.	403	The error message returned when the number of basic cloud disks that can be attached has reached the upper limit.
DeleteWithInstance.Conflict	The specified disk is not a portable disk and cannot be set to DeleteWithInstance attribute.	403	The error message returned when the specified disk cannot be attached or detached.

Error code	Error message	HTTP status code	Description
InstanceDiskNumLimitExceed	The number of specified disk in an instance exceeds.	403	The error message returned when the number of basic cloud disks attached to one ECS instance has reached the upper limit.
IoOptimized.NotSupported	The specified image is not support IoOptimized Instance.	403	The error message returned when the specified image does not support I/O optimized instances.
OperationDenied	Another Instance has been creating.	403	The error message returned when the more than one ECS instances is being created.
IoOptimized.NotSupported	The specified instancetype is not support IoOptimized instance.	403	The error message returned when the specified instance type does not support I/O optimized instances.
InvalidDiskCategory.NotSupported	The specified disk category is not support the specified instance type.	403	The error message returned when the specified disk category does not support the specified instance type.

Error code	Error message	HTTP status code	Description
OperationDenied	The specified zone does not support creating instance.	403	The error message returned when the specified zone does not support I/O optimized instances.
InstanceDiskCategoryLimitExceed	The specified DataDisk.n.Size beyond the permitted range, or the capacity of snapshot exceeds the size limit of the specified disk category.	400	The error message returned when the value of the DataDisk.n.Size parameter is not within the valid range.
DependencyViolation.Image	The specified imageid is not supported to create iooptimized instance.	400	The error message returned when the specified image does not support I/O optimized instances.
InstanceTypeNotSupported	The specified zone does not offer the specified instancetype.	403	The error message returned when the specified zone does not support the specified instance type.
DependencyViolation.IoOptimized	The specified instancetype must be IoOptimized instance.	404	The error message returned when the specified type of instance is not I/O optimized.

2.1.1.5.3. StartInstance

You can call this operation to start an instance.

When you call this operation, note that:

- After the operation is called, the status of the instance becomes Starting.
- The operation can be performed only when the instance is in the Stopped state.

- An instance cannot be started by calling this operation if it is locked for security reasons.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to StartInstance.
InstanceId	String	Yes	The ID of the instance to be started.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	404	The error message returned when the specified instance ID does not exist.
MissingParameter	The input parameter "InstanceId" that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the specified instance is in a state that does not support the current operation.
InstanceLockedForSecurity	The specified operation is denied as your instance is locked for security reasons.	403	The error message returned when the specified instance is locked for security reasons.
InternalError	The request processing has failed due to some unknown error.	500	The error message returned when an unknown internal error occurs.

Error code	Error message	HTTP status code	Description
InstanceNotReady	The specified instance is not ready for use.	403	The error message returned when the specified instance is not completely created.
DiskError	IncorrectDiskStatus	403	The error message returned when the disk is in an abnormal state.

Examples

Sample requests

```
https://ecs.example.com/?Action=StartInstance
&InstanceId=i-insta****
&Common request parameters
```

Sample responses

- XML format

```
<StartInstanceResponse>
  <RequestId>C0003E8B-B930-4F59-ADC0-0E209A9012A8</RequestId>
</StartInstanceResponse>
```

- JSON format

```
{
  "RequestId": "C0003E8B-B930-4F59-ADC0-0E209A9012A8"
}
```

2.1.1.5.4. StopInstance

You can call this operation to stop an instance.

When you call this operation, note that:

- The operation can be performed only when the instance is in the Running state.
- After the operation is called, the status of the instance becomes Stopping. After the instance is stopped, it enters the Stopped status in the background.
- An instance can be force stopped. Force stop is equivalent to power-off. Data that has not been written to the disk in the instance operating system may be lost.
- An instance cannot be stopped by calling this operation if it is locked for security reasons.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to StopInstance.
InstanceId	String	Yes	The ID of the instance to be stopped.
ForceStop	String	No	Indicates whether to force shutdown the instance after it is restarted. Valid values: • true • false Default value: false. The value false indicates that the instance is shut down normally. The value true indicates that the instance is force shut down. You can specify this parameter to control whether to force shutdown.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	404	The error message returned when the specified instance ID does not exist.
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.
InvalidParameter	The specified parameter ForceStop is not valid.	400	The error message returned when the specified ForceStop parameter is invalid.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the specified instance is in a state that does not support the current operation.

Error code	Error message	HTTP status code	Description
InstanceLockedForSecurity	The specified operation is denied as your instance is locked for security reasons.	403	The error message returned when the specified instance is locked for security reasons.

Examples

Sample requests

```
https://ecs.example.com/?Action=StopInstance
&InstanceId=i-insta****
&Common request parameters
```

Sample responses

- XML format

```
<StopInstanceResponse>
  <RequestId>1C488B66-B819-4D14-8711-C4EAAA13AC01</RequestId>
</StopInstanceResponse>
```

- JSON format

```
{
  "RequestId": "1C488B66-B819-4D14-8711-C4EAAA13AC01"
}
```

2.1.1.5.5. RebootInstance

You can call this operation to restart an instance.

When you call this operation, note that:

- The operation can be performed only when the instance is in the Running state.
- After the operation is called, the status of the instance becomes Starting.
- An instance can be force restarted. Force restart is equivalent to powering off traditional servers to restart them. Data that has not been written to the disk in the instance operating system may be lost.
- An instance cannot be restarted by calling this operation if it is locked for security reasons.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RebootInstance.
InstanceId	String	Yes	The ID of the instance to be restarted.
ForceStop	String	No	Indicates whether to force shutdown the instance when restarting it. Valid values: • true • false The value false indicates that the system is shut down normally. The value true indicates that the system is force shut down. By default, the value of this parameter is false if it is not specified.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	404	The error message returned when the specified instance ID does not exist.
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.
InvalidParameter	The specified parameter ForceStop is not valid.	400	The error message returned when the specified ForceStop parameter is invalid.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the specified instance is in a state that does not support the current operation.

Error code	Error message	HTTP status code	Description
InstanceLockedForSecurity	The specified operation is denied as your instance is locked for security reasons.	403	The error message returned when the specified instance is locked for security reasons.
DiskError	IncorrectDiskStatus	403	The error message returned when the disk is in an abnormal state.

Examples

Sample requests

```
https://ecs.example.com/?Action=RebootInstance
&InstanceId=i-insta****
&Common request parameters
```

Sample responses

- XML format

```
<RebootInstanceResponse>
  <RequestId>F2E2C40D-AB09-45A1-B5C5-EB9F5C4E4E4A</RequestId>
</RebootInstanceResponse>
```

- JSON format

```
{
  "RequestId": "F2E2C40D-AB09-45A1-B5C5-EB9F5C4E4E4A"
}
```

2.1.1.5.6. DeleteInstance

You can call this operation to release an instance and its resources. After an instance is released, the physical resources used by the instance will be recycled, including disks and snapshots. All related data will be deleted and can never be recovered.

When you call this operation, note that:

- The operation can be performed only when the instance is in the Stopped state. After the instance is released, its status becomes Deleted, indicating that the resources are released and the operation succeeds.
- When the instance is released, disks attached to the instance with the DeleteWithInstance attribute set to true will be released, and the snapshots of these disks are retained. If the

DeleteAutoSnapshot attribute is set to false, the automatic snapshots will be retained. If the DeleteAutoSnapshot attribute is set to true, the automatic snapshots will be deleted.

- After the instance is released, all related data will be deleted and can never be recovered.
- If the instance is locked for security reasons, the system will release attached independent basic cloud disks together with the instance even if the DeleteWithInstance attribute of the disks is set to false.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteInstance.
InstanceId	String	Required	The ID of the instance to be released.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the specified instance is in a state that does not support the current operation.
InternalError	The request processing has failed due to some unknown error.	500	The error message returned when an unknown internal error occurs.
DependencyViolation.SLBConfiguring	Specified operation is denied as the instance is being used by another product.	400	The error message returned when the specified instance is referenced by an SLB instance that is being configured.

Examples

Sample requests

```
https://ecs.example.com/?Action=DeleteInstance
&InstanceId=i-insta****
&Common request parameters
```

Sample responses

- XML format

```
<DeleteInstanceResponse>
  <RequestId>928E2273-5715-46B9-A730-238DC996A533</RequestId>
</DeleteInstanceResponse>
```

- JSON format

```
{
  "RequestId": "928E2273-5715-46B9-A730-238DC996A533"
}
```

2.1.1.5.7. AttachInstanceRamRole

You can call this operation to attach an instance RAM role to your ECS instance. If the instance already has a RAM role, an error will be returned when you attach another RAM role to the same instance.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AttachInstanceRamRole.
RegionId	String	Yes	The ID of the region. For more information, see Regions and zones.
InstanceIds	Array	Yes	A set of instance IDs. You can specify a maximum of 100 instance IDs, in the format of [“instanceId1” , “instanceId2” , “instanceId3” ...].
RamRoleName	String	Yes	The RAM role name of the instance. You can call the RAM operation ListRoles to query the RAM roles that you have created.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=AttachInstanceRamRole
&RegionId=cn-hangzhou
&RamRoleName=RamRoleTest
&InstanceIds=["i-insta****"]
&<Common request parameters>
```

Sample responses

XML format

```
<AttachInstanceRamRoleResponse>
  <RequestId>E6352369-5C2B-41CD-AB50-471550C8F674</RequestId>
  <AttachInstanceRamRoleResults>
    <AttachInstanceRamRoleResult>
      <InstanceId>i-insta****</InstanceId>
      <Code>200</Code>
      <Message>success</Message>
    </AttachInstanceRamRoleResult>
  </AttachInstanceRamRoleResults>
  <TotalCount>1</TotalCount>
  <FailCount>0</FailCount>
  <RamRoleName>RamRoleTest</RamRoleName>
</AttachInstanceRamRoleResponse>
```

JSON format

```
{
  "RequestId": "D9553E4C-6C3A-4D66-AE79-9835AF705639",
  "AttachInstanceRamRoleResults": {
    "AttachInstanceRamRoleResult": [
      {
        "Message": "success",
        "InstanceId": "i-insta****",
        "Code": "200"
      }
    ]
  },
  "TotalCount": 1,
  "FailCount": 0,
  "RamRoleName": "RamRoleTest"
}
```


Error codes

Error code	Error message	HTTP status code	Description
InvalidInstanceIds.Malformed	The specified InstanceIds is not valid.	400	The error message returned when the specified InstanceIds parameter is invalid.
MissingParameter.InstanceIds	The input parameter InstanceIds that is mandatory for processing this request is missing.	400	The error message returned when the required InstanceIds parameter is not specified.
MissingParameter.RamRoleName	The input parameter RamRoleName that is mandatory for processing this request is missing.	400	The error message returned when the required RamRoleName parameter is not specified.
MissingParameter.RegionId	The input parameter RegionId that is mandatory for processing this request is missing.	400	The error message returned when the required RegionId parameter is not specified.

Error code	Error message	HTTP status code	Description
InvalidUser.PassRoleForbidden	The RAM user does not have the privilege to pass a role.	403	The error message returned when the RAM account being used does not have the PassRole permission. Contact the owner of the Apsara Stack tenant account to grant the PassRole permission.
InvalidInstanceId.NotFound	The specified InstanceId does not exist.	404	The error message returned when the specified instance ID does not exist.
InvalidRamRole.NotFound	The specified RamRoleName does not exist.	404	The error message returned when the specified RAM role name does not exist.

2.1.1.5.8. DetachInstanceRamRole

You can call this operation to detach RAM roles from instances.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DetachInstanceRamRole.
RegionId	String	Yes	The ID of the region. For more information, see Regions and zones.
InstanceIds	String	Yes	A set of instance IDs. You can specify a maximum of 100 instance IDs at a time. The format is ["instanceId1", "instanceId2", "instanceId3"...].
RamRoleName	String	No	The name of the RAM role to be detached from the ECS instances. You can call the RAM operation ListRoles to query the RAM roles that you have created.

Response parameters

Name	Type	Description
FailCount	Integer	The number of ECS instances from which the instance RAM role failed to be detached.
RamRoleName	String	The name of the instance RAM role.
DetachInstanceRamRoleResults	Array	The returned information about an instance RAM role. It is an array consisting of DetachInstanceRamRoleResult data.
TotalCount	Integer	The number of ECS instances from which the instance RAM role is going to be detached.

DetachInstanceRamRoleResult data

Name	Type	Description
InstanceId	String	The ECS instance from which the instance RAM role is going to be detached.
Code	Integer	Indicates whether the instance RAM role was detached from the ECS instance. 200 indicates that the operation succeeded. Other values indicates that the operation failed. For more information, see Error codes.
Message	String	Indicates whether the instance RAM role was detached from the ECS instance. Success indicates that the operation succeeded. Other values indicates that the operation failed. For more information, see Error codes.

Examples

Sample requests

```
https://ecs.example.com/?Action=DetachInstanceRamRole
&RegionId=cn-hangzhou
&RamRoleName=RamRoleTest
&InstanceIds=["i-instance1"]
&<Common request parameters>
```

Sample responses

XML format

```
<DetachInstanceRamRoleResponse>
  <RequestId>E6352369-5C2B-41CD-AB50-471550C8F674</RequestId>
  <DetachInstanceRamRoleResults>
    <DetachInstanceRamRoleResult>
      <InstanceId>i-instance1</InstanceId>
      <Code>200</Code>
      <Message>success</Message>
    </DetachInstanceRamRoleResult>
  </DetachInstanceRamRoleResults>
  <TotalCount>1</TotalCount>
  <FailCount>0</FailCount>
  <RamRoleName>RamRoleTest</RamRoleName>
</DetachInstanceRamRoleResponse>
```

JSON format

```
{
  "RequestId": "E6352369-5C2B-41CD-AB50-471550C8F674",
  "DetachInstanceRamRoleResults": {
    "DetachInstanceRamRoleResult": [
      {
        "Message": "success",
        "InstanceId": "i-instance1",
        "Code": "200"
      }
    ]
  },
  "TotalCount": 1,
  "FailCount": 0,
  "RamRoleName": "RamRoleTest"
}
```

Error codes

Error code	Error message	HTTP status code	Description
MissingParameter.InstanceIds	The input parameter InstanceIds that is mandatory for processing this request is missing.	400	The error message returned when the required InstanceIds parameter is not specified.

Error code	Error message	HTTP status code	Description
MissingParameter.RegionId	The input parameter RegionId that is mandatory for processing this request is missing.	400	The error message returned when the required RegionId parameter is not specified.
InvalidInstanceIds.Malformed	The specified InstanceIds is not valid.	400	The error message returned when the specified InstanceIds parameter is invalid.
InvalidUser.PassRoleForbidden	The RAM user does not have the privilege to pass a RAM role.	403	The error message returned when the RAM account being used does not have the PassRole permission. Contact the owner of the Apsara Stack tenant account to grant the PassRole permission.
InvalidInstanceId.NotFound	The specified InstanceId does not exist.	404	The error message returned when the specified instance ID does not exist.
InvalidRamRole.NotFound	The specified RamRoleName does not exist.	404	The error message returned when the specified RAM role name does not exist.

2.1.1.5.9. DescribeInstanceStatus

You can call this operation to obtain a list of all instances for a current user and their status information.

When you call this operation, note the special limits on authorization-based resource access by using RAM:

- **A maximum of 100 instances can be queried. If the combination of the PageNumber and PageSize parameters exceeds 100 entries, the request will be denied and the error code Forbidden.AccessTooManyOthersResource will be returned.**
- **The TotalCount parameter indicates the number of instances that the caller is authorized to perform this operation on. When the number of instances is greater than 100, the TotalCount value is set to 100.**

Request parameters

Request parameter description

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeInstanceStatus.
RegionId	String	Yes	The ID of the region to which the instance belongs.
ZoneId	String	No	The ID of the zone to which the instance belongs.
PageNumber	Integer	No	The page number that you query in the instance status list. Starting value: 1. Default value: 1.
PageSize	Integer	No	The number of entries to be displayed per page. Maximum value: 50. Default value: 10.

Response parameters

Response parameter description

Name	Type	Description
TotalCount	Integer	The total number of instances.
PageNumber	Integer	The page number that you query in the instance list.
PageSize	Integer	The number of entries per page.
InstanceStatuses	InstanceStatusSetType	The returned instance information. It is an array consisting of InstanceStatusItemType data.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter "RegionId" that is mandatory for processing this request is not supplied.	400	The error message returned when the required RegionId parameter is not specified.
InvalidParameter	The specified parameter PageNumber is not valid.	400	The error message returned when the specified PageNumber parameter is invalid (not a digit).
InvalidParameter	The specified parameter PageSize is not valid.	400	The error message returned when the specified PageSize parameter is invalid (not a digit or beyond the valid range).

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeInstanceStatus
&RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

- XML format

```
<DescribeInstanceStatusResponse>
  <RequestId>6EF60BEC-0242-43AF-BB20-270359FB54A7</RequestId>
  <TotalCount>2</TotalCount>
  <PageNumber>1</PageNumber>
  <PageSize>10</PageSize>
  <InstanceStatuses>
    <InstanceStatus>
      <InstanceId>i-instance1</InstanceId>
        <Status>Running</Status>
      </InstanceStatus>
      <InstanceStatus>
        <InstanceId>i-ae4r89pp</InstanceId>
        <Status>Stopped</Status>
    </InstanceStatus>
  </InstanceStatuses>
</DescribeInstanceStatusResponse>
```

- JSON format

```
{
"RequestId": "6EF60BEC-0242-43AF-BB20-270359FB54A7",
"TotalCount": 2,
"PageNumber": 1,
"PageSize": 10,
"InstanceStatuses": {
  "InstanceStatus": [{
    "InstanceId": "i-instance1",
      "Status": "Running"
    },
    {
      "InstanceId": "i-ae4r89pp",
      "Status": "Stopped"
    }]
  }
}
```


2.1.1.5.10. DescribeInstances

You can call this operation to query the details of all instances.

When you call this operation, note that:

- This operation will not verify the dependency between parameters. The **intersection** of results that match all filtering conditions is returned.
- If a parameter is not specified, it will not be included in the filtering conditions. However, if the InstanceIds parameter is an empty JSON array ([]), it is regarded as an effective filtering condition and a blank result will be returned.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeInstances.
RegionId	String	Yes	The ID of the region.
VpcId	String	No	The ID of the VPC.
VSwitchId	String	No	The ID of the VSwitch.
ZoneId	String	No	The ID of the zone.

Name	Type	Required	Description
InstanceIds	String	No	The instance IDs. The parameter value is a JSON-formatted array: ["i-xxxxxxxxx","i-yyyyyyyyy", ... "izzzzzzzzz"]. You can specify a maximum of 100 instance IDs. Separate multiple instance IDs with commas (,).
InstanceType	String	No	The instance type.
InstanceTypeFamily	String	No	The instance type family.
InstanceNetworkType	String	No	The network type of the instance.
PrivateIpAddresses	String	No	The private IP addresses of VPC-type instances. This parameter is effective when the network type of the instances is VPC. The parameter value is a JSON-formatted array: ["172.16.1.1","172.16.2.1",..."172.16.10.1"]. You can specify a maximum of 100 IP addresses. Separate multiple IP addresses with commas (,).
SecurityGroupId	String	No	The security group to which the instance belongs.
InstanceName	String	No	The instance name.
ImageId	String	No	The image ID.
Status	String	No	The status of the instance. Valid values: • Running • Starting • Stopping • Stopped
DeviceAvailable	String	No	Indicates whether disks can be attached to the instance. Valid values: True | False.
IoOptimized	String	No	Indicates whether the instance is I/O optimized. Valid values: True | False.
Tag.n.Key	String	No	The key of the tag. The value of n ranges from 1 to 5. It cannot be a null string.
Tag.n.Value	String	No	The value of the tag. The value of n ranges from 1 to 5. It can be a null string.
PageNumber	Integer	No	The page number that you query in the instance list. Starting value: 1. Default value: 1.

Name	Type	Required	Description
PageSize	Integer	No	The number of entries to be displayed per page. Maximum value: 100. Default value: 10.

Response parameters

Response parameter description

Name	Type	Description
TotalCount	Integer	The total number of instances.
PageNumber	Integer	The page number that you query in the instance list.
PageSize	Integer	The number of entries per page.
Instances	InstanceAttributesType	The returned instance information. It is an array consisting of InstanceAttributesType data.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidNetworkType.NotFound	The specified InstanceNetworkType is not found.	404	The error message returned when the specified network type does not exist.
InvalidStatus.NotFound	The specified Status is not found.	404	The error message returned when the specified status does not exist.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeInstances
&RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

- XML format

```
<DescribeInstancesResponse>
  <CreationTime>2014-09-21T01:12:35Z</CreationTime>
```

```
<DeviceAvailable>true</DeviceAvailable>
<Description></Description>
<EipAddress>
    <AllocationId></AllocationId>
  <InternetChargeType></InternetChargeType>
  <IpAddress></IpAddress>
</EipAddress>
<ExpiredTime>2011-09-08T16:00Z</ExpiredTime>
<HostName>iZ25skktcp4Z</HostName>
 <ImageId>ubuntu1404_64_20G_aliaegis_20140703.vhd</ImageId>
<InnerIpAddress></InnerIpAddress>
<InstanceChargeType>PostPaid</InstanceChargeType>
<IpAddress></IpAddress>
<InstanceId>i-25skktcp4</InstanceId>
<InstanceName>iZ25skktcp4Z</InstanceName>
<InstanceNetworkType>vpc</InstanceNetworkType>
<InstanceType>ecs.t1.xsmall</InstanceType>
<InternetChargeType></InternetChargeType>
<InternetMaxBandwidthIn>-1</InternetMaxBandwidthIn>
<InternetMaxBandwidthOut></InternetMaxBandwidthOut>
<IoOptimized>false</IoOptimized>
<OperationLocks>
    <LockReason></LockReason>
</OperationLocks>
<PublicIpAddress>
  <IpAddress></IpAddress>
</PublicIpAddress>
<RegionId>cn-beijing</RegionId>
<SecurityGroupIds>
    <SecurityGroupId>sg-25am0n4q0</SecurityGroupId>
</SecurityGroupIds>
<SerialNumber>51d1353b-22bf-4567-a176-8b3e12e43135</SerialNumber>
<Status>Running</Status>
<VlanId></VlanId>
<VpcAttributes>
  <NatIpAddress>10.175.68.212</NatIpAddress>
  <PrivateIpAddress>
     <IpAddress>192.168.2.3</IpAddress>
    </PrivateIpAddress>
  <VSwitchId>vsw-25gbsqby3</VSwitchId>
  <VpcId>vpc-25onv3oi4</VpcId>
```

```
    </VpcAttributes>
    <ZoneId>cn-beijing-a</ZoneId>
</DescribeInstancesResponse>
```

- JSON format

```
{
 "Instances": {
  "Instance": [
   {
    "CreationTime": "2015-07-27T07:08Z",
    "DeviceAvailable": true,
    "EipAddress": {},
    "ExpiredTime": "2011-09-08T16:00Z",
    "HostName": "iZ94t3s0jxkZ",
    "ImageId": "centos6u5_64_20G_aliaegis_20150130.vhd",
    "InnerIpAddress": {
     "IpAddress": [
      "10.170.106.80"
     ]
    },
    "InstanceChargeType": "PostPaid",
    "InstanceId": "i-94t3s0jxk",
    "InstanceName": "dd\u6027\u80fd\u6d4b\u8bd5",
    "InstanceNetworkType": "classic",
    "InstanceType": "ecs.s2.large",
    "InternetChargeType": "PayByTraffic",
    "InternetMaxBandwidthIn": -1,
    "InternetMaxBandwidthOut": 1,
    "IoOptimized": false,
    "OperationLocks": {
     "LockReason": []
    },
    "PublicIpAddress": {
     "IpAddress": [
      "120.25.13.106"
     ]
    },
    "RegionId": "cn-shenzhen",
    "SecurityGroupIds": {
     "SecurityGroupId": [
      "sg-94kd0cyg0"
```

```
        ]
      },
      "SerialNumber": "51d1353b-22bf-4567-a176-8b3e12e43135",
      "Status": "Running",
      "VpcAttributes": {
        "PrivateIpAddress": {
          "IpAddress": []
        }
      },
      "ZoneId": "cn-shenzhen-a"
    }
  ]
 },
 "PageNumber": 1,
 "PageSize": 10,
 "RequestId": "14A07460-EBE7-47CA-9757-12CC4761D47A",
 "TotalCount": 1
}
```


2.1.1.5.11. DescribeInstanceVncUrl

You can call this operation to query the URL of the Web management terminal for an ECS instance.

When you call this operation, note that:

- The URL for a management terminal is valid for 15 seconds. If a connection is not established within 15 seconds of the query, the URL will become invalid and must be queried again.
- The keepalive time of a management terminal connection is 60 seconds. If the user does not interact with the management terminal within 60 seconds, the connection will be automatically ended.
- Interrupted connections can be reconnected a maximum of 30 times a minute.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeInstanceVncUrl.
RegionId	String	Yes	The ID of the region to which the ECS instance belongs.
InstanceId	String	Yes	The ID of the ECS instance that you want to query.

Response parameters

Response parameter description

Name	Type	Description
VncUrl	String	The URL of the management terminal.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the specified instance is in a state that does not support the current operation.

Error code	Error message	HTTP status code	Description
InternalError	The request processing has failed due to some unknown error.	500	The error message returned when the current process failed due to some unknown errors.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeInstanceVncUrl
&DescribeInstanceVncUrl
&InstanceId=AY121018033933eae8689
&Common request parameters
```

Sample responses

- XML format

```
<DescribeInstanceVncUrlResponse>
  <RequestId>1450F2D7-5435-4420-BBC9-49C514B0157E</RequestId>
  <VncUrl>ws%3A%2F%2Fhz01-vncproxy.aliyun.com%2Fwebsockify%2F%3Fs%3DDvh%252FIA%252BYc7
3gWO48cBx2gBxUDVzaAnSKr74pq30mzqUYgeUMcB%252FbkNixDxdEA996</VncUrl>
</DescribeInstanceVncUrlResponse>
```

- JSON format

```
{
 "RequestId": "1450F2D7-5435-4420-BBC9-49C514B0157E",
 "VncUrl": "ws%3A%2F%2Fhz01-vncproxy.aliyun.com%2Fwebsockify%2F%3Fs%3DDvh%252FIA%252BYc7
3gWO48cBx2gBxUDVzaAnSKr74pq30mzqUYgeUMcB%252FbkNixDxdEA996"
}
```

2.1.1.5.12. DescribeUserdata

You can call this operation to query the custom data of an ECS instance.

When you call this operation, note that:

- The returned custom data is encoded by using Base64.
- If no custom data exists, a null value will be returned.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeUserdata.
RegionId	String	Yes	The ID of the region to which the instance belongs.
InstanceId	String	Yes	The ID of the instance to be queried.

Response parameters

Response parameter description

Name	Type	Description
UserData	String	The custom data of the instance. It is encoded by using Base64.
InstanceId	String	The ID of the instance.
RegionId	String	The ID of the region.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The specified RegionId does not exist.	404	The error message returned when the specified region ID does not exist.
InvalidInstanceId.NotFound	The specified InstanceId does not exist.	404	The error message returned when the specified instance ID does not exist.

Examples

Sample requests

```
https://ecs.example.com/?Action= DescribeUserdata
&RegionId=cn-shenzhen
&InstanceId=i-instance1
&Common request parameters
```

Sample responses

- XML format

```
<DescribeUserdataResponse>
   <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
   <UserData>userdata1</UserData>
   <InstanceId> i-instance1</InstanceId>
   <RegionId> cn-shenzhen </RegionId>
</DescribeUserdataResponse>
```

- JSON format

```
{
   "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
   " UserData ": " userdata1"
   " InstanceId ": " i-instance1"
   " RegionId": "cn-shenzhen"
}
```

2.1.1.5.13. DescribeInstanceRamRole

You can call this operation to query information about the instance RAM roles for one or more ECS instances.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeInstanceRamRole.
InstanceIds	String	Yes	A set of instance IDs that you want to query. You can specify a maximum of 100 instances, in the format of ["instanceId1", "instanceId2","instanceId3"...].
RamRoleName	String	No	Queries all the ECS instances to which the specified RAM role is attached. You can call the RAM operation ListRoles to query the RAM roles that you have created.

Response parameters

Name	Type	Description
InstanceRamRoleSets	Array	The returned information about an instance RAM role. It is an array consisting of InstanceRamRoleSetType data.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeInstanceRamRole &RegionId=cn-hangzhou
&InstanceIds=["i-instance1"]
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeInstanceRamRoleResponse>
<RequestId>8F4CAE3F-7892-4662-83A5-2C2FFD639553</RequestId>
<InstanceRamRoleSets>
<InstanceRamRoleSet>
<InstanceId>i-instance1</InstanceId>
<RamRoleName>RamRoleTest</RamRoleName>
</InstanceRamRoleSet>
</InstanceRamRoleSets>
<TotalCount>1</TotalCount>
</DescribeInstanceRamRoleResponse>
```

JSON format

```
{
"RequestId": "8F4CAE3F-7892-4662-83A5-2C2FFD639553",
"InstanceRamRoleSets": {
"InstanceRamRoleSet": [
{
"InstanceId": "i-instance1",
"RamRoleName": "RamRoleTest"
}
]
},
"TotalCount": 1
}
```

Error codes

Error code	Error message	HTTP status code	Description

Error code	Error message	HTTP status code	Description
InvalidInstanceIds.Malformed	The specified InstanceIds is not valid.	400	The error message returned when the specified InstanceIds parameter is invalid.
InvalidInstanceId.NotFound	The specified InstanceId does not exist.	404	The error message returned when the specified instance ID does not exist.
InvalidRamRole.NotFound	The specified RamRoleName does not exist.	404	The error message returned when the specified RAM role name does not exist.

2.1.1.5.14. DescribeInstanceTypeFamilies

You can call this operation to query the instance type families provided by ECS.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeInstanceTypeFamilies.
RegionId	String	Yes	The ID of the region. You can call DescribeRegions to view latest regions.
Generation	String	No	The generation of the instance type family. Valid values: • ecs-1: Generation I, which consists of the earliest and most cost-effective instance types. • ecs-2: Generation II, which features upgraded hardware and higher performance than Generation I. • ecs-3: Generation III, which consists of the latest and highest performance instance types.

Response parameters

Name	Type	Description
InstanceTypeFamilies	InstanceTypeFamilyItemType	A set of InstanceTypeFamilyItemType data.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeInstanceTypeFamilies
&RegionId=cn-hangzhou
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeInstanceTypeFamiliesResponse>
<InstanceTypeFamilies>
<InstanceTypeFamily>
<InstanceTypeFamilyId>ecs.t1</InstanceTypeFamilyId>
<Generation>ecs-1</Generation>
</InstanceTypeFamily>
<InstanceTypeFamily>
<InstanceTypeFamilyId>ecs.s2</InstanceTypeFamilyId>
<Generation>ecs-1</Generation>
</InstanceTypeFamily>
<InstanceTypeFamily>
<InstanceTypeFamilyId>ecs.s3</InstanceTypeFamilyId>
<Generation>ecs-1</Generation>
</InstanceTypeFamily>
</InstanceTypeFamilies>
<RequestId>6B187E0A-C075-4D08-8B6F-6213950E8733</RequestId>
</DescribeInstanceTypeFamiliesResponse>
```

JSON

```
{
"InstanceTypeFamilies":{
"InstanceTypeFamily":[
{
"InstanceTypeFamilyId":"ecs.t1",
"Generation":"ecs-1"
},
{
"InstanceTypeFamilyId":"ecs.s2",
"Generation":"ecs-1"
},
{
"InstanceTypeFamilyId":"ecs.s3",
"Generation":"ecs-1"
}
]
},
"RequestId":"6B187E0A-C075-4D08-8B6F-6213950E8733"
}
```


Error codes

This operation returns only common errors.

2.1.1.5.15. DescribeInstanceTypes

You can call this operation to query the instance types provided by ECS.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeInstanceTypes.
InstanceTypeFamily	String	No	The instance type family. For more information, see **Instance type family** in *ECS Product Introduction*.

Response parameters

Name	Type	Description

Name	Type	Description
InstanceTypes	InstanceTypeItemType	A set of InstanceTypeItemType data.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeInstanceTypes
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeInstanceTypesResponse>
<RequestId>1651FBB6-4FBF-49FF-A9F5-DF5D696C7EC6</RequestId>
<InstanceTypes>
<InstanceType>
<InstanceTypeId>ecs.t1.xsmall</InstanceTypeId>
<CpuCoreCount>1</CpuCoreCount>
<MemorySize>0.5</MemorySize>
</InstanceType>
<InstanceType>
<InstanceTypeId>ecs.t1.small</InstanceTypeId>
<CpuCoreCount>1</CpuCoreCount>
<MemorySize>1</MemorySize>
</InstanceType>
</InstanceTypes>
</DescribeInstanceTypesResponse>
```

JSON format

```
{
"RequestId": "1651FBB6-4FBF-49FF-A9F5-DF5D696C7EC6",
"InstanceTypes": {
"InstanceType": [{
"InstanceTypeId": "ecs.t1.xsmall",
"CpuCoreCount": 1,
"MemorySize": 0.5
},
{
"InstanceTypeId": "ecs.t1.small",
"CpuCoreCount": 1,
"MemorySize": 1
}]
}
}
```


Error codes

This operation returns only common errors.

2.1.1.5.16. ModifyInstanceAttribute

You can call this operation to modify the attributes of an instance, such as the password, name, and security group.

When you call this operation, note that:

- This operation modifies only the attributes specified in the request parameters.
- The password of an instance in the Deleted or Starting state cannot be reset. The new password takes effect only after the instance is restarted.
- If an instance is locked for security reasons (the OperationLocks parameter is "LockReason": "security"), the password of the instance cannot be modified.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyInstanceAttribute.
InstanceId	String	Yes	The ID of the instance.

Name	Type	Required	Description
InstanceName	String	No	The name of the instance. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It cannot start with `http://` or `https://`.
Description	String	No	The description of the instance. The description must be 2 to 256 characters in length. It is displayed in Apsara Stack console. Default value: null. It cannot start with `http://` or `https://`.
Password	String	No	The password that you want to specify. The password is a string of 8 to 30 characters and must contain uppercase or lowercase letters, digits, and special characters. The password can contain any of the following special characters: ( ) ` ~ ! @ # $ % ^ & * - + = | { } [ ] : ; ' < > ,. ? / If the Password parameter is specified, you must use HTTPS to call the operation to ensure the password remains confidential.
UserData	String	No	The custom data of the instance. It is encoded by using Base64. The maximum size of the raw data is 16 KB.
HostName	String	No	The hostname in the operating system. It must contain at least two characters. It cannot start or end with a period (.) or hyphen (-). It cannot contain consecutive periods (.) or hyphens (-). On Windows, the hostname must be 1 to 15 characters in length and can contain a combination of uppercase or lowercase letters, digits, and hyphens (-). The hostname cannot contain periods (.) or contain only digits. On other OSs such as Linux, the hostname must be 1 to 30 characters in length and can contain multiple segments separated with periods (.). Each segment can contain uppercase or lowercase letters, digits, and hyphens (-).

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	404	The error message returned when the specified instance ID does not exist.
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.
InvalidInstanceName.Malformed	The specified parameter InstanceName is not valid.	400	The error message returned when the format of the InstanceName parameter is invalid.
InvalidDescription.Malformed	The specified parameter Description is not valid.	400	The error message returned when the format of the Description parameter is invalid.
InvalidHostPassword.Malformed	The specified parameter Password is not valid.	400	The error message returned when the format of the Password parameter is invalid.
InvalidHostName.Malformed	The specified parameter HostName is not valid.	400	The error message returned when the format of the HostName parameter is invalid.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when this operation is not supported under the current instance status.
InvalidUserData.SizeExceeded	The specified parameter UserData exceeds the size.	400	The error message returned when the raw data size exceeds 16 KB.

Error code	Error message	HTTP status code	Description
InvalidUserData.NotSupported	The specified parameter UserData only support the vpc and IoOptimized Instance.	400	The error message returned when the UserData parameter is not specified in a VPC or I/O optimized instance.
InstanceLockedForSecurity	The specified operation is denied as your instance is locked for security reasons.	403	The error message returned when the specified instance is locked for security reasons.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifyInstanceAttribute
&InstanceId=i-instance1
&Password=pwd
&Common request parameters
```

Sample responses

- XML format

```
<ModifyInstanceAttributeResponse>
    <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</ModifyInstanceAttributeResponse>
```

- JSON format

```
{
    "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

2.1.1.5.17. ModifyInstanceVpcAttribute

You can call this operation to modify the VPC attributes of an ECS instance.

When you call this operation, note that:

- If you change the VSwitchId attribute of a VPC, the new VSwitch must belong to the same VPC.
- The current VSwitch and the new VSwitch of the specified instance must belong to the same zone.

- When you specify the VSwitchId parameter and do not specify the PrivateIpAddress parameter, the system automatically allocates an idle private IP address to the ECS instance.
- When you specify both the VSwitchId and PrivateIpAddress parameters, the specified private IP address must be within the range of the VSwitch CIDR block.
- The PrivateIpAddress parameter depends on the VSwitch and cannot be specified separately.
- Only ECS instances that are in the Stopped state can have their attributes modified. For newly created ECS instances, the ECS must be started and stopped at least once before its VSwitch can be changed.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyInstanceVpcAttribute.
InstanceId	String	Yes	The ID of the instance.
VSwitchId	String	Yes	The ID of the new VSwitch. The new VSwitch of the instance must belong to the same zone as the original VSwitch.
PrivateIpAddress	String	No	The new private IP address. This parameter cannot be specified separately.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidVSwitchId.NotFound	Specified virtual switch does not exist.	404	The error message returned when the specified VSwitch ID does not exist.
InvalidVSwitchId.Mismatch	Specified instance and virtual switch are not in the same zone.	400	The error message returned when the specified instance and VSwitch do not belong to the same zone.
InvalidInstanceId.NotFound	Specified instance does not exist.	404	The error message returned when the specified ECS instance does not exist.

Error code	Error message	HTTP status code	Description
InvalidPrivateIpAddress.Mismatch	Specified private IP address is not in the CIDR block of virtual switch.	400	The error message returned when the specified private IP address is not within the CIDR block range of the specified VSwitch.
InvalidPrivateIpAddress.Malformed	Specified private IP address is malformed.	400	The error message returned when the specified private IP address is invalid.
InvalidPrivateIpAddress.Duplicated	Specified private IP address is duplicated.	400	The error message returned when the specified private IP address is already in use.
InvalidPrivateIp.Changing	Previous action is not finished yet.	400	The error message returned when the private IP address cannot be modified because a previous modification operation has not yet finished.
InvalidVSwitchId.NotFound	Specified virtual switch is not found in current VPC.	404	The error message returned when the specified VSwitch does not belong to the current VPC.
IncorrectInstanceStatus	The current status of instance does not support this operation.	400	The error message returned when the operation fails because the instance is not in the Stopped state.
OperationDenied	Specified operation is denied as your instance is not in VPC.	400	The error message returned when the instance does not belong to a VPC.
InvalidPrivateIp.Changing	Specified private IP address is not in the CIDR block of virtual switch.	400	The error message returned when the private IP address is being modified. The private IP address can be modified only once when the instance is stopped.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifyInstanceVpcAttribute
&InstanceId=35F20777-0DFF-C152-41FA-BCE0EA0B2FD7
&VSwitchId=[vswitchid]
&Common request parameters
```

Sample responses

- XML format

```
<ModifyInstanceAttributeResponse>
  <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</ModifyInstanceAttributeResponse>
```

- JSON format

```
{
  "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

2.1.1.5.18. ModifyInstanceVncPasswd

You can call this operation to modify the VNC password of an ECS instance.

When you call this operation, note that:

- The password must be six characters in length and contain uppercase letters, lowercase letters, and digits.
- For I/O optimized instances, the password takes effect immediately after the password is modified and no restart is required. For a non-I/O optimized instance, you must restart the instance for the password modification to take effect.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyInstanceVncPasswd.
RegionId	String	Yes	The ID of the region to which the ECS instance belongs.
InstanceId	String	Yes	The ID of the ECS instance.
VncPassword	String	Yes	The VNC password that you want to specify for the ECS instance.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403
InternalError	The request processing has failed due to some unknown error.	500
IncorrectVncPassword.Malformed	The specified parameter VncPassword is not valid.	400

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifyInstanceVncPasswd
&DescribeInstanceVncUrl
&InstanceId=AY121018033933eae8689
&VncPassword=123456
&Common request parameters
```

Sample responses

- XML format

```
<ModifyInstanceVncPasswdResponse>
  <RequestId>FDB6C963-9CE8-4B7F-BCA3-845F6BD29AFC</RequestId>
</ModifyInstanceVncPasswdResponse>
```

- JSON format

```
{
 "RequestId": "FDB6C963-9CE8-4B7F-BCA3-845F6BD29AFC",
}
```

2.1.1.6. Deployment set

2.1.1.6.1. CreateDeploymentSet

You can call this operation to create a deployment set. You can specify ECS instances in a deployment set.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateDeploymentSet.
RegionId	String	Yes	The ID of the region to which the deployment set belongs. You can call DescribeRegions to view available regions. For more information, see DescribeRegions.
ZoneId	String	Yes	The ID of the zone to which the deployment set belongs.
Description	String	No	The description of the deployment set. The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency in the Appendix.
DeploymentSetName	String	No	The name of the deployment set. If not specified, this parameter is null. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It is displayed in Apsara Stack console. It cannot start with `http://` or `https://`.
Domain	String	No	The deployment domain. Valid values: Default and Switch. Default value: Default.

Name	Type	Required	Description
Granularity	String	No	The deployment granularity. Valid values: • Host: The minimum scheduling granularity is a physical server. This is the default value. • Rack: The minimum scheduling granularity is a rack. • Switch: The minimum scheduling granularity is a VSwitch. If the deployment domain is Switch, the deployment granularity cannot be set to Switch.
Strategy	String	No	The deployment policy. • LooseDispersion: dispersed as much as possible. This is the default value. • LooseAggregation: aggregated as much as possible. • StrictAggregation: strictly aggregated. • StrictDispersion: strictly dispersed. If the deployment granularity is Switch, any of the four preceding policies can be specified. If the deployment granularity is Rack or Host, only the LooseDispersion or StrictDispersion policy can be specified.

Response parameters

Response parameter description

Name	Type	Description
DeploymentSetId	String	The ID of the deployment set.

Note The DeploymentSetId value is a serial number starting with ds-, such as a ds-ti0ekhm.

Error codes

Error code description

Error code	Error message	HTTP status code	Description

Error code	Error message	HTTP status code	Description
DependencyViolation.domain.granularity	The DeploymentSet domain and granularity is violation.	400	The error message returned when the specified deployment domain conflicts with the specified deployment granularity.
DependencyViolation.strategy.granularity	The DeploymentSet strategy and granularity is violation.	400	The error message returned when the specified deployment policy conflicts with the specified deployment granularity.
DEPLOYMENTSET.QUOTA_FULL	The deploymentSet quota is full	400	The error message returned when the deployment set quota has been reached.
InvalidDeploymentSetId.NotFound	The DeploymentSetId provided does not exist in our records.	400	The error message returned when the specified deployment set does not exist.
InvalidDescription.Malformed	The specified parameter Description is not valid.	400	The error message returned when the format of the Description parameter is invalid.
InvalidParameter.Domain	The specified parameter Domain is not valid.	400	The error message returned when the specified deployment domain is invalid.
InvalidParameter.granularity	The specified parameter Granularity is not valid.	400	The error message returned when the specified deployment granularity is invalid.
InvalidParameter.Strategy	The specified parameter Strategy is not valid	400	The error message returned when the specified deployment policy is invalid.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required RegionId parameter is not specified or when you are not authorized to access this region. RegionId You can call DescribeRegions to view available regions. For more information, see DescribeRegions.
MissingParameter	The input parameter DeploymentSetId that is mandatory for processing this request is not supplied.	400	The error message returned when the required DeploymentSetId parameter is not specified.
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist. You can call DescribeRegions to view available regions. For more information, see DescribeRegions.
InvalidZoneId.NotFound	The ZoneId provided does not exist in our records.	404	The error message returned when the specified zone ID does not exist.

2.1.1.6.2. DeleteDeploymentSet

You can call this operation to delete a deployment set.

When you call this operation, note that only deployment sets containing no instances can be deleted.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteDeploymentSet.

Name	Type	Required	Description
RegionId	String	Yes	The ID of the region to which the deployment set belongs. You can call DescribeRegions to view available regions. For more information, see DescribeRegions.
DeploymentSetId	String	Yes	The ID of the deployment set.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter DeploymentSetId that is mandatory for processing this request is not supplied.	400	The error message returned when the required DeploymentSetId parameter is not specified.
DependencyViolation.NotEmpty	There are still instance(s) in the specified DeploymentSetId.	403	The error message returned when the specified deployment set contains instances and cannot be deleted.
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist. You can call DescribeRegions to view available regions. For more information, see DescribeRegions.

2.1.1.6.3. ModifyDeploymentSetAttribute

You can call this operation to modify the attributes of a deployment set.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDeploymentSetAttribute.
RegionId	String	Yes	The ID of the region to which the deployment set belongs. You can call DescribeRegions to view available regions. For more information, see DescribeRegions.
DeploymentSetId	String	Yes	The ID of the deployment set.
DeploymentSetName	String	No	The name of the deployment set. If not specified, this parameter is null. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It is displayed in Apsara Stack console. It cannot start with `http://` or `https://`.
Description	String	No	The description of the deployment set. The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidDescription.Malformed	The specified parameter Description is not valid.	400	The error message returned when the format of the Description parameter is invalid.
InvalidPlacmentSetName.Malformed	Specified plamcent set name is not valid.	400	The error message returned when the format of the PlacmentSetName parameter is invalid.
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required RegionId parameter is not specified or when you are not authorized to access this region. You can call DescribeRegions to view available regions. For more information, see DescribeRegions.
MissingParameter	The input parameter DeploymentSetId that is mandatory for processing this request is not supplied.	400	The error message returned when the required DeploymentSetId parameter is not specified.
InvalidDeploymentSetId.NotFound	The DeploymentSetId provided does not exist in our records.	404	The error message returned when the specified deployment set does not exist.
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist. You can call DescribeRegions to view available regions. For more information, see DescribeRegions.

2.1.1.6.4. DescribeDeploymentSets

You can call this operation to query deployment sets.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDeploymentSets.
RegionId	String	Yes	The ID of the region to which the deployment set belongs. You can call DescribeRegions to view available regions. For more information, see DescribeRegions.
DeploymentSetIds	String	Yes	The IDs of deployment sets. The parameter value is a JSON-formatted array: [“ps-xxxxxxxxx” , ” ps-yyyyyyyyy” , ... “ps-zzzzzzzzz”]. You can specify a maximum of 100 IDs. Separate multiple deployment sets with commas (,).
DeploymentSetName	String	No	The name of the deployment set.
Domain	String	No	The deployment domain. Valid values: Default and Switch. Default value: Default.
Granularity	String	No	The deployment granularity. Valid values: • Host: The minimum scheduling granularity is a physical server. This is the default value. • Rack: The minimum scheduling granularity is a rack. • Switch: The minimum scheduling granularity is a VSwitch.

Name	Type	Required	Description
Strategy	String	No	The deployment policy. Valid values: • LooseDispersion: dispersed as much as possible. This is the default value. • LooseAggregation: aggregated as much as possible. • StrictAggregation: strictly aggregated. • StrictDispersion: strictly dispersed. If the deployment granularity is Switch, any of the four preceding policies can be specified. If the deployment granularity is Rack or Host, only the LooseDispersion or StrictDispersion policy can be specified.
PageNumber	Integer	No	The page number that you query in the instance status list. Starting value: 1. Default value: 1.
PageSize	Integer	No	The number of entries per page. Maximum value: 100. Default value: 10.

Response parameters

Response parameter description

Name	Type	Description
TotalCount	Integer	The total number of entries.
PageNumber	Integer	The page number that you query in the instance status list.
PageSize	Integer	The number of entries per page.
DeploymentSetList	DeploymentSetType	A set of DeploymentSetType data.

2.1.1.6.5. DescribeDeploymentSetTopology

You can call this operation to obtain the physical topology of a deployment set.

Request parameters

Request parameter description

Name	Type	Required	Description
DeploymentSetId	String	Yes	The ID of the deployment set.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDeploymentSetTopology.
RegionId	String	Yes	The ID of the region to which the deployment set belongs. You can call DescribeRegions to view available regions.

Response parameters

Response parameter description

Name	Type	Description
Switchs	Switch	The returned instance information. It is an array consisting of Switch data.
Racks	Rack	The returned instance information. It is an array consisting of Rack data.
RegionId	String	The region ID.
DeploymentSetId	String	The ID of the deployment set.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidDeploymentSetId.NotFound	The DeploymentSetId provided does not exist in our records.	404	The error message returned when the specified deployment set does not exist.
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.

2.1.1.7. Disks

2.1.1.7.1. CreateDisk

You can call this operation to create a disk.

When you call this operation, note that:

- This operation allows you to create detachable data disks, such as basic disks, ultra disks, and SSD disks. Snapshots of system disks cannot be used to create data disks.
- By default, the DeleteAutoSnapshot parameter is set to true when a disk is created. This indicates that when the disk is released, snapshots that were created from the disk are deleted together with the disk. You can call ModifyDiskAttribute to modify the parameter value. The Portable attribute of disks created by calling this operation is set to true.
- When creating the disk, you must specify either the Size or SnapshotId parameter.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateDisk.
RegionId	String	Yes	The ID of the region to which the instance belongs.
ZoneId	String	Yes	The ID of the zone.
DiskName	String	No	The name of the disk. If not specified, this parameter is null. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It is displayed in Apsara Stack console. It cannot start with `http://` or `https://`.
Description	String	No	The description of the disk. If not specified, this parameter is null. Default value: null. The description must be 2 to 256 characters in length. It is displayed in Apsara Stack console. It cannot start with `http://` or `https://`.
Encrypted	Boolean	No	Indicates whether the disk is encrypted. Valid values: • true • false Default value: false.
DiskCategory	String	No	The category of the data disk. Valid values: • cloud: basic disk • cloud_efficiency: ultra disk • cloud_ssd: SSD disk Default value: cloud.

Name	Type	Required	Description
Size	Integer	No	The disk capacity. Unit: GiB. • cloud: 5 to 2000 • cloud_efficiency: 20 to 2048 • cloud_ssd: 20 to 1024 The Size value of the data disk must be greater than or equal to the SnapshotId value.
SnapshotId	String	No	When this parameter is specified for the snapshot used to create the data disk, the Size parameter will be ignored, and the actual size to be allocated to the disk will be the same as that of the specified snapshot.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency.

Response parameters

Response parameter description

Name	Type	Description
DiskId	String	The disk ID.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required RegionId parameter is not specified.
MissingParameter	The input parameter ZoneId that is mandatory for processing this request is not supplied.	400	The error message returned when the required ZoneId parameter is not specified or when you are not authorized to access the zone.

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The specified region does not exist.	404	The error message returned when the specified region ID does not exist.
InvalidZoneId.NotFound	The specified zone does not exist.	404	The error message returned when the specified zone ID does not exist.
InvalidSnapshotId.NotFound	The specified snapshot does not exist.	404	The error message returned when the specified snapshot ID does not exist.
InvalidDiskName.Malformed	The specified disk name is wrongly formed.	400	The error message returned when the format of the DiskName parameter is invalid.
InvalidDescription.Malformed	The specified description is wrongly formed.	400	The error message returned when the format of the DescriptionName parameter is invalid.
InvalidParameter	The specified parameter Size is not valid.	400	The error message returned when the Size parameter is invalid.
InstanceDiskCategoryLimitExceed	The total size of specified disk category in an instance exceeds.	403	The error message returned when the total size of specified disks exceeds the maximum capacity of a single instance.
InvalidSnapshot.TooLarge	The capacity of snapshot exceeds 2000 GB.	403	The error message returned when the capacity of the specified snapshot exceeds the maximum capacity of the disk category.
OperationDenied	The specified snapshot is not allowed to create disk.	403	The error message returned when the specified snapshot cannot be used to create a disk.

Error code	Error message	HTTP status code	Description
QuotaExceed.PortableCloudDisk	The quota of portable cloud disk exceeds.	403	The error message returned when the number of detachable basic disks exceeds the quota.
MissingParameter	The input parameter either SnapshotId or Size should be specified.	400	The error message returned when one of the required SnapshotId or Size parameter is not specified.
InvalidDiskCategory.ValueUnauthorized	The disk category is not authorized.	403	The error message returned when the specified disk category is unauthorized.
InvalidSnapshotId.NotReady	The specified snapshot has not completed yet.	403	The error message returned when the specified snapshot is not completely created.
InvalidSnapshotId.NotDataDiskSnapshot	The specified snapshot is system disk snapshot.	403	The error message returned when the specified snapshot is not a data disk snapshot and cannot be used to create a data disk.
InvalidSnapshotId.NotFound	The specified snapshot does not exist.	404	The error message returned when the specified snapshot does not exist.

Examples

Sample requests

```
https://ecs.example.com/?action=CreateDisk
&RegionId=cn-qingdao
&ZoneId=cn-qingdao-b
&Size=200
&DiskName=ThisIsDiskName
&Description=ThisIsDescription&
&Common request parameters
```

Sample responses

- XML format

```
<CreateDiskResponse>
  <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</CreateDiskResponse>
```

- JSON format

```
{
  "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

2.1.1.7.2. DescribeDisks

You can call this operation to query disks.

When you call this operation, note that:

- Request parameters such as RegionId, ZoneId, DiskIds, and InstanceId act as filtering conditions and have a boolean `AND` relationship with each other.
- The DiskIds value is a JSON-formatted array. If the parameter is not specified, no filtering condition is applied. If the DiskIds parameter is an empty JSON array ([]), the filtering condition will be applied and a blank result will be returned.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDisks.
RegionId	String	Yes	The ID of the region to which the disk belongs.
ZoneId	String	No	Default value: null, indicating that disks in all zones are queried.

Name	Type	Required	Description
DiskIds	String	No	The disk IDs. The parameter value is an array of disk IDs, such as ["d-xxxxxxxxx", "dyyyyyyyyy", ... "dzzzzzzzzz"]. You can specify a maximum of 100 disk IDs at a time. Separate multiple IDs with commas (,).
InstanceId	String	No	The ID of the instance.
DiskType	String	No	The type of the disk. Valid values: all | system | data. Default value: all.
Category	String	No	The category of the disk. Valid values: all | cloud | cloud_efficiency | cloud_ssd | ephemeral | ephemeral_ssd. Default value: all.
Status	String	No	The disk status. Valid values: In_use | Available | Attaching | Detaching | Creating | ReIniting | All. Default value: All.
SnapshotId	String	No	The ID of the snapshot used to create the disk.
DiskName	String	No	The name of the disk.
Portable	String	No	Indicates whether the disk is detachable. • true: The disk can be attached to or detached from instances within the same zone. • false: The disk cannot be detached, and is created or released together with the instance it is attached to. To attach or detach a disk, you must first check that this attribute of the disk is true. This attribute is set to false for system disks of basic cloud disks, ultra disks, and SSD cloud disks. This attribute cannot be modified.
DeleteWithInstance	String	No	Indicates whether the disk is released together with the instance: • true: When the instance is released, the disk will be released with it. • false: When the instance is released, the disk will not be released.

Name	Type	Required	Description
DeleteAutoSnapshot	String	No	Indicates whether the automatic snapshot is deleted when the disk is released. • true • false
EnableAutoSnapshot	String	No	Indicates whether disks that apply automatic snapshot policies are queried. This parameter can be set only when the automatic snapshot policy function is enabled for your account. Valid values: • true: Disks that apply automatic snapshot policies are queried. • false: Disks that apply automatic snapshot policies are not queried. Default value: null, indicating that the parameter value remains unchanged and the parameter is not included in the filtering conditions.
Tag.n.Key	String	No	The key of the tag. The value of n ranges from 1 to 5. It cannot be a null string.
Tag.n.Value	String	No	The value of the tag. The value of n ranges from 1 to 5. It can be a null string.
PageNumber	Integer	No	The page number that you query in the disk status list. Starting value: 1. Default value: 1.
PageSize	Integer	No	The number of entries per page. Maximum value: 100. Default value: 10.

Response parameters

Response parameter description

Name	Type	Required
TotalCount	Integer	The total number of disks.
PageNumber	Integer	The page number that you query in the disk list.
PageSize	Integer	The number of entries per page.
Disks	DiskItemType	A set of DiskItemType data.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidDiskType.ValueNotSupported	The specified disk type is not supported.	400	The error message returned when the specified disk type does not support the operation.
InvalidCategory.ValueNotSupported	The specified disk category is not supported.	400	The error message returned when the specified disk category is not supported or you are not authorized to perform the operation.
InvalidStatus.ValueNotSupported	The specified disk status is not supported.	400	The error message returned when the operation is not supported in the current status of the disk.
InvalidDiskIds.Malformed	The amount of specified disk Ids exceeds the limit.	403	The error message returned when the format of the DiskId parameter is invalid.
InvalidDiskChargeType.NotFound	The DiskChargeType does not exist in our records	404	The error message returned when the specified DiskChargeType parameter does not exist.
InvalidLockReason.NotFound	The specified LockReason is not found	404	The error message returned when the specified LockReason parameter does not exist.
InvalidTag.Mismatch	The specified Tag.n.Key and Tag.n.Value does not match.	400	The error message returned when the specified Tag.n.Key and Tag.n.Value parameters do not match.
InvalidTagCount	The specified tags are beyond the permitted range.	400	The error message returned when more than five tags are specified.
InvalidRegion.NotFound	The specified parameter RegionId is not valid.	400	The error message returned when the specified region ID does not exist.
InvalidZoneId.NotFound	The zoneId provided does not exist in our records.	400	The error message returned when the specified zone ID does not exist.

Examples

Sample requests

```
https://ecs.example.com/?action=DescribeDisks
&RegionId=cn-qingdao
&PageNumber=1
&ZoneId=cn-qingdao-b
&Common request parameters
```

Sample responses

- XML format

```
<DescribeDisksResponse>
  <Disks>
    <Disk>
      <DeleteAutoSnapshot>true</DeleteAutoSnapshot>
      <DeleteWithInstance>false</DeleteWithInstance>
      <EnableAutoSnapshot>false</EnableAutoSnapshot>
      <Category>cloud</Category>
      <Description></Description>
      <DiskName></DiskName>
      <Size>5</Size>
      <Type>data</Type>
      <InstanceId></InstanceId>
      <CreationTime>2014-07-23T02:44:07Z</CreationTime>
      <ImageId></ImageId>
      <ZoneId>cn-qingdao-b</ZoneId>
      <AttachedTime>2014-07-23T07:47:35Z</AttachedTime>
      <DetachedTime>2014-07-23T08:28:48Z</DetachedTime>
      <Device></Device>
      <OperationLocks></OperationLocks>
      <Portable>true</Portable>
      <ProductCode></ProductCode>
      <RegionId>cn-qingdao</RegionId>
      <DiskId>d-28m5zbua0</DiskId>
      <SourceSnapshotId></SourceSnapshotId>
      <Status>Available</Status>
    </Disk>
    <Disk>
      <DeleteAutoSnapshot>true</DeleteAutoSnapshot>
      <DeleteWithInstance>false</DeleteWithInstance>
      <EnableAutoSnapshot>false</EnableAutoSnapshot>
      <Category>cloud</Category>
```

```
        <Description></Description>
        <DiskName></DiskName>
        <Size>5</Size>
        <Type>data</Type>
        <InstanceId></InstanceId>
        <CreationTime>2014-07-23T02:44:06Z</CreationTime>
        <ImageId></ImageId>
        <ZoneId>cn-qingdao-b</ZoneId>
        <AttachedTime></AttachedTime>
        <DetachedTime></DetachedTime>
        <Device></Device>
        <OperationLocks></OperationLocks>
        <Portable>true</Portable>
        <ProductCode></ProductCode>
        <RegionId>cn-qingdao</RegionId>
        <DiskId>d-28zfrmo13</DiskId>
        <SourceSnapshotId></SourceSnapshotId>
        <Status>Available</Status>
      </Disk>
    </Disks>
    <PageNumber>1</PageNumber>
    <PageSize>2</PageSize>
    <TotalCount>9</TotalCount>
    <RequestId>ED5CF6DD-71CA-462C-9C94-A61A78A01479</RequestId>
</DescribeDisksResponse>
```

- JSON format

```
{
  "Disks": {
    "Disk": [
      {
        "AttachedTime": "2014-07-23T07:47:35Z",
        "Category": "cloud",
        "CreationTime": "2014-07-23T02:44:07Z",
        "DeleteAutoSnapshot": true,
        "DeleteWithInstance": false,
        "EnableAutoSnapshot": false
        "Description": "",
        "DetachedTime": "2014-07-23T08:28:48Z",
        "Device": "",
        "DiskId": "d-28m5zbua0"
```

```
      "DiskId": "d-28fn5zbda0",
      "DiskName": "",
      "ImageId": "",
      "InstanceId": "",
      "OperationLocks": {
        "OperationLock": []
      },
      "Portable": true,
      "ProductCode": "",
      "RegionId": "cn-qingdao",
      "Size": 5,
      "SourceSnapshotId": "",
      "Status": "Available",
      "Type": "data",
      "ZoneId": "cn-qingdao-b"
    },
    {
      "AttachedTime": "",
      "Category": "cloud",
      "CreationTime": "2014-07-23T02:44:06Z",
      "DeleteAutoSnapshot": true,
      "DeleteWithInstance": false,
      "EnableAutoSnapshot": false
      "Description": "",
      "DetachedTime": "",
      "Device": "",
      "DiskId": "d-28zfrmo13",
      "DiskName": "",
      "ImageId": "",
      "InstanceId": "",
      "OperationLocks": {
        "OperationLock": []
      },
      "Portable": true,
      "ProductCode": "",
      "RegionId": "cn-qingdao",
      "Size": 5,
      "SourceSnapshotId": "",
      "Status": "Available",
      "Type": "data",
      "ZoneId": "cn-qingdao-b"
    }
```

```
    ]
  },
  "PageNumber": 1,
  "PageSize": 2,
  "RequestId": "ACD9BBB0-A9D1-46D7-9630-B7A69889E110",
  "TotalCount": 9
}
```


2.1.1.7.3. AttachDisk

You can call this operation to attach a disk to an instance.

When you call this operation, note that:

- The operation can be performed only when the instance is in the Running or Stopped state, and the instance is not locked for security reasons.
- If the instance is locked for security reasons, the DeleteWithInstance attribute will be ignored and the disk will be released together with the instance.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AttachDisk.
InstanceId	String	Yes	The ID of the instance to which you want to attach a disk.
DiskId	String	Yes	The ID of the disk to be attached. The disk and the instance must belong to the same zone.
Device	String	No	The value null indicates that the value is allocated by default, starting from /dev/xvdb to /dev/xvdz. Default value: null.
DeleteWithInstance	String	No	Indicates whether the disk is to be released together with the instance: • true: When the instance is released, the disk will be released with it. • false: When the instance is released, the disk will not be released. Default value: null, indicating that the parameter value remains unchanged.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.
MissingParameter	The input parameter DiskId that is mandatory for processing this request is not supplied.	400	The error message returned when the required DiskId parameter is not specified.
InvalidInstanceId.NotFound	The specified instances do not exist.	404	The error message returned when the specified instance ID does not exist.
InvalidDiskId.NotFound	The specified region does not exist.	404	The error message returned when the specified disk does not exist.
InvalidDevice.Malformed	The specified device is not valid.	400	The error message returned when the specified disk does not exist.
InvalidParameter	The specified parameter DeleteWithInstance is not valid.	400	The error message returned when the specified DeleteWithInstance parameter is invalid.
InstanceDiskLimitExceeded	The amount of the disk on instance in question reach its limits.	403	The error message returned when the number of disks has already reached the upper limit supported by the specified instance.

Error code	Error message	HTTP status code	Description
InvalidDevice.InUse	The specified device has been occupied.	403	The error message returned when the specified device already has an attached disk.
IncorrectDiskStatus	The operation is not supported in this status.	403	The error message returned when this operation is not supported under the current disk status.
DiskNotPortable	It is not a portable disk.	403	The error message returned when the specified disk cannot be detached.
InstanceLockedForSecurity	The instance is locked due to security.	403	The error message returned when the specified instance is locked for security reasons.
ResourcesNotInSameZone	The specified instance and disk are not in the same zone.	403	The error message returned when the specified disk and instance are not in the same zone.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	400	The error message returned when this operation is not supported under the current instance status.
DiskError	IncorrectDiskStatus	403	The error message returned when the disk is in an abnormal state.

Examples

Sample requests

```
https://ecs.example.com/?action=AttachDisk
&InstanceId=i-23jggx34b
&DiskId=d-23jbf2v5m
&Common request parameters
```

Sample responses

- XML format

```
<AttachDiskResponse>
  <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</AttachDiskResponse>
```

- JSON format

```
{
  "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

2.1.1.7.4. DetachDisk

You can call this operation to detach a disk from an instance.

When you call this operation, note that:

- The operation can be performed only when all the following conditions are met: the Portable attribute of the disk is true, the instance that the disk is attached to is in the Running or Stopped state, and the instance is not locked for security reasons.
- After an independent basic cloud disk is detached from an instance by this operation, the DeleteWithInstance attribute will be set to false.
- If the disk specified in the DiskId parameter is not attached to the instance specified in the InstanceId parameter, this operation will fail.
- The DetachDisk operation is asynchronous. After the response is returned, it will take about one minute before the disk is detached.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DetachDisk.
InstanceId	String	Yes	The ID of the instance from which you want to detach the disk.
DiskId	String	Yes	The disk ID. The disk and the instance must belong to the same zone.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidInstanceId.NotFound	The specified instances do not exist.	404	The error message returned when the specified instance ID does not exist.
InvalidDiskId.NotFound	The specified disk does not exist.	404	The error message returned when the specified disk does not exist.
IncorrectDiskStatus	The current disk status does not support this operation.	403	The error message returned when this operation is not supported under the current disk status.
DiskNotPortable	It is not a portable disk.	403	The error message returned when the specified disk cannot be detached.
InstanceLockedForSecurity	The instance is locked due to security.	403	The error message returned when the specified instance is locked for security reasons.
DependencyViolation	The specified disk has not been attached on the specified instance.	403	The error message returned when the specified disk is not attached to the specified instance.
DiskTypeViolation	The specified disk is a system disk and cannot support the operation.	403	The error message returned when the specified disk is a system disk and cannot be detached from its associated instance.
InvalidDiskId.Released	The specified disk has been released.	403	The error message returned when the specified disk has already been released.

Error code	Error message	HTTP status code	Description
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when this operation is not supported under the current instance status.
InvalidParameter	The input parameter that is mandatory for processing this request is empty.	400	The error message returned when a required parameter is not specified.
InvalidDiskId.NotFound	The specified DiskId does not exist.	404	The error message returned when the specified disk does not exist.

Examples

Sample requests

```
https://ecs.example.com/?action=DetachDisk
&InstanceId=i-23jggx34b
&DiskId=d-23jbf2v5m
&Common request parameters
```

Sample responses

- XML format

```
<DetachDiskResponse>
  <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</DetachDiskResponse>
```

- JSON format

```
{
  "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

2.1.1.7.5. ModifyDiskAttribute

You can call this operation to modify the attributes of a disk.

When you call this operation, note that:

If the instance is locked for security reasons (the OperationLocks parameter is "LockReason": "security"), the DeleteWithInstance attribute will be ignored and the disk will be released together with the instance.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDiskAttribute.
DiskId	String	Yes	The ID of the disk to be modified.
DiskName	String	No	The name of the disk. If not specified, the parameter value remains unchanged. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It is displayed in Apsara Stack console. It cannot start with http:// or https://.
Description	String	No	The description of the disk. If not specified, the parameter value remains unchanged. Default value: null. The description must be 2 to 256 characters in length. It is displayed in Apsara Stack console. It cannot start with http:// or https://.
DeleteWithInstance	String	No	Indicates whether the disk is released together with the instance: • true: When the instance is deleted, the disk will be released together with it. • false: When the instance is released, the disk will be retained. If this parameter is set to false, an error will be returned if you specify a disk whose Portable attribute is false. Default value: null, indicating that the parameter value remains unchanged.
DeleteAutoSnapshot	String	No	Indicates whether the automatic snapshot is deleted when the disk is released. • true • false Default value: null, indicating that the parameter value remains unchanged.

Name	Type	Required	Description
EnableAutoSnapshot	String	No	Indicates whether an automatic snapshot policy is applied to the disk. Your automatic snapshot policy must be enabled. Valid values: • true • false Default value: null, indicating that the parameter value remains unchanged.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter DiskId that is mandatory for processing this request is not supplied.	400	The error message returned when the required DiskId parameter is not specified.
InvalidDiskId.NotFound	The specified disk does not exist.	404	The error message returned when the specified disk does not exist.
InvalidDiskName.Malformed	The specified disk name is wrongly formed.	400	The error message returned when the format of the DiskName parameter is incorrect.

Error code	Error message	HTTP status code	Description
InvalidDescription.Malformed	The specified description is wrongly formed.	404	The error message returned when the format of the Description parameter is incorrect.
InvalidParameter	The specified parameter DeleteWithInstance is not valid.	400	The error message returned when the specified DeleteWithInstance parameter is invalid.
NoAttributeToModify	No attribute to be modified in this request.	400	The error message returned when no attributes are modified.
DiskNotPortable	It is not a portable disk.	403	The error message returned when the disk cannot be detached.

Examples

Sample requests

```
https://ecs.example.com/?action=ModifyDiskAttribute
&DiskId=d-23jbf2v5m
&DiskName=MyDiskName
&Common request parameters
```

Sample responses

- XML format

```
<ModifyDiskAttributeResponse>
  <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</ModifyDiskAttributeResponse>
```

- JSON format

```
{
  "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

2.1.1.7.6. ReInitDisk

You can call this operation to reinitialize a disk.

When you call this operation, note that:

- The operation can be performed only when the disk is in the In_use state and the instance is in the Stopped state.
- If the instance has not been activated for the first time after creation, the disks attached to it cannot be reinitialized.
- An empty data disk that you create will be initialized to the empty disk status.
- A data disk created by using a snapshot will be initialized to the snapshot status.
- A system disk will be initialized to the initial status of the image.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ReInitDisk.
DiskId	String	Yes	The ID of the disk that you want to reinitialize.

Response parameters

- This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter DiskId that is mandatory for processing this request is not supplied.	400	The error message returned when the required DiskId parameter is not specified.
InvalidDiskId.NotFound	The specified disk does not exist.	404	The error message returned when the specified disk does not exist.
IncorrectDiskStatus	The current disk status does not support this operation.	403	The error message returned when the operation is not supported when the disk is in the current state.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the operation is not supported when the instance is in the current state.
InstanceLockedForSecurity	The instance is locked due to security.	403	The error message returned when the specified instance is locked for security reasons.
InvalidSourceSnapshot	The snapshot which is used to create the specified disk has been deleted.	403	The error message returned when the disk cannot be reinitialized because the source snapshot of the specified disk is deleted.
DiskCreatingSnapshot	The operation is denied due to a snapshot of the specified disk is not completed yet.	403	The error message returned when the specified disk is already being used to create a snapshot.
IncorrectDiskStatus.NeverUsed	The specified disk has never been used after creating.	403	The error message returned when the content of the disk is unchanged because it has not been used since creation.

Examples

Sample requests

```
https://ecs.example.com/?Action=ReInitDisk
&DiskId=d-23jbf2v5m
&Common request parameters
```

Sample responses

- XML format

```
<ReInitDiskResponse>
   <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
</ReInitDiskResponse>
```

- JSON format

```
{
   "RequestId":"F3CD6886-D8D0-4FEE-B93E-1B73239673DE"
}
```

2.1.1.7.7. ResetDisk

You can call this operation to restore the content of a disk using its snapshot.

When you call this operation, note that:

- The operation can be performed only when the instance is in the Stopped state.
- The operation can be performed only when the disk is in the In_use state.
- The specified snapshot must be created by using the DiskId parameter. Otherwise, an error will be returned.
- If the instance is locked for security reasons (the OperationLocks parameter is "LockReason": "security"), an error will be returned.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ResetDisk.
DiskId	String	Yes	The ID of the disk that you want to restore.
SnapshotId	String	Yes	The ID of the snapshot for the disk that you want to restore.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter DiskId that is mandatory for processing this request is not supplied.	400	The error message returned when the required DiskId parameter is not specified.
MissingParameter	The input parameter SnapshotId that is mandatory for processing this request is not supplied.	400	The error message returned when the required SnapshotId parameter is not specified.
InvalidDiskId.NotFound	The specified disk does not exist.	404	The error message returned when the specified disk does not exist.
InvalidSnapshotId.NotFound	The specified snapshot does not exist.	404	The error message returned when the specified snapshot does not exist.

Error code	Error message	HTTP status code	Description
IncorrectDiskStatus	The current disk status does not support this operation.	403	The error message returned when the operation is not supported when the disk is in the current state.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the operation is not supported when the instance is in the current state.
InstanceLockedForSecurity	The instance is locked due to security.	403	The error message returned when the specified instance is locked for security reasons.
InvalidParameter.Mismatch	The specified snapshot is not created from the specified disk.	403	The error message returned when the specified snapshot was not created from the specified disk.

Error code	Error message	HTTP status code	Description
InvalidSnapshotId.NotReady	The specified snapshot has not completed yet.	403	The error message returned when the specified snapshot is being created.

Examples

Sample requests

```
https://ecs.example.com/?Action=ResetDisk
&DiskId= d-23jbf2v5m
&SnapshotId=s-snapshot1
&Common request parameters
```

Sample responses

- XML format

```
<ResetDiskResponse>
  <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
</ResetDiskResponse>
```

- JSON format

```
{
  "RequestId":"F3CD6886-D8D0-4FEE-B93E-1B73239673DE"
}
```

2.1.1.7.8. ReplaceSystemDisk

You can call this operation to replace a system disk.

When you call this operation, note that:

- Replacing the system disk will change the ID of the system disk for this ECS instance. After the system disk is replaced, the original system disk will be released, but the disk type remains unchanged.
- When you replace a system disk, you can specify a new capacity by setting the SystemDiskSize parameter for the system disk. The parameter value must be at least 40 GiB, or greater than or equal to the disk capacity before the replacement.
- To replace a system disk, ensure that the instance is in the Stopped state and is not locked for security reasons (the OperationLocks parameter is "LockReason": "security").

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ReplaceSystemDisk.
InstanceId	String	Yes	The ID of the target instance.
ImageId	String	Yes	The ID of the image to be used to replace the system disk.
SystemDisk.Size	String	No	The capacity of the new system disk. Unit: GiB. Valid values: min to 500. The capacity must be at least 40 GiB, or greater than or equal to the current value of ImageSize.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency in the Appendix.

Response parameters

Response parameter description

Name	Type	Description
DiskId	String	The ID of the new system disk.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter ImageId that is mandatory for processing this request is not supplied.	400	The error message returned when the required ImageId parameter is not specified.
InvalidSystemDiskSize.LessThanImageSize	The specified parameter SystemDisk.Size is less than the image size.	404	The error message returned when the SystemDisk.Size value is smaller than the image size.
InvalidSystemDiskSize.MoreThanMaxSize	The specified parameter SystemDisk.Size is more than the max size.	404	The error message returned when the SystemDisk.Size value is greater than the maximum capacity.
InvalidSystemDiskSize.LessThanMinimumSize	The specified parameter SystemDisk.Size is less than the minimum size.	404	The error message returned when the SystemDisk.Size value is smaller than the minimum capacity.
InvalidInstanceId.NotFound	The specified instance does not exist.	404	The error message returned when the specified instance does not exist.
InvalidImageId.NotFound	The specified Image is disabled or is deleted.	404	The error message returned when the specified image does not exist.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the operation is not supported when the instance is in the current state.
InstanceLockedForSecurity	The instance is locked due to security.	403	The error message returned when the specified instance is locked for security reasons.
OperationDenied	Internal Error.	500	The error message returned when an internal error occurs.

Error code	Error message	HTTP status code	Description
InvalidParameter.Conflict	The specified image does not support the specified instance type.	400	The error message returned when the specified image cannot be used on the specified instance type.
InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	404	The error message returned when the specified instance does not exist.
DiskCreatingSnapshot	The operation is denied due to a snapshot of the specified disk is not completed yet.	403	The error message returned when the specified disk is already being used to create a snapshot.
IoOptimized.NotSupported	The specified image is not support IoOptimized Instance.	403	The error message returned when the specified image is not supported on I/O optimized instances.
InvalidParameter.Conflict	The specified image does not support the specified instance type.	400	The error message returned when the specified image is not supported on the specified instance type.
OperationDenied	The specified image that contains the snapshot of the data disk does not support this operation.	400	The error message returned when the specified image contains a data disk snapshot and does not support system disk replacement.

Examples

Sample requests

```
https://ecs.example.com/?Action=ReplaceSystemDisk
&InstanceId=i-23jggx34b
&ImageId=m-myimage11
&Common request parameters
```

Sample responses

- XML format

```
<ResetDiskResponse>
  <DiskId>d-23jbf2v5m</DiskId>
  <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
</ResetDiskResponse>
```

- JSON format

```
{
  "RequestId":"337568C5-64F3-4B76-8CDD-D3D8C57B5B8C",
  "DiskId":"d-j6cam2z21u4ks3dj6flb"
}
```

2.1.1.7.9. ResizeDisk

You can call this operation to scale up a disk.

When you call this operation, note that:

- Only data disks can be scaled up.
- A data disk attached to an instance can be scaled up only when the instance is in the Running or Stopped state.
- A disk cannot be scaled up if a snapshot is being created from it.
- For the scaling operation to take effect on the disk attached to the instance, you must restart the instance through the console or through open APIs.
- The scale-up operation applies only to the disk capacity and not to the partitions and file systems. After a disk is scaled up, you must allocate its storage space manually.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ResizeDisk.
DiskId	String	Yes	The ID of the disk to be scaled up.
NewSize	Integer	Yes	The disk capacity that you want to specify.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidDiskSize.TooSmall	Specified new disk size is less than the original disk size	403	The error message returned when the specified disk capacity is smaller than the original capacity.
InvalidParameter	The specified parameter NewSize is not valid.	403	The error message returned when the specified disk capacity exceeds the upper limit.
OperationDenied	The status of the disk or the instance that the disk is attaching with does not support the operation.	403	The error message returned when the scale-up operation is not supported in the current status of the disk or instance.
OperationDenied	The type of the disk does not support the operation.	403	The error message returned when the disk cannot be scaled up due to its disk type.
InvalidDiskId.NotFound	The specified disk does not exist.	404	The error message returned when the specified disk does not exist.
InvalidInstanceId.NotFound	The specified instance does not exist.	404	The error message returned when the instance to which the disk is attached does not exist.

Examples

Sample requests

```
https://ecs.example.com/?Action=ResizeDisk
&DiskId=xxx
&NewSize=1024
&Common request parameters
```

Sample responses

- XML format

```
<ResizeDiskResponse>
   <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
</ResizeDiskResponse>
```

- JSON format

```
{
  "RequestId": "F3CD6886-D8D0-4FEE-B93E-1B73239673DE"
}
```

2.1.1.7.10. DeleteDisk

You can call this operation to delete a disk that is no longer in use. Only independent cloud disks can be deleted.

When you call this operation, note that:

- Only disks in the Available state can be deleted.
- If the specified disk does not exist, the request will be ignored.
- Because your snapshots are retained, you can retain automatic snapshots as needed. Make sure you delete unnecessary orphaned user snapshots and automatic snapshots (snapshots that are still retained after the disks are deleted) in time. This helps maintain sufficient snapshot quota for periodic automatic snapshot policies.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteDisk.
DiskId	String	Yes	The ID of the disk that you want to delete.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
IncorrectDiskStatus	The current disk status does not support this operation.	403	The error message returned when the operation is not supported when the disk is in the current state.
DiskNotPortable	The operation is denied due to the specified disk is not a portable disk.	403	The error message returned when the specified disk cannot be detached from its instance.

Error code	Error message	HTTP status code	Description
DiskTypeViolation	The specified disk is a system disk and cannot support the operation.	403	The error message returned when the specified disk is a system disk and cannot be detached from its instance.
DiskCreatingSnapshot	The operation is denied due to a snapshot of the specified disk is not completed yet.	403	The error message returned when the specified disk is already being used to create a snapshot.

Examples

Sample requests

```
https://ecs.example.com/?Action=DeleteDisk
&DiskId=d-23jbf2v5m
&Common request parameters
```

Sample responses

- XML format

```
<DeleteDiskResponse>
  <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</DeleteDiskResponse>
```

- JSON format

```
{
"RequestId": "CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.1.1.7.11. migrate_disk

You can call this operation to migrate a disk online.

Request parameters

Request parameter description

Name	Type	Required	Description
region_id	String	Yes	The ID of the region to which the target disk belongs.

Name	Type	Required	Description
disk_id	String	Yes	The ID of the disk to be migrated. This parameter corresponds to the disk_id parameter in Server Controller.
dest_zone_id	String	Yes	The ID of the destination zone.
dest_disk_type	String	No	The type of the destination disk. You can specify this parameter when the disk type of the destination disk is different from that of the source disk, such as when migrating an io3 disk to an io7 disk. By default, the destination disk type is the same as that of the source disk.
dest_disk_iops	String	No	The IOPS of the destination disk. This parameter must be specified if the disk type is io7 or io8.
dest_disk_bps	String	No	The bit/s of the destination disk. This parameter must be specified if the disk type is io7 or io8.

Responses

```
{"code":200,  "msg":"successful",}
```

Error codes

Error code description

Error code	Error message	Description
-14000400	miagrate specfied dst region is invalid.	The error message returned when the specified destination region is different from the source region.
-14000401	parameter error, parameter is not null.	The error message returned when a required parameter is not specified.

Error code	Error message	Description
-14000402	migrate task is already exist.	The error message returned when the disk is already being migrated.
-14000404	parameter error, parameter is not exist.	The error message returned when specified parameters such as region_id and zone_id do not exist.
-14000501	migrate disk fail without retry.	The error message returned when the migration fails and does not need to be retried.
-14000502	migrate disk fail with retry.	The error message returned when the migration fails and must be retried.

Restrictions

- Only migration between cloud disks is supported.
- Only migration within the same zone is supported.
- Disk sharing is not supported.
- Disks in the old state can be migrated.
- Each disk can have only one task that is in the migrating state.
- When the disk type is io7 or io8, the dest_disk_iops and dest_disk_bps parameters must be specified.

Failover

Retry: When the TDC component returns the error code that requires a retry, the regionmaster sends a retry request (the workflow retries three times).

taskId policy

The disk_id, dest_cluster_no, and dest_disk_type parameters define a unique taskId. If the same migration task already exists, the task status of the current migration task is returned. Otherwise, a new taskId is generated.

2.1.1.7.12. query_load_progress

You can call this operation to query the progress of a migration operation for a disk.

Request parameters

Request parameter description

Name	Type	Required	Description
region_id	String	Yes	The ID of the region to which the target disk belongs.

Name	Type	Required	Description
disk_id	String	Yes	The ID of the disk to be queried. This parameter corresponds to the disk_id parameter in Server Controller.

Responses

```
{ "code":200, "msg":"80",}
```

2.1.1.8. Snapshots

2.1.1.8.1. CreateSnapshot

You can call this operation to create a snapshot for a disk storage device.

When you call this operation, note that:

- A snapshot can be created only for ECS instances in the Stopped or Running state. Snapshots cannot be created for ECS instances which have been created but not yet activated.
- If you create a snapshot of a disk immediately after a system disk is created or after a data disk is added from another snapshot, an error will be returned because the system disk or data disk has not finished loading data. Typically, a snapshot can be created one hour after the system disk is created. The amount of time after which a data disk snapshot can be created varies based on the amount of data stored on the disk.
- A newly added disk cannot be used to create snapshots if the instance has not been activated.
- A snapshot that is not completely created (the creation progress has not reached 100%) cannot be used to create a custom image.
- If a snapshot is not completely created (the creation progress has not reached 100%), you cannot create another snapshot from the same disk.
- The snapshot quota depends on the total number of disks owned by your account.
- If the disk is in the In_use state and the attached instance is locked (the OperationLocks parameter is "LockReason": "security"), no snapshots can be created.
- A disk can be used to create snapshots only after the instance to which the disk is attached has been activated for the first time.
- An error message is returned when you create a snapshot for an independent basic disk that has never been attached to any instances.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateSnapshot.

Name	Type	Required	Description
DiskId	String	Yes	The disk ID.
SnapshotName	String	No	The name of the snapshot. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with the string 'auto'. Snapshot names starting with the string 'auto' are reserved for automatic snapshots. The snapshot name is displayed in Apsara Stack console. It cannot start with http:// or https://.
Description	String	No	The description of the instance. The description must be 2 to 256 characters in length. The snapshot description is displayed in Apsara Stack console. If not specified, this parameter is null. Default value: null. It cannot start with http:// or https://.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency in the Appendix.

Response parameters

Response parameter description

Name	Type	Description
SnapshotId	String	The snapshot ID.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidDiskId.NotFound	The specified DiskId does not exist.	404	The error message returned when the specified disk does not exist.
InvalidSnapshotName.Malformed	The specified SnapshotName is wrongly formed.	400	The error message returned when the format of the SnapshotName parameter is invalid.

Error code	Error message	HTTP status code	Description
InvalidDescription.Malformed	The specified description is wrongly formed.	404	The error message returned when the format of the Description parameter is invalid.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	400	The error message returned when the operation is not supported when the instance is in the current state.
IncorrectDiskStatus.CreatingSnapshot	The snapshot of the disk is still creating.	403	The error message returned when the specified disk is already being used to create a snapshot.
InstanceLockedForSecurity	The disk attached instance is locked due to security.	403	The error message returned when the specified instance is locked for security reasons.
IncorrectDiskStatus.NeverAttached	The specified disk has never been attached to any instance.	403	The error message returned when the specified disk has never been attached to any instances.
QuotaExceed.Snapshot	The snapshot quota exceeds.	403	The error message returned when the snapshot quota has been exhausted.
IncorrectDiskStatus.NeverUsed	The specified disk has never been used after creating.	403	The error message returned when the content of the disk is unchanged because it has not been used since creation.
CreateSnapshot.Failed	The process of creating snapshot is failed	403	The error message returned when the snapshot fails to be created.

Examples

Sample requests

```
https://ecs.example.com/?Action=CreateSnapshot
&DiskId=1033-60053321
&Common request parameters
```

Sample responses

XML format

```
<CreateSnapshotResponse>
    <RequestId>C8B26B44-0189-443E-9816-D951F59623A9</RequestId>
    <SnapshotId>s-923FE2BF0</SnapshotId>
</CreateSnapshotResponse>
```

JSON format

```
{
  "RequestId": "C8B26B44-0189-443E-9816-D951F59623A9",
  "SnapshotId": "s-923FE2BF0"
}
```

2.1.1.8.2. DeleteSnapshot

You can call this operation to delete a snapshot.

When you call this operation, note that:

- You can call this operation to delete a snapshot that is being created (the creation progress has not reached 100%).
- If the specified snapshot does not exist, the request will be ignored.
- A snapshot that has already been used to create custom images cannot be deleted. The snapshot can be deleted only after the corresponding custom images are deleted.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteSnapshot.
SnapshotId	String	Yes	The ID of the snapshot to be deleted.

- **Response parameters**

  This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
SnapshotCreatedImage	The snapshot has been used to create user defined image(s).	403	The error message returned when the specified snapshot has already been used to create custom images.
SnapshotCreatedDisk	The snapshot has been used to create disk(s).	403	The error message returned when the specified snapshot has already been used to create disks.
MissingParameter	The input parameter SnapshotId that is mandatory for processing this request is not supplied.	400	The error message returned when the required SnapshotId parameter is not specified.

Examples

Sample requests

```
https://ecs.example.com/?Action=DeleteSnapshot
&SnapshotId=s-923FE2BF0
&Common request parameters
```

Sample responses

XML format

```
<DeleteSnapshotResponse>
    <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</DeleteSnapshotResponse>
```

JSON format

```
{
    "RequestId": "CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.1.1.8.3. DescribeSnapshots

You can call this operation to query all snapshots of a disk device in ECS.

When you call this operation, note that:

Request parameters such as InstanceId, DiskId, and SnapshotIds act as filtering conditions and have logic AND relations.

Request parameters

Request parameter description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSnapshots.
RegionId	String	Yes	The ID of the region to which the disk belongs.
InstanceId	String	No	The ID of the specified instance.
DiskId	String	No	The ID of the specified disk device.
SnapshotIds	String	No	The snapshot IDs. This parameter is a JSON-formatted array: ["s-xxxxxxxxx", "s-yyyyyyyyy", ... "szzzzzzzzz"]. You can specify a maximum of 100 IDs. Separate multiple IDs with commas (,).
SnapshotName	String	No	The name of the snapshot.
Status	String	No	The status of the snapshot. Valid values: progressing | accomplished | failed | all.
SnapshotType	String	No	The type of the snapshot. Valid values: auto | user | all.
SourceDiskType	String	No	The type of the source disk. Valid values: System | Data.
Usage	String	No	The referenced resource type. Valid values: image | disk | image_disk | none.
Tag.n.Key	String	No	The key of the tag. Valid values of n: 1 to 5. It cannot be a null string.
Tag.n.Value	String	No	The value of the tag. Valid values of n: 1 to 5. It can be a null string.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 1 to 100. Default value: 10.

Response parameters

Response parameter description

Parameter	Type	Description
TotalCount	Integer	The total number of snapshots.
PageNumber	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
Snapshots	SnapshotType	A set of SnapshotType data.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidSnapshotIds.Malformed	The amount of specified specified snapshotIds exceeds the limit.	403	The error message returned because the format of the SnapshotIds parameter is incorrect.
InvalidStatus.NotFound	The specified Status is not found	404	The error message returned because the specified Status parameter does not exist.
InvalidSnapshotType.NotFound	The specfied SnapshotType is not found	404	The error message returned because the specified SnapshotType parameter does not exist.
InvalidFilterKey.NotFound		404	The error message returned because the specified start time or end time is incorrect.
InvalidUsage	The specifed Usage is not valid	404	The error message returned because the specified Usage parameter is invalid.
InvalidSourceDiskType	The specifed SourceDiskType is not valid	404	The error message returned because the specified SourceDiskType parameter is invalid.
InvalidTag.Mismatch	The specified Tag.n.Key and Tag.n.Value are not match.	400	The error message returned because the specified Tag.n.Key and Tag.n.Value parameters do not match.
InvalidTagCount	The specified tags are beyond the permitted range.	400	The error message returned because more than five tags have been specified.

Sample requests

```
https://ecs.example.com/?Action=DescribeSnapshots
&amp;RegionId=cn-hangzhou
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeSnapshotsResponse>
  <Snapshots>
    <Snapshot>
      <CreationTime>2014-07-24T13:00:52Z</CreationTime>
      <Description></Description>
      <SourceDiskId>d-23x0r****</SourceDiskId>
      <SourceDiskType>DATA</SourceDiskType>
      <ProductCode></ProductCode>
      <SnapshotName>auto_20140****</SnapshotName>
      <Progress>100%</Progress>
      <SourceDiskSize>50</SourceDiskSize>
      <Status>accomplished</Status>
      <SnapshotId>s-23f2i****</SnapshotId>
      <Usage>none</Usage>
    </Snapshot>
    <Snapshot>
      <CreationTime>2014-07-24T13:00:42Z</CreationTime>
      <Description></Description>
      <SourceDiskId>101-7010****</SourceDiskId>
      <SourceDiskType>DATA</SourceDiskType>
      <ProductCode></ProductCode>
      <SnapshotName>auto_2014****</SnapshotName>
      <Progress>100%</Progress>
      <SourceDiskSize>5</SourceDiskSize>
      <Status>accomplished</Status>
      <SnapshotId>s-23izt****</SnapshotId>
      <Usage>none</Usage>
    </Snapshot>
  </Snapshots>
  <PageNumber>1</PageNumber>
  <PageSize>2</PageSize>
  <TotalCount>36</TotalCount>
  <RequestId>2F409D67-329A-4405-B924-2FC28566B366</RequestId>
</DescribeSnapshotsResponse>
```

JSON format

```
{
 "PageNumber": 1,
 "PageSize": 2,
 "RequestId": "659F91C6-1949-43B0-90C4-B6342CA757D5",
 "Snapshots": {
  "Snapshot": [
   {
    "CreationTime": "2015-07-30T05:00:14Z",
    "Progress": "100%",
    "SnapshotId": "s-943yp****",
    "SnapshotName": "auto_20150****",
    "SourceDiskId": "d-944qy****",
    "SourceDiskSize": 20,
    "SourceDiskType": "system",
    "Status": "accomplished",
    "Usage": "none"
   },
   {
    "CreationTime": "2015-07-30T05:00:14Z",
    "Progress": "100%",
    "SnapshotId": "s-94osg****",
    "SnapshotName": "auto_20150****",
    "SourceDiskId": "d-94j35****",
    "SourceDiskSize": 20,
    "SourceDiskType": "system",
    "Status": "accomplished",
    "Usage": "none"
   }
  ]
 },
 "TotalCount": 36
}
```


2.1.1.8.4. ImportSnapshot

You can call this operation to import a snapshot stored in an OSS bucket to the snapshots listed in the ECS console.

Description

- Make sure that the region of the snapshot to be imported is the same as that of the OSS bucket that stores this snapshot.

- Make sure that the RAM user has the permissions to read data from the OSS bucket.

Request parameters

Request parameter description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this value to ImportSnapshot.
RegionId	String	Yes	The ID of the region.
SnapshotName	String	No	The name of the snapshot to be imported. Default value: null.
OssBucket	String	Yes	The name of the OSS bucket.
OssObject	String	Yes	The name of the OSS object.

Response parameters

Response parameter description

Parameter	Type	Description
SnapshotId	String	The ID of the imported snapshot in the snapshot list.
TaskId	String	The ID of the import task.

Sample requests

```
https://ecs.example.com/?Action=ImportSnapshot
&RegionId=cn-hangzhou
&OSSBucket=ecsimportsnapshot
&OSSObject=CentOS_snapshot
&SnapshotName=testsnapshotimportName
&<Common request parameters>
```

Sample responses

XML format

```
<ImportSnapshotResponse>
  <RequestId>C8B26B44-0189-443E-9816-D951F59623A0</RequestId>
  <TaskId>tsk-231234568</ExportTaskId>
  <SnapshotId>s-abcdxxxxx</SnapshotId>
</ImportSnapshotResponse>
```

JSON format

```
{
  "RequestId":"C8B26B44-0189-443E-9816-D951F59623A0",
  "TaskId":"tsk-2312345901",
  "SnapshotId":"s-abcdxxxxx"
}
```

2.1.1.8.5. ExportSnapshot

You can call this operation to export a snapshot listed in the ECS console to an OSS bucket.

Description

- Make sure the target OSS bucket is in the same region as the snapshot to be exported.
- Make sure that the RAM user has the permissions to write data to the OSS bucket.

Request parameters

Request parameter description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this value to ExportSnapshot.
RegionId	String	Yes	The ID of the region.
SnapshotId	String	Yes	The ID of the snapshot to be exported.
OssBucket	String	Yes	The name of the OSS bucket.

Response parameters

Response parameter description

Parameter	Type	Description
TaskId	String	The ID of the export task.

Sample requests

```
https://ecs.example.com/?Action=ExportSnapshot
&SnapshotId=s-abcxxxx
&OSSBucket=testExportSnapshot
&RegionId=cn-hangzhou
&<Common request parameters>
```

Sample responses

XML format

```
<ExportSnapshotResponse>
  <RequestId>C8B26B44-0189-443E-9816-D951F59623A9</RequestId>
  <TaskId>tsk-231234567</ExportTaskId>
</ExportSnapshotResponse>
```

JSON format

```
{
  "RequestId":"C8B26B44-0189-443E-9816-D951F59623A9",
  "TaskId":"tsk-231234567"
}
```

Error codes

Error code description

HTTP status code	Error code	Error message	Description
403	INTERNAL_ERROR	Exporting snapshot is failed, Please contact the administrator.	The error message returned because the snapshot failed to be exported. Contact the administrator.
403	CREATE_TASK_RECORD_FAILED	Exporting snapshot is failed, Please contact the administrator.	The error message returned because the snapshot failed to be exported. Contact the administrator.
403	SNAPSHOT_IS_EXPORTING	The specified snapshot is already exporting.	The error message returned because the specified snapshot is already being exported.

HTTP status code	Error code	Error message	Description
403	SNAPSHOT_NOT_EXIST	The specified snapshot is not exists.	The error message returned because the specified snapshot does not exist.
403	SNAPSHOT_CREATE_NOT_FINISHED	The specified snapshot is not finished yet.	The error message returned because the specified snapshot is being created.
403	OSS_AUTHORIZED_FAILED	ECS service account Have no right to access your OSS. please attach a role of access your oss to ECS service account.	The error message returned because the RAM user has no permission to access OSS. Confirm that the RAM user has the permissions to write data to OSS.
403	OSS_BUCKET_NOT_FOUND	The specified OSS bucket does not exist in this region.	The error message returned because the specified OSS bucket does not exist.
403	USER_NOT_IN_SNAPSHOT_IMPORT_EXPORT_WHITE_LIST	The user is not in the white list of exporting snapshot.	The error message returned because you are not included in the whitelist. Only users in the whitelist can export snapshots.

2.1.1.8.6. DescribeSnapshotLinks

You can call this operation to query the snapshot links of one or more disks.

When you call this operation, note that:

- Request parameters such as RegionId, DiskIds, and InstanceId act as filtering conditions and have a boolean AND relationship.
- If no parameters are specified, no filtering conditions are applied. If the DiskIds and SnapshotLinkIds parameters are empty JSON arrays ([]), the filtering conditions are regarded as effective and a blank result will be returned.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSnapshotLinks.

Name	Type	Required	Description
RegionId	String	Yes	The ID of the region to which the target disk belongs. For more information, see Regions and zones. You can call DescribeRegions to view latest regions.
InstanceId	String	No	The ID of the instance to which the target disk belongs.
DiskIds	String	No	The disk IDs. You can specify a maximum of 100 disk IDs at a time. The parameter value is an array of disk IDs, such as ["d-xxxxxxxxx", "dyyyyyyyyy", ... "dzzzzzzzzz"]. Separate multiple IDs with commas (,).
SnapshotLinkIds	String	No	The IDs of the target snapshot links. You can specify a maximum of 100 snapshot link IDs at a time. The parameter value is an array of snapshot link IDs, such as ["p-xxxxxxxxx", "p-yyyyyyyyy", ... "pzzzzzzzzz"]. Separate multiple IDs with commas (,).
PageNumber	Integer	No	The page number that you query in the disk status list. Starting value: 1. Default value: 1.
PageSize	Integer	No	The number of entries per page. Valid values: [1, 50]. Default value: 10.

Response parameters

Name	Type	Description
RegionId	String	The ID of the region to which the source disk of a snapshot link belongs.
TotalCount	Integer	The total number of snapshot links.
PageNumber	Integer	The page number that you query in the snapshot link list.

Name	Type	Description
PageSize	Integer	The number of entries per page.
SnapshotLinks	SnapshotLinkType	A set of snapshot link information.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeSnapshotLinks
&RegionId=cn-beijing
&ZoneId=cn-beijing-btc-a01
&PageNumber=1
&<Common request parameter>
```

Sample responses

XML format

```
<DescribeSnapshotLinksResponse>
<SnapshotLinks>
<SnapshotLink>
<SnapshotLinkId>d-25okbh2pj</SnapshotLinkId >
<SourceDiskId>d-25okbh2pj</SourceDiskId>
<SourceDiskType>data</SourceDiskType>
<SourceDiskSize>20</SourceDiskSize>
<RegionId> cn-beijing-btc-a01</RegionId>
<TotalCount>1</TotalCount>
<TotalSize>2097152</TotalSize>
</SnapshotLink>
<SnapshotLink>
<SnapshotLinkId>d-2ze0y1jwzpb1geqxkroq</SnapshotLinkId >
<SourceDiskId>d-2ze0y1jwzpb1geqxkroq</SourceDiskId>
<SourceDiskType>system</SourceDiskType>
<SourceDiskSize>40</SourceDiskSize>
<RegionId> cn-beijing-btc-a01</RegionId>
<TotalCount>1</TotalCount>
<TotalSize>2097152</TotalSize>
</SnapshotLink>
</SnapshotLinks>
<PageNumber>1</PageNumber>
<PageSize>2</PageSize>
<TotalCount>9</TotalCount>
<RequestId>ED5CF6DD-71CA-462C-9C94-A61A78A01479</RequestId>
</DescribeSnapshotLinksResponse>
```

JSON format

```
{
"SnapshotLinks": {
"SnapshotLink": [
{
"SourceDiskSize": 20, "TotalSize": 2097152,
"SourceDiskType": "data",
"RegionId": "cn-beijing-btc-a01",
"SnapshotLinkId": "d-25okbh2pj",
"SourceDiskId": "d-25okbh2pj",
"TotalCount": 1
},
{
"SourceDiskSize": 40, "TotalSize": 2097152,
"SourceDiskType": "data",
"RegionId": "cn-beijing-btc-a01",
"SnapshotLinkId": "d-2ze0y1jwzpb1geqxkroq",
"SourceDiskId": "d-2ze0y1jwzpb1geqxkroq",
"TotalCount": 1
}
]
},
"PageNumber": 1,
"PageSize": 2,
"RequestId": "ACD9BBB0-A9D1-46D7-9630-B7A69889E110", "TotalCount": 9
}
```


Error codes

Error code	Error message	HTTP status code	Description
InvalidDiskIds	The specified diskIds is invalid.	400	The error message returned when the specified DiskIds parameter is invalid.
InvalidRegionId	The specified regionId is invalid.	400	The error message returned when the specified RegionId parameter is invalid.
InvalidSnapshotLinkIds	The specified snapshotLinkIds is invalid.	400	The error message returned when the specified SnapshotLinkIds parameter is invalid.

Error code	Error message	HTTP status code	Description
InternalError	The request processing has failed due to some unknown error.	500	The error message returned when an internal error occurs.

2.1.1.8.7. CreateAutoSnapshotPolicy

You can call this operation to create an automatic snapshot policy.

When you call this operation, note that:

- After you create an automatic policy, you can apply it to any disks.
- After you create an automatic policy, you can modify it as required.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateAutoSnapshotPolicy.
RegionId	String	Yes	The ID of the region in which you want to create the automatic snapshot policy.
AutoSnapshotPolicyName	String	Yes	The name of the automatic snapshot policy. If not specified, this parameter is null. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, underscores (_), and hyphens (-). It is displayed in Apsara Stack console. The name cannot start with http:// or https://.
TimePoints	String	Yes	The point in time at which automatic snapshots are to be created. The smallest interval that snapshots can be taken at is one hour. Valid values: 0 to 23, corresponding to 24 hours in the range of 00:00 to 23:00. You can specify multiple points in time. The parameter is a JSON-formatted array: ["0", "1", ... "23"]. You can specify a maximum of 24 points in time. Separate multiple points in time with commas (,).
RepeatWeekdays	String	Yes	The repeat date for the automatic snapshot. This parameter specifies which days of the week that automatic snapshots are created on. Valid values: 1 to 7, corresponding to the week, where 1 indicates Monday. You can specify multiple dates. The parameter is a JSON-formatted array: ["1", "2", ... "7"].

Name	Type	Required	Description
RetentionDays	Integer	No	The retention period of the automatic snapshot. Unit: day. • The automatic snapshot is retained permanently by default. • 1-65536: The automatic snapshot is retained for the specified number of days.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency in the Appendix.

Response parameters

Response parameter description

Name	Type	Description
AutoSnapshotPolicyId	String	The ID of the automatic snapshot policy.

Error codes

For more information, see Common errors.

Examples

Sample requests

```
https://ecs.example.com/?Action=CreateAutoSnapshotPolicy
&SettingTimePoints=[ “0” , “11 ” , “21 ” ]&SettingRepeatWeekdays=[ “1” , “2” , “4” , “7” ] &Re
tentionDays=30
&Common request parameters
```

Sample responses

XML format

```
<CreateAutoSnapshotPolicyResponse>
  <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
<AutoSnapshotPolicyId>p-233e6ylv0</AutoSnapshotPolicyId>
</CreateAutoSnapshotPolicyResponse>
```

JSON format

```
{
   "RequestId":"F3CD6886-D8D0-4FEE-B93E-1B73239673DE"
"AutoSnapshotPolicyId":"p-233e6ylv0"
}
```

2.1.1.8.8. DeleteAutoSnapshotPolicy

You can call this operation to delete an automatic snapshot policy.

When you call this operation, note that:

After you delete an automatic snapshot policy, the policy will no longer be applied to the disks that it previously took effect on.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteAutoSnapshotPolicy.
RegionId	String	Yes	The ID of the region in which you want to delete the automatic snapshot policy.
AutoSnapshotPolicyId	String	Yes	The ID of the automatic snapshot policy that you want to delete.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=DeleteAutoSnapshotPolicy
&AutoSnapshotPolicyId=p-233e6ylv0
&Common request parameters
```

Sample responses

XML format

```
<DeleteAutoSnapshotPolicyResponse>
   <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
</DeleteAutoSnapshotPolicyResponse>
```

JSON format

```
{
  "RequestId":"F3CD6886-D8D0-4FEE-B93E-1B73239673DE"
}
```

2.1.1.8.9. ModifyAutoSnapshotPolicyEx

You can call this operation to modify an automatic snapshot policy.

When you call this operation, note that:

After you modify an automatic snapshot policy, the new policy takes effect immediately on the disks that have applied the policy.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyAutoSnapshotPolicyEx.
RegionId	String	No	The ID of the region where you want to modify the automatic snapshot policy.
AutoSnapshotPolicyId	String	Yes	The ID of the automatic snapshot policy that you want to modify.
AutoSnapshotPolicyName	String	No	The name of the automatic snapshot policy. If this parameter is not specified, the policy will not be modified.
TimePoints	String	No	The point in time at which automatic snapshots are to be created. The smallest interval that snapshots can be taken at is one hour. Valid values: 0 to 23, corresponding to 24 hours in the range of 00:00 to 23:00. You can specify multiple points in time. If this parameter is not specified, the points in time of the specified policy will not be modified. The parameter is a JSON-formatted array: ["0", "1", ... "23"]. You can specify a maximum of 24 points in time. Separate multiple points in time with commas (,).

Name	Type	Required	Description
RepeatWeekdays	String	No	The repeat date for the automatic snapshot. This parameter specifies which days of the week that automatic snapshots are created on. Valid values: 1 to 7, corresponding to the week, where 1 indicates Monday. You can specify multiple dates. If this parameter is not specified, the days of the specified policy will not be modified. The parameter is a JSON-formatted array: ["1", "2", ... "7"].
RetentionDays	Integer	No	The retention period of the automatic snapshot. Unit: day. • -1: The automatic snapshot is retained permanently. • 1-65536: The automatic snapshot is retained for the specified number of days. If this parameter is not specified, the retention period of the specified policy will not be modified.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency in the Appendix.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifyAutoSnapshotPolicy
&AutoSnapshotPolicyId=p-233e6ylv0&SettingTimePoints=[ “0” , “11 ” , “21 ” ]&SettingRepeatWeekday
s=[ “1” , “2” , “4” , “7” ] &RetentionDays=30
&Common request parameters
```

Sample responses

XML format

```
<ModifyAutoSnapshotPolicyResponse>
   <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
</ModifyAutoSnapshotPolicyResponse>
```

JSON format

```
{
  "RequestId":"F3CD6886-D8D0-4FEE-B93E-1B73239673DE"
}
```

2.1.1.8.10. DescribeAutoSnapshotPolicyEx

You can call this operation to query automatic snapshot policies.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeAutoSnapshotPolicyEx.
RegionId	String	Yes	The ID of the region in which you want to query automatic snapshot policies.
AutoSnapshotPolicyId	String	No	The ID of the automatic snapshot policy that you want to query. If this parameter is not specified, all policies will be returned. The parameter is a JSON-formatted array: ["p-xxxxxxxxx", "p-yyyyyyyyy", ... "pzzzzzzzzz"].
PageNumber	Integer	No	The page number that you query in the automatic snapshot policy list. Starting value: 1. Default value: 1.
PageSize	Integer	No	The number of entries per page. Maximum value: 50. Default value: 10.

Response parameters

Response parameter description

Name	Type	Description
TotalCount	Integer	The total number of snapshots.
PageNumber	Integer	The page number that you query in the snapshot list.
PageSize	Integer	The number of entries per page.
AutoSnapshotPolicys	AutoSnapshotPolicyType	A set of AutoSnapshotPolicyType data.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeAutoSnapshotPolicy
&Common request parameters
```

Sample responses

XML format

```
<DescribeAutoSnapshotPolicyResponse>
<AutoSnapshotPolicies>
    <AntoSnapshotPolicy>
      <CreationTime>2014-04-21T12:08:52Z</CreationTime>
      <AutoSnapshotPolicyId>p-23f2i9s4t</AutoSnapshotPolicyId>
     <SettingTimePoints>[ “2” , “9” ]</SettingTimePoints>
      <SettingRepeatWeekdays>[ “3” , “4” , “5” , “7” ]</SettingRepeatWeekdays>
      <RetentionDays>-1</RetentionDays>
      </AntoSnapshotPolicy>
    <AntoSnapshotPolicy>
      <CreationTime>2014-07-24T13:00:52Z</CreationTime>
      <AutoSnapshotPolicyId>p-23f2i9s4t</AutoSnapshotPolicyId>
      <SettingTimePoints>[ “0” , “1” ]</SettingTimePoints>
      <SettingRepeatWeekdays>[ “1” , “7” ]</SettingRepeatWeekdays>
      <RetentionDays>30</RetentionDays>
    </AntoSnapshotPolicy>
  </AutoSnapshotPolicies>
  <PageNumber>1</PageNumber>
  <PageSize>2</PageSize>
  <TotalCount>2</TotalCount>
  <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
</DescribeAutoSnapshotPolicyResponse>
```

JSON format

```
{
 "PageNumber": 1,
 "PageSize": 2,
 "RequestId": "659F91C6-1949-43B0-90C4-B6342CA757D5",
 "AntoSnapshotPolicys": {
  " AutoSnapshotPolicy": [
   {
    "CreationTime": "2014-07-24T13:00:52Z",
    "AutoSnapshotPolicyId": "p-23f2i9s4t",
    "SettingTimePoints": "[ “0” , “1” ]",
    "SettingRepeatWeekdays": "[ “1” , “7” ]",
    "RetentionDays": "30",
   },
   {
    "CreationTime": "2014-04-21T12:08:52Z",
    "AutoSnapshotPolicyId": "p-a1fd3g5s1",
    "SettingTimePoints": "[ “2” , “9” ]",
    "SettingRepeatWeekdays": "[ “3” , “4” , “5” , “7” ]",
    "RetentionDays": "-1",
   }
  ]
 },
 "TotalCount": 2
}
```


2.1.1.8.11. ApplyAutoSnapshotPolicy

You can call this operation to apply an automatic snapshot policy to one or more disks.

When you call this operation, note that:

- A disk can have only one automatic snapshot policy. If you apply an automatic snapshot policy to a disk that already has an automatic policy, the new policy takes effect on the disk in place of the original one.
- A single automatic snapshot policy can be applied to multiple disks.
- However, the same snapshot policy being applied to multiple disks does not necessarily mean that snapshots for these disks will be generated concurrently.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ApplyAutoSnapshotPolicy.
RegionId	String	Yes	The ID of the region where you want to apply the automatic snapshot policy.
AutoSnapshotPolicyId	String	Yes	The ID of the automatic snapshot policy that you want to apply.
DiskIds	String	Yes	The IDs of disks for which you want to apply the automatic snapshot policy. The parameter is a JSON-formatted array: ["dxxxxxxxxx", "dyyyyyyyyy", ... "dzzzzzzzzz"]. Separate multiple IDs with commas (,).

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=ApplyAutoSnapshotPolicy
&Snapshots =[ “d-233e6ylv0” , “d-23vbpbi03 ” , “d-23vasz3ds ” ]
&Common request parameters
```

Sample responses

XML format

```
<ApplyAutoSnapshotPolicyResponse>
  <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
</ApplyAutoSnapshotPolicyResponse>
```

JSON format

```
{
  "RequestId":"F3CD6886-D8D0-4FEE-B93E-1B73239673DE"
}
```

2.1.1.8.12. CancelAutoSnapshotPolicy

You can call this operation to cancel the automatic snapshot policy of one or more disks.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CancelAutoSnapshotPolicy.
RegionId	String	Yes	The ID of the region in which you want to cancel the automatic snapshot policy.
DiskIds	String	Yes	The set of disks for which you want to cancel the automatic snapshot policy. The parameter is a JSON-formatted array: ["dxxxxxxxxx", "dyyyyyyyyy", ... "dzzzzzzzzz"]. Separate multiple IDs with commas (,).

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=DeleteAutoSnapshotPolicy
&AutoSnapshotPolicyId=p-233e6ylv0
&Common request parameters
```

Sample responses

XML format

```
<ApplyAutoSnapshotPolicyResponse>
  <RequestId>F3CD6886-D8D0-4FEE-B93E-1B73239673DE</RequestId>
</ApplyAutoSnapshotPolicyResponse>
```

JSON format

```
{
  "RequestId":"F3CD6886-D8D0-4FEE-B93E-1B73239673DE"
}
```

2.1.1.9. Images

2.1.1.9.1. CreateImage

You can call this operation to create a custom image. When the custom image is in the available state, the image can be used to create an ECS instance or replace the system disk of an existing instance.

You can use the following methods to create a custom image based on your business scenarios:

- To create a custom image from the system disk of an existing instance, specify a snapshot ID.
  - Only a system disk snapshot can be used to create a custom image.
  - Only a snapshot in the accomplished state (the progress is 100%) can be used to create a custom image.
  - A snapshot that is locked for security reasons (the OperationLocks parameter is "LockReason": "security") cannot be used to create a custom image.
  - A snapshot created on or before July 15, 2013 cannot be used to create a custom image. When a request is denied for this reason, the error code in Response is InvalidSnapshot.TooOld.
- To create a template for an ECS instance, you can specify an instance ID to create a custom image.
  - The specified instance must be in the Running or Stopped state.
  - A snapshot is added to each disk of the instance.
  - The image is available only after the snapshot is created.
- To combine multiple snapshots into an image template, you can specify the DiskDeviceMappings parameter to create a custom image.
  - Only one system disk snapshot can be specified, and the name of the device with the system disk snapshot must be /dev/xvda.
  - The names of devices with data disk snapshots are allocated by the system in the default order. The value ranges from /dev/xvdb to /dev/xvdz. Each device name must be unique.
  - If you do not specify the snapshot ID, an empty disk without data is created with the specified capacity.
  - Only a snapshot in the accomplished state (the progress is 100%) can be used to create a custom image.
  - A snapshot that is locked for security reasons (the OperationLocks parameter is "LockReason": "security") cannot be used to create a custom image.
  - A snapshot created on and before July 15, 2013 cannot be used to create a custom image. When a request is denied for this reason, the error code in Response is InvalidSnapshot.TooOld.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateImage.
RegionId	String	Yes	The ID of the region to which the custom image belongs.
SnapshotId	String	No	The snapshot ID. The custom image is created from the specified snapshot.
InstanceId	String	No	The ID of the instance.

Name	Type	Required	Description
DiskDeviceMapping.N.Size	String	No	The disk capacity. Valid values: 5 to 2000 GB. If this parameter is not specified, the snapshot size is applied by default. If neither this parameter or the snapshot ID is specified, the disk capacity is set to 5 GB by default. The disk capacity cannot be smaller than the snapshot size.
DiskDeviceMapping.N.SnapshotId	String	No	The snapshot ID.
ImageName	String	No	The name of the custom image. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with http:// or https://.
ImageVersion	String	No	The version number of the image. The version number must be 1 to 40 characters in length.
Description	String	No	The description of the custom image. The description must be 0 to 256 characters in length. If not specified, this parameter is null. Default value: null. It cannot start with http:// or https://.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency.

Response parameters

Response parameter description

Name	Type	Description
ImageId	String	The ID of the custom image.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The specified region does not exist.	404	The error message returned when the specified region ID does not exist.
InvalidImageName.Malformed	The specified Image name is wrongly formed.	400	The error message returned when the value of the ImageName parameter contains unsupported characters or exceeds the maximum length.
InvalidDescription.Malformed	The specified description is wrongly formed.	400	The error message returned when the Description parameter is invalid.
InvalidImageVersion.Malformed	The specified ImageVersion is wrongly formed.	400	The error message returned when the ImageVersion parameter is invalid or you are not authorized to use the snapshot.
OperationDenied	The specified snapshot is not allowed to create image.	403	The error message returned when the specified snapshot cannot be used to create custom images.
QuotaExceed.Image	The Image Quota exceeds.	403	The error message returned when the custom image quota has been exhausted.
OperationDenied	The specified snapshot is not from system disk.	403	The error message returned when the specified snapshot is not from a system disk.
InvalidParamter.Conflict	The specified same token is trying to make requests with different parameters.	403	The error message returned when the specified token conflicts with the parameters.

Error code	Error message	HTTP status code	Description
InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	400	The error message returned when the specified instance does not exist.
IncorrectInstanceStatus	The current status of the instance does not support this operation.	400	The error message returned when the instance is in a state that does not support the current operation.
InstanceLockedForSecurity	The specified operation is denied as your instance is locked for security reasons.	400	The error message returned when the specified instance is locked for security reasons.
InvalidSnapshotId.NotFound	The specified snapshot does not exist.	404	The error message returned when the specified snapshot does not exist.
InvalidImageName.Duplicated	The specified Image name has already bean used.	400	The error message returned when the specified image name is already in use.
InvalidSnapshotId.NotReady	The current status of the DiskDeviceMapping.n.SnapshotId or SnapshotId does not support this operation.	403	The error message returned when the snapshot is in a state that does not support the current operation.
InvalidSnapshot.TooOld	This operation is denied because the specified snapshot by DiskDeviceMapping.n.SnapshotId or SnapshotId is created before 2013-07-15.	403	The error message returned when the specified snapshot was created on or before July 15, 2013.
InvalidSnapshotId.NotFound	The specified snapshot by DiskDeviceMapping.n.SnapshotId or SnapshotId does not exist.	404	The error message returned when the specified snapshot does not exist.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter SnapshotId or InstanceId or DiskDeviceMapping that is mandatory for processing this request is not supplied.	400	The error message returned when one of the required SnapshotId, InstanceId, or DiskDeviceMapping parameters is not specified.
InvalidSize.ValueNotSupported	The specified parameter DiskDeviceMapping.n.Size beyond the permitted range.	400	The error message returned when the specified DiskDeviceMapping.n.Size value is beyond the valid range.
OperationDenied	The specified parameter DiskDeviceMapping.n.SnapshotId does not contain system disk snapshot.	400	The error message returned when the specified DiskDeviceMapping.n.SnapshotId parameter does not contain the system disk snapshot.
OperationDenied	The specified parameter DiskDeviceMapping.n.SnapshotId contains two or more system disk snapshots.	400	The error message returned when the specified DiskDeviceMapping.n.SnapshotId parameter contains multiple system disk snapshots.
InvalidInstanceId.ValueNotSupported	The specified InstanceId is not allowed to create image.	400	The error message returned when the specified instance cannot be used to create custom images.
InvalidAccountStatus.SnapshotServiceUnavailable	Snapshot service has not been opened yet.	403	The error message returned when you have not activated the snapshot service yet.

Examples

Sample requests

```
https://ecs.example.com/?Action=CreateImage
&RegionId=cn-hangzhou
&SnapshotId=s-snapshot1
&ImageName=demo_image
&Common request parameters
```

Sample responses

XML format

```
<CreateImageResponse>
   <RequestId>C8B26B44-0189-443E-9816-D951F59623A9</RequestId>
   <ImageId>m-63DFD5FB2</ImageId>
</CreateImageResponse>
```

JSON format

```
{
   "RequestId": "C8B26B44-0189-443E-9816-D951F59623A9",
   "ImageId": "m-63DFD5FB2"
}
```

2.1.1.9.2. DescribeImages

You can call this operation to query available images.

When you call this operation, note that:

- You can query both your own images and system resources provided by Alibaba Cloud.
- This operation supports paged query. The response contains the total number of available image resources and the image resources on the current page. Ten entries are displayed on each page by default.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeImages.
RegionId	String	Yes	The ID of the region to which the images belong.
ImageId	String	No	The IDs of images to be queried. You can specify a maximum of 100 IDs, separated with commas (,).

Name	Type	Required	Description
Status	String	No	The image status. Valid values: UnAvailable | Available | Creating | CreateFailed. Default value: Available. Value description: • Creating: The image is being created. • Available: The image is available. • Unavailable: The image is unavailable. • CreateFailed: The image failed to be created.
SnapshotId	String	No	The ID of the snapshot used to create the image.
ImageName	String	No	The name of the image.
ImageOwnerAlias	string	No	The alias of the image owner. Valid values: system | self | others | marketplace. Default value: null, indicating that results that match "system + self + others" are returned. If not specified, this parameter is not used as a filtering condition. Value description: • system: The image is provided by Alibaba Cloud. • self: The image is created by the user. • others: The image is available and is created by other users.
Usage	String	No	The referenced resource type. Valid values: instance | none.
Tag.n.Key	String	No	The key of the tag. The value of n ranges from 1 to 5. It cannot be a null string.
Tag.n.Value	String	No	The value of the tag. The value of n ranges from 1 to 5. It can be a null string.
PageNumber	Integer	No	The page number that you query in the instance status list. Starting value: 1. Default value: 1.
PageSize	Integer	No	The number of entries to be displayed per page. Maximum value: 100. Default value: 10.

Response parameters

Response parameter description

Name	Type	Description
RegionId	String	The ID of the region to which the image belongs.
TotalCount	Integer	The total number of queried entries.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of entries on the current page.
Images	ImageType	A set of ImageType data.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidImageOwnerAlias.ValueNotSupported	The specified ImageOwnerAlias value is not supported.	400	The error message returned when the ImageOwnerAlias parameter is invalid.
InvalidUsage	The specified Usage is not valid.	404	The error message returned when the Usage parameter is invalid.
InvalidTag.Mismatch	The specified Tag.n.Key and Tag.n.Value are not match.	400	The error message returned when the specified Tag.n.Key and Tag.n.Value parameters do not match.
InvalidTagCount	The specified tags are beyond the permitted range.	400	The error message returned when more than five tags are specified.

Error code	Error message	HTTP status code	Description
InvalidInstanceType.ValueNotSupported	The specified InstanceType beyond the permitted range.	400	The error message returned when the InstanceType parameter is invalid.
InvalidOSType	The specified OSType is not valid.	404	The error message returned when the OSType parameter is invalid.
InvalidArchitecture	The specified Architecture is not valid.	404	The error message returned when the specified system architecture is invalid.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeImages
&RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

XML format

```
<DescribeImagesResponse>
  <Images>
    <Image>
      <Architecture>i386</Architecture>
      <CreationTime>2014-07-22T09:53:44Z</CreationTime>
      <Description></Description>
      <DiskDeviceMappings>
        <DiskDeviceMapping>
          <Device>/dev/xvda</Device>
          <Size>20</Size>
          <SnapshotId></SnapshotId>
        </DiskDeviceMapping>
      </DiskDeviceMappings>
      <ImageId>suse11sp3_64_20G_aliaegis_20150428.vhd</ImageId>
      <ImageName>suse11sp3_64_20G_aliaegis_20150428.vhd</ImageName>
      <ImageOwnerAlias>system</ImageOwnerAlias>
      <ImageVersion>1.0</ImageVersion>
      <IsCopied>false</IsCopied>
      <IsSubscribed>false</IsSubscribed>
      <OSName>SUSE Linux  Enterprise Server 11 SP3 64 bit</OSName>
      <ProductCode></ProductCode>
      <OSType>linux</OSType>
      <Platform>SUSE</Platform>
      <Progress>100</Progress>
      <Size>20</Size>
      <Status>Available</Status>
      <Usage>instance</Usage>
    </Image>
  </Images>
  <PageNumber>1</PageNumber>
  <PageSize>2</PageSize>
  <RegionId>cn-hangzhou</RegionId>
  <TotalCount>24</TotalCount>
  <RequestId>7871BB26-3002-4950-B2E6-98D333077EA5</RequestId>
</DescribeImagesResponse>
```

JSON format

```
{
 "Images": {
  "Image": [
   {
    "Architecture": "x86_64",
    "CreationTime": "2015-05-06T09:01:32Z",
    "DiskDeviceMappings": {
     "DiskDeviceMapping": [
      {
       "Device": "/dev/xvda",
       "Size": "20"
      }
     ]
    },
    "ImageId": "suse11sp3_64_20G_aliaegis_20150428.vhd",
    "ImageName": "suse11sp3_64_20G_aliaegis_20150428.vhd",
    "ImageOwnerAlias": "system",
    "ImageVersion": "1",
    "IsCopied": false,
    "IsSubscribed": false,
    "OSName": "SUSE Linux  Enterprise Server 11 SP3 64 bit",
    "OSType": "linux",
    "Platform": "SUSE",
    "Progress": "100%",
    "Size": 20,
    "Status": "Available",
    "Usage": "instance"
   }
  ]
 }
 "PageNumber": 1,
 "PageSize": 1,
 "RegionId": "cn-hangzhou",
 "RequestId": "49CBCED4-C9B9-4851-BEB5-8FB5E5169E30",
 "TotalCount": 24
}
```


2.1.1.9.3. ModifyImageAttribute

You can call this operation to modify the name and description of a custom image.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyImageAttribute.
RegionId	String	Yes	The ID of the region to which the custom image belongs.
ImageId	String	Yes	The ID of the custom image.
ImageName	String	No	The name of the custom image. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with http:// or https://.
Description	String	No	The description of the custom image. The description must be 0 to 256 characters in length. If not specified, this parameter is null. Default value: null. It cannot start with http:// or https://.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Description	HTTP status code	Description
MissingParameter	An input parameter \"RegionId\" that is mandatory for processing the request is not supplied.	400	The error message returned when the required parameter RegionId is not specified.
MissingParameter	An input parameter \"ImageId\" that is mandatory for processing the request is not supplied.	400	The error message returned when the required parameter ImageId is not specified.
InvalidImageId.NotFound	The image does not exist.	403	The error message returned when the specified image ID does not exist.

Error code	Description	HTTP status code	Description
InvalidImageName.Malformed	The specified destination Image name is wrongly formed.	400	The error message returned when the specified image name is invalid.
InvalidDescription.Malformed	The specified destination image description is wrongly formed.	400	The error message returned when the specified image description is invalid.
InvalidImageName.Duplicated	The destination image is exist.	400	The error message returned when the name of the custom image is already in use.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifyImageAttribute
&ImageId=m-281234567
&RegionId=cn-qingdao
&ImageName=testImage123
&Common request parameters
```

Sample responses

XML format

```
<ModifyImageAttributeResponse>
    <RequestId>C8B26B44-0189-443E-9816-D951F59623A9</RequestId>
</ModifyImageAttributeResponse>
```

JSON format

```
{
    "RequestId": "C8B26B44-0189-443E-9816-D951F59623A9"
}
```

2.1.1.9.4. DeleteImage

You can call this operation to delete a custom image. A deleted image cannot be used to create or reset an ECS instance.

When you call this operation, note that:

If the specified image does not exist, the request will be ignored.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteImage.
RegionId	String	Yes	The ID of the region to which the custom image belongs.
ImageId	String	Yes	The ID of the custom image.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The specified region does not exist.	404	The error message returned when the Region parameter is invalid or you are not authorized to access the region.
ImageUsingByInstance	The specified image has been used to create instance(s).	403	The error message returned when the specified image is still being used by an instance and cannot be deleted.
ImageUseShared	The specified image has been shared to others.	403	The error message returned when the specified image has been shared.
OperationDenied.ImageCopying	The Image is coping.	403	The error message returned when the specified image is being copied.

Error code	Error message	HTTP status code	Description
ImageIsCreating	The specified image is creating.	403	The error message returned when the specified image is being created.

Examples

Sample requests

```
https://ecs.example.com/?Action=DeleteImage
&RegionId=cn-hangzhou
&ImageId=m-63DFD5FB2
&Common request parameters
```

Sample responses

XML format

```
<DeleteImageResponse>
    <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</DeleteImageResponse>
```

JSON format

```
{
  "RequestId": "CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.1.1.9.5. CopyImage

You can call this operation to copy a custom image from one region to another for consistent deployment. The copied image can be used to perform operations in the target region, such as creating instances and replacing system disks.

When you call this operation, note that:

- Only custom images that are in the Available state can be copied.
- You must submit a ticket to activate the image copy service.
- You can only copy the image within your own Apsara Stack tenant account. You cannot copy an image to another Apsara Stack tenant account.
- While the image copy operation is being performed, the original image cannot be deleted. The image copy operation can be canceled before the operation is completed.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CopyImage.
RegionId	String	Yes	The ID of the region to which the source custom image belongs.
ImageId	String	Yes	The ID of the source custom image.
DestinationRegionId	String	Yes	The ID of the region that the custom image is to be copied to.
DestinationImageName	String	No	The name of the destination image. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with http:// or https://.
DestinationDescription	String	No	The description of the destination image. The description must be 0 to 256 characters in length. If not specified, this parameter is null. Default value: null. It cannot start with http:// or https://.

Response parameters

Response parameter description

Name	Type	Description
ImageId	String	The ID of the destination image.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidImageId.NotFound	The image does not exist.	400	The error message returned when the specified image ID does not exist.
InvalidImageName.Malformed	The specified destination Image name is wrongly formed.	400	The error message returned when the specified image name is invalid.

Error code	Error message	HTTP status code	Description
SourceRegion.NotFound	The source region not found	400	The error message returned when the specified region ID does not exist.
DestinationRegion.NotFound	The destination region not found	400	The error message returned when the specified region ID does not exist.
InvalidImageName.Duplicated	The destination image is exist.	400	The error message returned when the name of the destination image is already in use.
QuotaExceed.Image	The Image Quota exceeds.	403	The error message returned when no more images can be copied because the number of custom images has reached the upper limit.
QuotaExceed.Snapshot	The Snapshot Quota exceeds.	403	The error message returned when no more images can be copied because the number of snapshots has reached the upper limit.
Forbidden	User not authorized to operate on the specified resource.	403	The error message returned when you have no permission to copy the image.
RegionNotSupportCopy	The region not support copy.	403	The error message returned when the source region or destination region do not support image copying.
IncorrectDestinationRegion	The destination region is not equal the target region.	403	The error message returned when the destination region is the same as the source region.

Error code	Error message	HTTP status code	Description
InvalidImageName.Malformed	The specified Image name is wrongly formed.	400	The error message returned when the value of the ImageName parameter contains unsupported characters or exceeds the maximum length.
InvalidDescription.Malformed	The specified destination description is wrongly formed.	400	The error message returned when the Description parameter is invalid.
InvalidDescription.Malformed	The specified description is wrongly formed.	400	The error message returned when the Description parameter is invalid.
IncorrectImageStatus	The image not available.	400	The error message returned when the image is in a state that does not support the current operation.
InvalidSnapshotId.NotFound	The snapshot for the image does not exist.	400	The error message returned when the specified snapshot does not exist.
OperationDenied.ImageCopying	The Image are coping.	403	The error message returned when the specified image is being copied.
InvalidSnapshot.TooOld	This operation is denied because the specified snapshot is created before 2013-07-15.	403	The error message returned when the snapshot of the specified image was created on or before July 15, 2013.
OperationDenied	The specified snapshot is not allowed to create image.	403	The error message returned when the snapshot of a specific disk cannot be used to create an image.

Examples

Sample requests

```
https://ecs.example.com/?Action=CopyImage
&DestinationRegionId=cn-hangzhou
&ImageId=m-281234567
&RegionId=cn-qingdao
&Common request parameters
```

Sample responses

XML format

```
<CopyImageResponse>
  <RequestId>C8B26B44-0189-443E-9816-D951F59623A9</RequestId>
  <ImageId>Img-231234567</ImageId>
</CopyImageResponse>
```

JSON format

```
{
  "RequestId": "C8B26B44-0189-443E-9816-D951F59623A9",
  "ImageId": "Img-231234567"
}
```

2.1.1.9.6. CancelCopyImage

You can call this operation to cancel an image copy task. The image is automatically deleted after the task is canceled.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CancelCopyImage.
RegionId	String	Yes	The ID of the region to which the target image belongs.
ImageId	String	Yes	The ID of the target image being copied.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
IncorrectImageStatus	The image has completed copy.	400	The error message returned when the image copy operation cannot be canceled because the operation has already completed.
InvalidRegionId.NotFound	The specified region does not exist.	404	The error message returned when the specified region ID does not exist.
InvalidImageId.NotFound	The specified image does not exist.	404	The error message returned when the specified image does not exist.
ImageCreatedNotFromCopy	The specified image not from copy.	400	The error message returned when the specified image is not the original copy of the image.
IncorrectImageStatus	The image is copied finished.	400	The error message returned when the image copy has already completed.
IncorrectImageStatus	The specified snapshot is not coping.	400	The error message returned when the snapshot of the specified image is not being copied.
IncorrectImageStatus	The specified image is not coping.	400	The error message returned when the specified image is not being copied.
IncorrectImageStatus	The Image copy has been failed.	400	The error message returned when the image copy operation failed for some other reasons.

Examples

Sample requests

```
https://ecs.example.com/?Action=CancelCopyImage
&RegionId=cn-hangzhou
&ImageId=img-2012-12-01-1300
&Common request parameters
```

Sample responses

XML format

```
<CancelCopyImageResponse>
  <RequestId>C8B26B44-0189-443E-9816-D951F59623A9</RequestId>
</CancelCopyImageResponse>
```

JSON format

```
{"RequestId": "C8B26B44-0189-443E-9816-D951F59623A9"}
```

2.1.1.9.7. ModifyImageSharePermission

You can call this operation to manage what accounts a custom image is shared to. You can share a custom image to other Apsara Stack tenant accounts and allow those accounts to create instances and change system disks.

When you call this operation, note that:

- You can share only your own custom images to other Apsara Stack tenant accounts.
- A single image can be shared to a maximum of 10 accounts at a time. Each request can remove a maximum of 10 accounts that an image is shared to. If more than 10 accounts are specified by the AddAccount.n or RemoveAccount.n parameter, the parameter will be ignored.
- A single user can have a maximum of 30 images that are shared by other users. You can configure a whitelist for these images.
- A single image can be shared to a maximum of 50 users. These users can apply to be included into the whitelist and share their custom images to more users.
- If an image that is shared to you is deleted by the owner or if the owner stops sharing the image to you, instances you own that rely on the shared image will fail to reset their system disks.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyImageSharePermission.
RegionId	String	Yes	The ID of the region to which the custom image belongs.

Name	Type	Required	Description
ImageId	String	Yes	The ID of the custom image.
AddAccount.n	String	No	The IDs of Apsara Stack tenant accounts that you want to add to the shared group. Value range of n: [1, 10]. If n is greater than 10, this parameter will be ignored.
RemoveAccount.n	String	No	The IDs of Apsara Stack tenant accounts that you want to remove from the shared group. Value range of n: [1, 10]. If n is greater than 10, this parameter will be ignored.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	An input parameter \"RegionId\" that is mandatory for processing the request is not supplied.	400	The error message returned when the required parameter RegionId is not specified.
MissingParameter	An input parameter \"ImageId\" that is mandatory for processing the request is not supplied.	400	The error message returned when the required parameter ImageId is not specified.
InvalidRegionId.NotFound	The specified region does not exist.	400	The error message returned when the specified region ID does not exist.
InvalidImageId.NotFound	The specified Image does not exist or not you owner.	403	The error message returned when the specified image ID does not exist.
IncorrectImageStatus	The image is not available.	400	The error message returned when the image is in a state that does not support the current operation.

Error code	Error message	HTTP status code	Description
InvalidAccount.NotFound	The specified parameter AddAccount.n or RemoveAccount.n does not exist.	404	The error message returned when the specified account does not exist.
QuotaExceed.ShareImage	The share Image Quota exceeds.	403	The error message returned when the number of custom images has reached the upper limit.
QuotaExceed.ShareImageUser	The shared image user quota exceeds.	403	The error message returned when the number of users to which one image is shared has reached the upper limit.
InvalidAccount.Forbbiden	The specified account does not yourself.	404	The error message returned when you are trying to share the image to your own account.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifyImageSharePermission
&RegionId=cn-hangzhou
&ImageId=m-281234567
&AddAccount. 1=23412345234
&Common request parameters
```

Sample responses

XML format

```
<ModifyImageSharePermissionResponse>
  <RequestId>C8B26B44-0189-443E-9816-D951F59623A9</RequestId>
</ModifyImageSharePermissionResponse>
```

JSON format

```
{
  "RequestId": "C8B26B44-0189-443E-9816-D951F59623A9"
}
```

2.1.1.9.8. DescribeImageSharePermission

You can call this operation to query the accounts to which a custom image is shared. This operation supports paged query. Ten entries are displayed on each page by default.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeImageSharePermission.
RegionId	String	Yes	The ID of the region to which the custom image belongs.
ImageId	String	Yes	The ID of the custom image.
PageNumber	Integer	No	The page number that you query in the account list. Starting value: 1. Default value: 1.
PageSize	Integer	No	The number of entries to be displayed per page. Maximum value: 50. Default value: 10.

Response parameters

Response parameter description

Name	Type	Description
ImageId	String	The ID of the custom image.
RegionId	String	The ID of the region to which the custom image belongs.
ShareGroups	ShareGroupType	The shared group information.
Accounts	AccountType	The Apsara Stack tenant accounts to which the custom image is shared.
TotalCount	Integer	The total number of entries.
PageNumber	Integer	The page number.
PageSize	Integer	The maximum number of entries per page. Maximum value: 50. Default value: 10.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required parameter RegionId is not specified.
MissingParameter	The input parameter ImageId that is mandatory for processing this request is not supplied.	400	The error message returned when the required parameter ImageId is not specified.
InvalidRegionId.NotFound	The specified region does not exist.	404	The error message returned when the specified region ID does not exist.
InvalidImageId.NotFound	The specified ImageId does not exist.	404	The error message returned when the specified image ID does not exist.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeImageSharePermission
&RegionId=cn-qingdao
&ImageId=m-282dzntc7
&Common request parameters
```

Sample responses

XML format

```
<DescribeImageSharePermissionResponse>
  <ImageId>m-282dzntc7</ImageId>
  <PageNumber>1</PageNumber>
  <PageSize>10</PageSize>
  <RegionId>cn-qingdao</RegionId>
  <TotalCount>1</TotalCount>
  <RequestId>441CF898-42FF-47CF-9348-3C3BFF557278</RequestId>
  <ShareGroups>
    <ShareGroup>
      <Group>all</Group>
    </ShareGroup>
  </ShareGroups>
  <Accounts>
    <Account>
      <AliyunId>188650852989****</AliyunId>
    </Account>
  </Accounts>
</DescribeImageSharePermissionResponse>
```

2.1.1.9.9. ImportImage

You can call this operation to import an offline image file to ECS to create a custom image. You can use the custom image to create an ECS instance or replace a system disk.

When you call this operation, note that:

- Before you call this operation, upload the offline image file to OSS.
- The imported image must belong to the same account and region as the OSS bucket that stores the image file.
- The DiskDeviceMapping.N parameter can only be set to 1. This indicates that only system disk images can be used by this operation to create disks. Data disks cannot be created from images.
- Before the image has finished being imported, the image cannot be deleted but the import operation can be canceled.
- You must use RAM to grant the OSS read permission to your Apsara Stack tenant account.
  i. Create a role named AliyunECSImageImportDefaultRole (image import fails if a different name is used). The role policy is as follows:

     ```
     { "Statement": [ { "Action": "sts:AssumeRole", "Effect": "Allow", "Principal": { "Service": [ "ecs.example.com" ] } } ], "Version": "1"}
     ```

  ii. Add the default system permission policy AliyunECSImageImportRolePolicy to the role. It is the default policy provided by ECS for image import. You can also create a custom policy with the following permissions:

```
{ "Version": "1", "Statement": [ { "Action": [ "oss:GetObject", "oss:GetBucketLocation" ], "Resource" : "*", "Effect": "Allow" } ] }
```

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ImportImage.
RegionId	String	Yes	The ID of the region to which the custom image to be imported belongs.
ImageName	String	No	The name of the image. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It cannot start with `http://` or `https://`.
Description	String	No	The description of the image. The description must be 0 to 256 characters in length. This parameter is null if it is not specified. Default value: null. It cannot start with `http://` or `https://`.
Architecture	String	No	The system architecture of the imported image. Valid values: i386 | x86_64. Default value: x86_64.
OSType	String	No	The operating system type of the imported image. Valid values: windows | linux. Default value: linux.

Name	Type	Required	Description
Platform	String	No	The release version of the operating system. Valid values: • CentOS • Ubuntu • SUSE • OpenSUSE • RedHat • Debian • CoreOS • Aliyun Linux • Windows Server 2003 • Windows Server 2008 • Windows Server 2012 • Windows 7 • Others Linux Default value: Others Linux.
DiskDeviceMapping.n.Format	String	No	The format of the imported image. Valid values: RAW and VHD. Default value: RAW.
DiskDeviceMapping.n.OSSBucket	String	Yes	The OSS bucket where the image file is stored.
DiskDeviceMapping.n.OSSObject	String	Yes	The key in the OSS object.
DiskDeviceMapping.n.DiskImageSize	String	No	The capacity of the system disk that is created by using an image file. The space of the system disk must be larger than or equal to that of the file system. • If the operating system is Linux, the value range is 20 GB to 1 TB and the default value is 20 GB. • If the operating system is Windows, the value range is 40 GB to 1 TB and the default value is 40 GB.

Response parameters

Response parameter description

Name	Type	Description
RegionId	String	The region ID.
ImageId	String	The image ID.

Name	Type	Description
ImportTaskId	String	The ID of the image import task.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	An input parameter \"RegionId\" that is mandatory for processing the request is not supplied.	400	The error message returned when the required RegionId parameter is not specified.
MissingParameter	An input parameter \"DiskDeviceMapping.n.OSSBucket\" that is mandatory for processing this request is not supplied.	400	The error message returned when the required OSSBucket parameter is not specified.
MissingParameter	An input parameter "DiskDeviceMapping.n.OSSObject" that is mandatory processing this request is not supplied.	400	The error message returned when the required OSSObject parameter is not specified.
InvalidImageName.Malformed	The specified destination Image name is wrongly formed.	400	The error message returned when the specified image name is invalid.
InvalidDescription.Malformed	The specified destination image description is wrongly formed.	400	The error message returned when the specified description of the imported image is invalid.

Error code	Error message	HTTP status code	Description
RegionId.NotFound	The specified region is not found.	400	The error message returned when the specified region ID does not exist.
IncorrectImageStatus	The specified image is not available.	400	The error message returned when the specified image is in a state that does not support the current operation.
InvalidImageName.Duplicated	The destination image is exist.	400	The error message returned when the specified image name already exists.
QuotaExceed.Image	The Image Quota exceeds.	403	The error message returned when no more images can be imported because the maximum number of custom images has been reached.
QuotaExceed.Snapshot	The Snapshot Quota exceeds.	403	The error message returned when no more images can be imported because the maximum number of snapshots has been reached.

Error code	Error message	HTTP status code	Description
Forbidden	User not authorized to operate on the specified resource	400	The error message returned when you do not have the permission to import the image.
InvalidArchitecture.Malformed	The specified Architecture is wrongly formed.	400	The error message returned when the specified system architecture is invalid.
InvalidPlatform.Malformed	The specified Platform is wrongly formed.	400	The error message returned when the specified operating system release version is invalid.
InvalidOSType.Malformed	The specified OSType is wrongly formed.	400	The error message returned when the specified operating system type is invalid.
InvalidFormat.Malformed	The specified Image format is wrongly formed.	400	The error message returned when the format of the specified image file is invalid.
InvalidImageSize	The specified "DiskDeviceMapping.n.DiskImageSize" should be not less than system device size.	400	The error message returned when the disk capacity specified for the image is invalid.

Error code	Error message	HTTP status code	Description
ImageIsImporting	The specified Image is importing.	403	The error message returned when the specified image is being copied.
InvalidRegion.NotSupport	The specified region does not support image import or export.	403	The error message returned when the specified region does not support image import.

Examples

Sample requests

```
https://ecs.example.com/?Action=ImportImage
&RegionId=cn-hangzhou
&DiskDeviceMapping. 1. OSSBucket=ecsimageos
&DiskDeviceMapping. 1. OSSObject=CentOS_5.4_32.raw
&Common request parameters
```

Sample responses

XML format

```
<ImportImageResponse>
   <RequestId>C8B26B44-0189-443E-9816-D951F59623A9</RequestId>
   <ImageId>Img-231234567</ImageId>
   <ImportTaskId>123-345-2332-22323</ImportTaskId>
</ImportImageResponse>
```

JSON format

```
{
   "RequestId": "C8B26B44-0189-443E-9816-D951F59623A9",
   "ImageId": "Img-231234567",
   "ImportTaskId":"123-345-2332-22323"
}
```

2.1.1.9.10. ExportImage

You can call this operation to export a custom image to an OSS bucket within the same region.

When you call this operation, note that:

- Only available custom images can be exported.
- Before a custom image can be exported, you must use RAM to grant the OSS write permission to your Apsara Stack tenant account.
  i. Create a role named AliyunECSImageExportDefaultRole (image export fails if a different name is used). The role policy is as follows:

```
{ "Statement": [ { "Action": "sts:AssumeRole", "Effect": "Allow", "Principal": { "Service": [ "ecs.example.com" ] } } ], "Version": "1"}
```

  ii. Add the default system permission policy AliyunECSImageExportRolePolicy to the role. This is the default policy for image export provided by ECS. You can also create a custom policy with the following permissions:

```
{ "Version": "1", "Statement": [ { "Action": [ "oss:GetObject", "oss:PutObject", "oss:DeleteObject", "oss:GetBucketLocation", "oss:AbortMultipartUpload", "oss:ListMultipartUploads", "oss:ListParts" ], "Resource": "*", "Effect": "Allow" } ]}
```

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ExportImage.
RegionId	String	Yes	The ID of the region to which the custom image to be exported belongs.
ImageId	String	Yes	The ID of the custom image to be exported.
OSSBucket	String	Yes	The OSS bucket to which the image is to be exported.
OSSPrefix	String	No	The prefix of your OSS object.

Name	Type	Required	Description
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency in the Appendix.

Response parameters

Response parameter description

Name	Type	Description
RegionId	String	The region ID.
ExportTaskId	String	The ID of the image export task.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	An input parameter \"RegionId\" that is mandatory for processing the request is not supplied.	400	The error message returned when the required RegionId parameter is not specified.
MissingParameter	An input parameter \"ImageId\" that is mandatory for processing the request is not supplied.	400	The error message returned when the required ImageId parameter is not specified.
MissingParameter	An input parameter \"OSSBucket\" that is mandatory for processing the request is not supplied.	400	The error message returned when the required OSSBucket parameter is not specified.

Error code	Error message	HTTP status code	Description
ImageId.NotFound	The image does not exist.	403	The error message returned when the specified image ID does not exist.
RegionId.NotFound	The specified region is not found.	400	The error message returned when the specified region ID does not exist.
IncorrectImageStatus	The image is not available.	400	The error message returned when the specified instance is in a state that does not support the current operation.
OSSBucket.NotFound	The specified OSSBucket is not exist.	400	The error message returned when the specified OSS bucket does not exist in the current region.
Forbidden	User not authorized to operate on the specified resource.	400	The error message returned when you do not have permission to export the image.
OperationDenied.ImageExporting	The Image is exporting.	403	The error message returned when the specified image is being exported.
OSSPrefix.Malformed	The specified OSSPrefix Format is wrongly formed.	400	The error message returned when the format of the specified OSS object prefix is invalid.

Error code	Error message	HTTP status code	Description
InvalidRegion.NotSupport	The specified region does not support image import or export.	403	The error message returned when the specified region does not support image export.
ExportImageFailed	Exporting image is failed,Please contact the administrator.	403	The error message returned when the image failed to be exported. Contact an administrator.

Examples

Sample requests

```
https://ecs.example.com/?Action=ExportImage
&RegionId=cn-hangzhou
&ImageId=m-231234567
&OSSBucket=testexportImage
&Common request parameters
```

Sample responses

XML format

```
<ExportImageResponse>
 <RequestId>C8B26B44-0189-443E-9816-D951F59623A9</RequestId>
 <ExportTaskId>tsk-231234567</ExportTaskId>
   <RegionId>cn-hangzhou</RegionId>
</ExportImageResponse>
```

JSON format

```
{
   "RequestId": "C8B26B44-0189-443E-9816-D951F59623A9",
   "RegionId": "cn-hangzhou",
   "ExportTaskId": "tsk-231234567"
}
```

2.1.1.10. Network

2.1.1.10.1. AllocatePublicIpAddress

You can call this operation to assign an available public IP address to a specific instance.

When you call this operation, note that:

- This operation can be called only when the instance is in the Running or Stopped state.
- The assigned IP address will take effect only after the instance is started or restarted.
- Each instance can only be assigned a single IP address.
- IP address segments cannot be assigned to instances. If this operation is called for an instance which has already been assigned a public IP address, the original IP address is returned.
- If an instance is locked for security reasons, no public IP addresses can be assigned to the instance.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AllocatePublicIpAddress.
InstanceId	String	Yes	The ID of the instance to which you want to assign an IP address.

Response parameters

Response parameter description

Name	Type	Description
IpAddress	String	The public IP address that you want to assign to the instance.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	404	The error message returned when the specified instance ID does not exist.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the current instance status does not support this operation.

Error code	Error message	HTTP status code	Description
InstanceLockedForSecurity	The specified operation is denied as your instance is locked for security reasons.	403	The error message returned when the specified instance is locked for security reasons.
IpInUse	The specified IP is already in use.	403	The error message returned when the specified IP address is already in use by another host.
AllocatedAlready	There is an IpAddress allocated already for the specified instance.	403	The error message returned when an IP address is already assigned to the specified instance.
OperationDenied	Specified operation is denied as your instance is in VPC.	400	The error message returned when the specified instance belongs to a VPC.
InsufficientPublicIp	Ip address not found	400	The error message returned when no IP addresses can be assigned.

Examples

Sample requests

```
https://ecs.example.com/?Action=AllocatePublicIpAddress
&InstanceId=i-instance1
&Common request parameters
```

Sample responses

XML format

```
<AllocatePublicIpAddressResponse>
    <RequestId>F2EF6A3B-E345-46B9-931E-0EA094818567</RequestId>
    <IpAddress>10.1.149.159</IpAddress>
</AllocatePublicIpAddressResponse>
```

JSON format

```
{
    "RequestId": "F2EF6A3B-E345-46B9-931E-0EA094818567",
    "IpAddress": "10.1.149.159"
}
```

2.1.1.10.2. ModifyInstanceNetworkSpec

You can call this operation to modify the bandwidth configurations of an ECS instance.

When the specified bandwidth of an existing network is insufficient, you can call this operation to modify the bandwidth and improve network performance. When you call this operation, note that:

- Only the parameters that are specified in the request are modified, all other parameters will remain the same.
- You can modify the maximum inbound and outbound bandwidth of an instance only when the instance is in the Stopped or Running state.
- If an instance is locked for security reasons, the bandwidth specifications of the instance cannot be modified.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyInstanceNetworkSpec.
InstanceId	String	Yes	The ID of the instance that you want to modify.
InternetMaxBandwidthOut	Integer	No	The maximum outbound bandwidth to the Internet. Unit: Mbit/s.
InternetMaxBandwidthIn	Integer	No	The maximum inbound bandwidth from the Internet. Unit: Mbit/s.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description

Error code	Error message	HTTP status code	Description
InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	404	The error message returned when the specified insatnce does not exist.
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.
InvalidParameter	The specified parameter InternetMaxBandwidthIn is not valid.	400	The error message returned when the specified InternetMax BandwidthIn parameter is not a numeric value.
InvalidInternetMax-BandwidthIn.ValueNotSupported	The specified InternetMaxBandwidthIn beyond the permitted range.	400	The error message returned when the specified InternetMax BandwidthIn value exceeds the valid range.

Error code	Error message	HTTP status code	Description
InvalidParameter	The specified parameter InternetMaxBandwidthOut is not valid.	400	The error message returned when the specified InternetMaxBandwidthOut parameter is not a numeric value.
InvalidInternetMax-BandwidthOut.ValueNotSupported	The specified InternetMaxBandwidthOut beyond the permitted range.	400	The error message returned when the specified InternetMaxBandwidthOut value exceeds the valid range.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the current instance status does not support this operation.
InstanceLockedForSecurity	The specified operation is denied as your instance is locked for security reasons.	403	The error message returned when the specified instance is locked for security reasons.
InternalError	The request processing has failed due to some unknown error.	500	The error message returned when an internal error occurs.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifyInstanceNetworkSpec
&InstanceId=i-23nn22421
&InternetMaxBandwidthOut=20
&Common request parameters
```

Sample responses

XML format

```
<ReleasePublicIpAddressResponse>
  <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</ReleasePublicIpAddressResponse>
```

JSON format

```
{
  "RequestId":"CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.1.1.11. Security groups

2.1.1.11.1. CreateSecurityGroup

You can call this operation to create a security group. You can configure the firewall rules for a group of instances. One security group can contain multiple instances.

When you call this operation, note that:

- A newly created security group only authorizes access for instances within the group. All other access permissions are denied. If you want to permit access from instances in other groups or from the Internet, you can call AuthorizeSecurityGroup or AuthorizeSecurityGroupEgress to change the firewall policies of the security group.
- Firewall rules are differentiated between the Intranet and the Internet.
- Each user can create a maximum of 100 security groups.
- You must specify the VpcId parameter if you want to create a VPC security group.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateSecurityGroup.

Name	Type	Required	Description
RegionId	String	Yes	The ID of the region to which the security group belongs.
SecurityGroupName	String	No	The name of the security group. If not specified, this parameter is null. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It is displayed in Apsara Stack Operations Console. It cannot start with `http://` or `https://`.
Description	String	No	The description of the security group. The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.
VpcId	String	No	The ID of the VPC to which the security group belongs.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency in the Appendix.

Response parameters

Response parameter description

Name	Type	Description
SecurityGroupId	String	The ID of the security group.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.

Error code	Error message	HTTP status code	Description
InvalidSecurity-GroupName.Malformed	Specified security group name is not valid.	400	The error message returned when the format of the SecurityGroupName parameter is invalid.
InvalidDescription.Malformed	The specified parameter Description is not valid.	400	The error message returned when the format of the DescriptionName parameter is invalid.
QuotaExceed.SecurityGroup	The security group quota exceeds.	403	The error message returned when the number of security groups has reached the quota.
InvalidVpcId.NotFound	Specified VPC does not exist.	404	The error message returned when the specified VPC does not exist.
InvalidSecurityGroupDiscription.Malformed	Specified security group description is not valid.	400	The error message returned when the Description parameter is invalid.
InvalidVpcId.NotFound	vpc id must not empty when only support vpc vm.	403	The error message returned when the required VpcId parameter is not specified.
IncorrectVpcStatus	Current VPC status does not support this operation.	400	The error message returned when the current VPC status does not support this operation.

Examples

Sample requests

```
https://ecs.example.com/?Action=CreateSecurityGroup
&RegionId=cn-hangzhou
&Description=for_demo
&Common request parameters
```

Sample responses

XML format

```
<CreateSecurityGroupResponse>
    <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
    <SecurityGroupId>sg-F876FF7BA</SecurityGroupId>
</CreateSecurityGroupResponse>
```

JSON format

```
{
    "RequestId":"CEF72CEB-54B6-4AE8-B225-F876FF7BA984",
    "SecurityGroupId":"sg-F876FF7BA"
}
```

2.1.1.11.2. AuthorizeSecurityGroup

You can call this operation to set the inbound access permissions of a security group.

When you call this operation, note that:

- You can set the authorization policy to accept or drop. Accept will grant access to the security group, while drop will deny access.
- Both Internet and intranet network types are supported and are controlled by the NicType parameter. A VPC-type ECS instance supports only intranet.
- A maximum of 100 rules can be configured for one security group.
- The security group priorities are sorted by creation time in descending order.
- The priority of a rule can be set to a value from 1 to 100. The default value is 1, which is the highest priority. A greater value indicates a lower priority.
- If the priority of two conflicting authorization rules are equal, drop rules will take precedence over accept rules.
- Cross-group authorization can only be performed on security groups with the NicType parameter set to intranet.
- A security group rule is defined by one of the following parameter sets: set 1 (SourceGroupOwnerAccount, SourceGroupId, IpProtocol, PortRange, NicType, and Policy) and set 2 (SourceCidrIp, IpProtocol, PortRange, NicType, and Policy). An error will be returned if the rule being created matches an existing rule.
- Two authorization methods are supported:
  - Grant access permissions to other security groups in the same region. (Cross-user authorization is allowed when using this method.)
  - Grant access permissions to the range of IP addresses specified in CIDR notation.

Request parameters

Request parameter description

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AuthorizeSecurityGroup.
SecurityGroupId	String	Yes	The ID of the destination security group.
RegionId	String	Yes	The ID of the region to which the destination security group belongs.
IpProtocol	String	Yes	The IP protocol to be used for the security group. Valid values: tcp | udp | icmp | gre | all. The value all indicates the support of all the four protocols.
PortRange	String	Yes	The range of port numbers corresponding to the IP protocol. • When IpProtocol is set to tcp or udp, the default port numbers are used, and the port number range is 1 to 65535. For example, 1/200 indicates that the port number range is 1 to 200. If 200/1 is specified, the operation will return an error. • When IpProtocol is set to icmp, the port number range is -1/-1, indicating that all values are valid. • When IpProtocol is set to gre, the port number range is -1/-1, indicating that all values are valid. • When IpProtocol is set to all, the port number range is -1/-1, indicating that all values are valid.
SourceGroupId	String	No	The ID of the source security group. Either SourceGroupId or SourceCidrIp must be set. If both parameters are set, the system will authorize the source CIDR block specified by the SourceCidrIp parameter by default. If the SourceGroupId parameter is specified, but the SourceCidrIp parameter is not, you must set the NicType parameter to intranet.
SourceGroupOwnerAccount	String	No	Optional. The Apsara Stack tenant account of the source security group when you grant security group permissions across users. If neither this parameter nor the SourceGroupOwnerID parameter is specified, the authorization policy will be applied to the security groups of the same account by default. If the SourceCidrIp parameter is specified, the SourceGroupOwnerAccount parameter will be ignored.

Name	Type	Required	Description
SourceGroupOwnerId	String	No	Optional. The Apsara Stack tenant account of the source security group when you grant security group permissions across users. If neither this parameter nor the SourceGroupOwnerAccount parameter is specified, the authorization policy will be applied to the security groups of the same account by default. If the SourceCidrIp parameter is specified, the SourceGroupOwnerId parameter will be ignored.
SourceCidrIp	String	No	The source CIDR block, such as 10.159.6.18/12. Default value: 0.0.0.0/0 (which allows access from any IP addresses). Only IPv4 addresses are supported.
Policy	String	No	The authorization policy. Valid values: • accept: grants access • drop: denies access Default value: accept.
Priority	String	No	The priority of the authorization policy. Valid values: 1 to 100. Default value: 1.
NicType	String	No	The network type. Valid values: • internet • intranet Default value: internet. In mutual security group authorizations where SourceGroupId is specified and SourceCidrIp is not, you must set NicType to intranet.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.
InvalidSecurityGroupId.NotFound	The SecurityGroupId provided does not exist in our records.	404	The error message returned when the specified security group ID does not exist.
OperationDenied	The specified IpProtocol does not exist or IpProtocol and PortRange do not match.	400	The error message returned when the IP protocol does not exist or does not match the specified port.
InvalidIpProtocol.Malformed	The specified parameter PortRange is not valid.	400	The error message returned when the format of the IpProtocol parameter is incorrect.
InvalidPriority.Malformed	The specified parameter Priority is not valid.	400	The error message returned when the format of the Priority parameter is incorrect.
InvalidSourceGroupId.Mismatch	NicType is required or NicType expects intranet.	403	The error message returned when the NicType parameter is not specified or not set to intranet.
InvalidSourceCidrIp.Malformed	The specified parameter SourceCidrIp is not valid.	400	The error message returned when the format of the SourceCidrIp parameter is incorrect.
MissingParameter	The input parameter SourceGroupId or SourceCidrIp cannot both be blank.	403	The error message returned when one of the required SourceGroupId and SourceCidrIp parameters is not specified.
InvalidPolicy.Malformed	The specified parameter Policy is not valid.	400	The error message returned when the format of the Policy parameter is incorrect.

Error code	Error message	HTTP status code	Description
InvalidNicType.ValueNotSupported	The specified image does not exist.	400	The error message returned when the specified NicType parameter is invalid.
InvalidParamter.Conflict	The specified SecurityGroupId should be different from the SourceGroupId.	403	The error message returned when when the values specified for the SecurityGroupId and SourceGroupId parameters are the same.
InvalidSourceGroupId.Mismatch	Specified security group and source group are not in the same VPC.	400	The error message returned when the specified destination security group and source security group do not belong to the same VPC.
InvalidSourceGroupId.NotFound	The SourceGroupId provided does not exist in our records.	404	The error message returned when the specified source group ID does not exist.
InvalidNicType.Mismatch	Specified nic type conflicts with the authorization record.	400	The error message returned when the specified network type does not match the security group rule.
AuthorizationLimitExceed	The limit of authorization records in the security group reaches.	403	The error message returned when the maximum number of security group rules has been reached.
InvalidSourceGroup.NotFound	Specified source security group does not exist.	400	The error message returned when the specified source security group does not exist.
InvalidPriority.ValueNotSupported	The specified Priority is invalid.	400	The error message returned when the Priority parameter is invalid.

Error code	Error message	HTTP status code	Description
InvalidNetworkType.Mismatch	The specified SecurityGroup network type should be same with SourceGroup network type (vpc or classic).	403	The error message returned when the network types of the two security groups in the security group rules are different.

Examples

Sample requests

- Grant access permissions to other security groups

```
https://ecs.example.com/?Action=AuthorizeSecurityGroup
&SecurityGroupId=sg-F876FF7BA
&SourceGroupId=sg-1651FBB64
&SourceGroupOwnerAccount=test@aliyun.com
&IpProtocol=tcp
&PortRange=1/65535
&Common request parameters
```

- Grant access permissions to a specified range of IP addresses

```
https://ecs.example.com/?Action=AuthorizeSecurityGroup
&SecurityGroupId=sg-F876FF7BA
&SourceCidrIp=0.0.0.0/0
&IpProtocol=tcp
&PortRange=1/65535
&Common request parameters
```

Sample responses

XML format

```
<AuthorizeSecurityGroupResponse>
  <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</AuthorizeSecurityGroupResponse>
```

JSON format

```
{
  "RequestId":"CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.1.1.11.3. AuthorizeSecurityGroupEgress

You can call this operation to set the outbound access permissions of a security group.

When you call this operation, note that:

- You can set the authorization policy to the following values: accept, to grant access, or drop, to deny access.
- Internet and intranet networks are supported and can be controlled by setting the NicType parameter.
- A maximum of 100 authorization rules can be configured for one security group.
- The security group priorities are sorted by creation time in descending order.
- Cross-group authorization can only be performed for intranets. For these cases, you must set NicType to intranet.
- The rule priority ranges from 1 to 100. The default value is 1, which is the highest priority. A greater value indicates a lower priority.
- When the priorities of two or more authorization rules are the same, drop rules will take precedence over accept rule.
- A security group rule is defined by one of the following parameter sets: set 1 (DestGroupOwnerAccount, DestGroupId, IpProtocol, PortRange, NicType, and Policy) and set 2 (DestCidrIp, IpProtocol, PortRange, NicType, and Policy). An error will be returned if the rule being created matches an existing rule.
- Two authorization methods are supported:
  - Grant access permissions to other security groups in the same region. Cross-user authorization is allowed.
  - Grant access permissions to a specified range of IP addresses (CIDR block).

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AuthorizeSecurityGroupEgress.
SecurityGroupId	String	Yes	The ID of the source security group.
RegionId	String	Yes	The ID of the region to which the source security group belongs.
IpProtocol	String	Yes	The IP protocol. Valid values: tcp | udp | icmp | gre | all. The value all indicates that all four protocols are supported.

Name	Type	Required	Description
PortRange	String	Yes	The range of port numbers corresponding to the IP protocol. • When IpProtocol is set to tcp or udp, the default port numbers are used, and the port number range is 1 to 65,535. For example, 1/200 indicates that the port number range is 1 to 200. If 200/1 is specified, the operation will return an error. • When IpProtocol is set to icmp, the port number range is -1/-1, indicating any values. • When IpProtocol is set to gre, the port number range is -1/-1, indicating any values. • When IpProtocol is set to all, the port number range is -1/-1, indicating any values.
DestGroupId	String	No	If more than one security group from the same region is authorized, the DestGroupId or DestCidrIp parameter must be set. If both parameters are set, the system will authorize the destination CIDR block specified by the DestCidrIp parameter by default. If the DestGroupId parameter is specified, but the DestCidrIp parameter is not, you must set the NicType parameter to intranet.
DestGroupOwnerAccount	String	No	Optional. The Apsara Stack tenant account of the destination security group when you grant security group permissions across users. If this parameter is not specified, authorization is performed for security groups of the same account by default. If the DestCidrIp parameter is specified, the DestGroupOwnerAccount parameter will be ignored.
DestGroupOwnerId	String	No	Optional. The Apsara Stack tenant account of the destination security group when you grant security group permissions across users. If both this parameter and the DestGroupOwnerAccount parameter are not specified, authorization is performed for security groups of the same account by default. If the DestCidrIp parameter is specified, the DestGroupOwnerId parameter will be ignored.
DestCidrIp	String	No	The destination CIDR block, such as 10.159.6.18/12. Default value: 0.0.0.0/0 (which allows access from any IP addresses). Only IPv4 addresses are supported.
Policy	String	No	The authorization policy to be added. Valid values: • accept: grants access • drop: denies access Default value: accept.

Name	Type	Required	Description
Priority	String	No	The priority of the authorization policy. Valid values: 1 to 100. Default value: 1.
NicType	String	No	The network type to be given to the policy. Valid values: • internet • intranet Default value: internet. In mutual security group authorization where DestGroupId is specified while DestCidrIp is not, you must set NicType to intranet.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.
InvalidSecurity-GroupId.NotFound	The SecurityGroupId provided does not exist in our records.	404	The error message returned when the specified security group ID does not exist.
OperationDenied	The specified IpProtocol does not exist or IpProtocol and PortRange do not match.	400	The error message returned when the IP protocol does not exist or when the IP protocol does not match the port.
InvalidIpProtocol.Malformed	The specified parameter PortRange is not valid.	400	The error message returned when the format of the IpProtocol parameter is incorrect.

Error code	Error message	HTTP status code	Description
InvalidPriority.Malformed	The specified parameter Priority is not valid.	400	The error message returned when the format of the Priority parameter is incorrect.
InvalidDestCidrIp.Malformed	The specified parameter DestCidrIp is not valid.	400	The error message returned when the format of the DestCidrIp parameter is incorrect.
MissingParameter	The input parameter DestGroupId or DestCidrIp cannot be both blank.	403	The error message returned when either the DestGroupId or DestCidrIp parameter is not specified.
InvalidPolicy.Malformed	The specified parameter Policy is not valid.	400	The error message returned when the format of the Policy parameter is incorrect.
InvalidNicType.Value-NotSupported	The specified NicType does not exist.	400	The error message returned when the specified NicType parameter is invalid.
InvalidDestGroupId.Mismatch	Specified security group and destination group are not in the same VPC.	400	The error message returned when the destination security group does not belong to the same VPC as the specified source security group.
InvalidDestGroupId.NotFound	The DestGroupId provided does not exist in our records.	404	The error message returned when the specified destination group ID does not exist.

Error code	Error message	HTTP status code	Description
InvalidDestGroupId.Mismatch	NicType is required or NicType expects intranet.	403	The error message returned when the NicType is not set to intranet.
InvalidNicType.Mismatch	Specified nic type conflicts with the authorization record.	400	The error message returned when the specified network type does not match the security group rule.
AuthorizationLimitExceed	The limit of authorization records in the security group reaches.	403	The error message returned when the number of security group rules has reached the upper limit.
InvalidParamter.Conflict	The specified SecurityGroupId should be different from the SourceGroupId.	403	The error message returned when the SecurityGroupId and SourceGroupId values are the same.
InvalidDestGroup.NotFound	Specified destination security group does not exist.	400	The error message returned when the specified destination security group does not exist.
InvalidPriority.ValueNotSupported	The specified priority is illegal.	400	The error message returned when the Priority parameter is invalid.
InvalidDestCidrIp.Malformed	The specified parameter DestCidrIp is not valid.	400	The error message returned when the format of the DestCidrIp parameter is incorrect.

Error code	Error message	HTTP status code	Description
InvalidNetworkType.Conflict	The specified SecurityGroup network type should be same with SourceGroup network type (vpc or classic).	403	The error message returned when the network types of the two security groups specified in the security group rules are different.
InvalidSecurityGroup.IsSame	The authorized SecurityGroupId should be different from the DestGroupId.	403	The error message returned when the SecurityGroupId and DestGroupId values are the same.

Examples

- **Sample requests**

  Configure access permissions for other security groups

  ```
  https://ecs.example.com/?Action=RevokeSecurityGroupEgress
  &SecurityGroupId=sg-94n63e80l
  &IpProtocol=all
  &DestGroupId=sg-94oi1r1bp
  &IpProtocol=tcp
  &PortRange=1/65535
  &Common request parameters
  ```

  - **Grant access permissions to a specified range of IP addresses**

    ```
    https://ecs.example.com/?Action=RevokeSecurityGroupEgress
    &SecurityGroupId=sg-94n63e80l
    &IpProtocol=all
    &DestCidrIp=10.0.0.0/8
    &IpProtocol=tcp
    &PortRange=1/65535
    &Common request parameters
    ```

- **Sample responses**

  XML format

```
<RevokeSecurityGroupEgressResponse>
    <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</RevokeSecurityGroupEgressResponse>
```

JSON format

```
<RevokeSecurityGroupEgressResponse>
    <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</RevokeSecurityGroupEgressResponse>
```

2.1.1.11.4. RevokeSecurityGroup

You can call this operation to lift security group rules.

You can use either of the following methods to revoke access permissions on a security group:

- Lift the security group rules that allow other security groups within a VPC to access the security group through a specific protocol and port.
- Lift the security group rules that allow access to the security group from a specific IP network segment through a specific protocol and port. Only the permission entries that were authorized by calling the AuthorizeSecurityGroupEgress operation can be deleted.

A security group rule is defined by one of the following parameter sets: set 1 (SourceGroupOwnerAccount, SourceGroupId, IpProtocol, PortRange, NicType, and Policy) and set 2 (SourceCidrIp. IpProtocol. PortRange, NicType, Policy). An error will be returned if no matching rules are found.

Both RevokeSecurityGroup and RevokeSecurityGroupEgress are used to operate security group rules, but they have differences:

- RevokeSecurityGroup is used to lift the security group rules in the inbound direction.
- RevokeSecurityGroupEgress is used to lift the security group rules in the outbound direction.

RevokeSecurityGroup is used more often. You can select either operation as required.

AuthorizeSecurityGroup is used to specify rules in the inbound direction, and AuthorizeSecurityGroupEgress is used to specify rules in the outbound direction.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RevokeSecurityGroup.
SecurityGroupId	String	Yes	The ID of the destination security group.
RegionId	String	Yes	The ID of the region to which the destination security group belongs.

Name	Type	Required	Description
IpProtocol	String	Yes	The IP protocol. Valid values: tcp | udp | icmp | gre | all. The value all indicates that all four protocols are supported.
PortRange	String	Yes	The range of port numbers corresponding to the IP protocol. • When IpProtocol is set to tcp or udp, the default port numbers are used, and the port number range is 1 to 65,535. For example, 1/200 indicates that the port number range is 1 to 200. If 200/1 is specified, the operation will return an error. • When IpProtocol is set to icmp, the port number range is -1/-1, indicating any values. • When IpProtocol is set to gre, the port number range is -1/-1, indicating any values. • When IpProtocol is set to all, the port number range is -1/-1, indicating any values.
SourceGroupId	String	No	The ID of the source security group. The SourceGroupId or SourceCidrIp parameter must be set. If both parameters are set, the system will authorize the source CIDR block specified by the SourceCidrIp parameter by default. You can specify up to 10 security groups separated with commas (,).
SourceGroupOwnerAccount	String	No	Optional. The Apsara Stack tenant account of the source security group when you lift security group rules from different tenant accounts. If this parameter is not specified, the rules between security groups of the same account are lifted by default. If the SourceCidrIp parameter is specified, the SourceGroupOwnerAccount parameter will be ignored.
SourceCidrIp	String	No	The source CIDR block, such as 10.159.6.18/12. Default value: 0.0.0.0/0 (which allows access from any IP addresses). Only IPv4 addresses are supported.
Policy	String	No	The authorization policy. Valid values: • accept: grants access • drop: denies access Default value: accept.

Name	Type	Required	Description
NicType	String	No	The network type. Valid values: • internet • intranet Default value: internet. In mutual security group authorization where SourceGroupId is specified, while SourceCidrIp is not, you must set NicType to intranet.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required RegionId parameter is not specified.
InvalidSecurityGroupId.NotFound	The SecurityGroupId provided does not exist in our records.	404	The error message returned when the specified security group ID does not exist.
MissingParameter	The input parameter SecurityGroupId that is mandatory for processing this request is not supplied.	400	The error message returned when the required SecurityGroupId parameter is not specified.
InvalidIpProtocol.ValueNotSupported	The specified IpProtocol does not exist.	400	The error message returned when the specified IpProtocol parameter is invalid.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter IpProtocol that is mandatory for processing this request is not supplied.	400	The error message returned when the required IpProtocol parameter is not specified.
InvalidIpPortRange.Malformed	The specified parameter PortRange is not valid.	400	The error message returned when the format of PortRange is incorrect.
MissingParameter	The input parameter PortRange that is mandatory for processing this request is not supplied.	400	The error message returned when the required PortRange parameter is not specified.
InvalidSourceGroupId.NotFound	The SourceGroupId provided does not exist in our records.	404	The error message returned when the specified source group ID does not exist.
InvalidSourceGroupId.Mismatch	NicType is required or NicType expects intrnet.	403	The error message returned when the NicType parameter is not specified or set to intranet.
InvalidSourceCidrIp.Malformed	The specified parameter SourceCidrIp is not valid.	400	The error message returned when the format of the SourceCidrIp parameter is incorrect.
MissingParameter	The input parameter SourceGroupId or SourceCidrIp cannot be both blank.	400	The error message returned when either the SourceGroupId or SourceCidrIp parameter is not specified.
InvalidPolicy.Malformed	The specified parameter Policy is not valid.	400	The error message returned when the format of the Policy parameter is incorrect.
InvalidNicType.ValueNotSupported	The specified NicType does not exist.	400	The error message returned when the specified NicType parameter is invalid.

Error code	Error message	HTTP status code	Description
InvalidSourceGroupId.Mismatch	SourceGroupOwnerAccount is required	403	The error message returned when the SourceGroup parameter is specified, but the SourceGroupOwnerUserAccount parameter is not.
InvalidSourceGroupOwnerUserAccount.Mismatch	The specified SourceGroupId is not belong to the SourceGroupOwnerAccount	403	The error message returned when the specified source group does not belong to the user specified in the SourceGroupOwnerUserAccount parameter.

Examples

Sample requests

```
https://ecs.example.com/?Action=RevokeSecurityGroup
&SecurityGroupId=C0003E8B-B930-4F59-ADC0-0E209A9012B0
&SourceGroupId=sg-F876FF7BA
&SourceGroupOwnerAccount=test@aliyun.com
&IpProtocol=tcp
&PortRange=1/65535
&Common request parameters
```

Sample responses

XML format

```
<RevokeSecurityGroupResponse>
    <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</RevokeSecurityGroupResponse>
```

JSON format

```
{
   "RequestId":"CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.1.1.11.5. RevokeSecurityGroupEgress

You can call this operation to lift the security group rules on outbound traffic.

To lift the rules, you can use one of the following methods:

- In a VPC, you can specify the protocol and port to access other security groups.
- You can specify the protocol and port to access an IP address range. Only the permissions that were granted by calling the AuthorizeSecurityGroupEgress operation can be deleted. The parameter values used for deletion must be the same as those used for authorization.

Description

A security group rule is defined by one of the following parameter sets: set 1 (DestGroupOwnerAccount, DestGroupId, IpProtocol, PortRange, NicType, and Policy) and set 2 (DestCidrIp, IpProtocol, PortRange, NicType, and Policy). An error will be returned if no matching rules are found.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RevokeSecurityGroupEgress.
SecurityGroupId	String	Yes	The ID of the source security group.
RegionId	String	Yes	The ID of the region to which the source security group belongs.
IpProtocol	String	Yes	The IP protocol used by the security group. Valid values: tcp | udp | icmp | gre | all. The value all indicates the support of all the four protocols.
PortRange	String	Yes	The range of port numbers corresponding to the IP protocol. • When IpProtocol is set to tcp or udp, the default port numbers are used, and the port number range is 1 to 65,535. For example, 1/200 indicates that the port number range is 1 to 200. If 200/1 is specified, the operation will return an error. • When IpProtocol is set to icmp, the port number range is -1/-1, indicating any values. • When IpProtocol is set to gre, the port number range is -1/-1, indicating any values. • When IpProtocol is set to all, the port number range is -1/-1, indicating any values.

Name	Type	Required	Description
DestGroupId	String	No	If more than one security group from the same region is authorized, the SourceGroupId or SourceCidrIp parameters must be set. If both parameters are set, the system will authorize the source CIDR block specified by the SourceCidrIp parameter by default. You can specify up to 10 security groups separated with commas (,).
DestGroupOwnerAccount	String	No	Optional. The Apsara Stack tenant account that owns the security group rules that you want to lift. If this parameter is not specified, the rules between security groups of the same account are lifted by default. If the DestCidrIp parameter is specified, the DestGroupOwnerAccount parameter will be ignored.
DestCidrIp	String	No	The destination CIDR block, such as 10.159.6.18/12. Default value: 0.0.0.0/0 (which allows access from any IP addresses). Only IPv4 addresses are supported.
Policy	String	No	The authorization policy. Valid values: • accept: grants access • drop: denies access Default value: accept.
NicType	String	No	The network type. Valid values: • internet • intranet Default value: internet. In mutual security group authorization (DestGroupId is specified, while DestCidrIp is not), you must set NicType to intranet.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Description	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required RegionId parameter is not specified.
InvalidSecurityGroupId.NotFound	The SecurityGroupId provided does not exist in our records.	404	The error message returned when the specified security group ID does not exist.
MissingParameter	The input parameter SecurityGroupId that is mandatory for processing this request is not supplied.	400	The error message returned when the required SecurityGroupId parameter is not specified.
InvalidIpProtocol.ValueNotSupported	The specified IpProtocol does not exist.	400	The error message returned when the specified IP protocol is not supported.
MissingParameter	The input parameter IpProtocol that is mandatory for processing this request is not supplied.	400	The error message returned when the required IpProtocol parameter is not specified.
InvalidIpPortRange.Malformed	The specified parameter PortRange is not valid.	400	The error message returned when the format of PortRange is incorrect.
MissingParameter	The input parameter PortRange that is mandatory for processing this request is not supplied.	400	The error message returned when the required PortRange parameter is not specified.
InvalidDestGroupId.NotFound	The DestGroupId provided does not exist in our records.	404	The error message returned when the specified DestGroupId parameter does not exist.

Error code	Description	HTTP status code	Description
InvalidDestGroupId.Mismatch	NicType is required or NicType expects intrnet.	403	The error message returned when the NicType parameter is not specified or not set to intranet.
InvalidDestCidrIp.Malformed	The specified parameter DestCidrIp is not valid.	400	The error message returned when the format of the DestCidrIp parameter is incorrect.
MissingParameter	The input parameter DestGroupId or DestCidrIp cannot be both blank.	400	The error message returned when either the DestGroupId or DestCidrIp parameter is not specified.
InvalidPolicy.Malformed	The specified parameter Policy is not valid.	400	The error message returned when the format of the Policy parameter is incorrect.
InvalidNicType.ValueNotSupported	The specified NicType does not exist.	400	The error message returned when the specified NicType parameter is invalid.
InvalidDestGroupId.Mismatch	DestGroupOwnerAccount is required	403	The error message returned when the DestGroup parameter is specified, but the DestGroupOwnerUserAccount parameter is not.
InvalidDestGroupOwnerUserAccount.Mismatch	The specified DestGroupId is not belong to the DestGroupOwnerAccount	403	The error message returned when the specified destination group does not belong to the user specified in the DestGroupOwnerUserAccount parameter.

Examples

- Sample requests

  Authorize access permissions on other security groups

```
https://ecs.example.com/?Action=RevokeSecurityGroupEgress
&SecurityGroupId=sg-94n63e80l
&IpProtocol=all
&DestGroupId=sg-94oi1r1bp
&IpProtocol=tcp
&PortRange=1/65535
&Common request parameters
```

Grant access permissions to a specified range of IP addresses

```
https://ecs.example.com/?Action=RevokeSecurityGroupEgress
&SecurityGroupId=sg-94n63e80l
&IpProtocol=all
&DestCidrIp=10.0.0.0/8
&IpProtocol=tcp
&PortRange=1/65535
&Common request parameters
```

- Sample responses

  XML format

```
<RevokeSecurityGroupEgressResponse>
    <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</RevokeSecurityGroupEgressResponse>
```

  JSON format

```
{
   "RequestId":"CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.1.1.11.6. JoinSecurityGroup

You can call this operation to add an instance to a security group.

When you call this operation, note that:

- The instance to be added must be in the Stopped or Running state.
- An instance can be added to a maximum of five security groups.
- A security group can manage up to 1,000 instances.
- The specified security group and instance must belong to the same region.
- The specified security group and instance must belong to the same VPC.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to JoinSecurityGroup.
InstanceId	String	Yes	The ID of the instance. You can call DescribeInstances to view available instances.
SecurityGroupId	String	Yes	The ID of the security group. You can call DescribeSecurityGroups to view available security groups.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=JoinSecurityGroup
&InstanceId= i-instance1
&SecurityGroupId=F876FF7BA984
&<Common request parameters>
```

Sample responses

XML format

```
<JoinSecurityGroupResponse>
<RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId> </JoinSecurityGroupResponse>
```

JSON format

```
{
"RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

Error codes

Error code	Error message	HTTP status code	Description
InvalidInstanceId.Mismatch	Specified instance and security group are not in the same VPC.	400	The error message returned when the specified security group and instance do not belong to the same VPC.
InstanceSecurityGroupLimitExceeded	Exceeding the allowed amount of security groups that an instance can be in.	400	The error message returned when the specified instance would belong to over five security groups.
MissingParameter	The input parameter InstanceId that is mandatory for processing this request is not supplied.	400	The error message returned when the required InstanceId parameter is not specified.
MissingParameter	The input parameter SecurityGroupId that is mandatory for processing this request is not supplied.	400	The error message returned when the required SecurityGroupId parameter is not specified.
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the specified instance is not in the Stopped or Running state.
InstanceLockedForSecurity	The specified operation is denied as your instance is locked for security reasons.	403	The error message returned when the specified instance is locked for security reasons and the operation cannot be completed.
SecurityGroupInstanceLimitExceeded	The maximum number of instances in a security group is exceeded.	403	The error message returned when the number of instances in a security group exceeds 1,000.
InvalidInstanceId.AlreadyExists	The specified instance already exists in the specified security group.	403	The error message returned when the specified security group already contains the specified instance.

Error code	Error message	HTTP status code	Description
OperationDenied	The specified operation is denied as your instance is locked for security reasons.	403	The error message returned when the specified instance is locked for security reasons and the operation cannot be completed.
InvalidInstanceId.NotFound	The specified InstanceId does not exist.	404	The error message returned when the specified instance ID does not exist.
InvalidSecurityGroupId.NotFound	The specified SecurityGroupId does not exist.	404	The error message returned when the specified security group ID does not exist.

2.1.1.11.7. LeaveSecurityGroup

You can call this operation to remove an instance from a security group.

When you call this operation, note that:

- The instance to be removed must be in the Stopped or Running state.
- An instance must belong to at least one security group. If the instance to be removed only belongs to a single security group, the LeaveSecurityGroup request fails.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to LeaveSecurityGroup.
InstanceId	String	Yes	The ID of the instance to be removed.
SecurityGroupId	String	Yes	The ID of the security group.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=LeaveSecurityGroup
&InstanceId=i-instance1
&SecurityGroupId=F876FF7BA984
&<Common request parameters>
```

Sample responses

XML format

```
<LeaveSecurityGroupResponse>
<RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</LeaveSecurityGroupResponse>
```

JSON format

```
{
"RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
```

Error codes

Error code	Error message	HTTP status code	Description
IncorrectInstanceStatus	The current status of the resource does not support this operation.	403	The error message returned when the specified instance is not in the Stopped or Running state.
InstanceLastSecurityGroup	The specified security group is the last security group for the instance.	403	The error message returned when you try to remove the only security group of an instance. Each instance must belong to at least one security group.
InstanceLockedForSecurity	The specified operation is denied as your instance is locked for security reasons.	403	The error message returned when the instance is locked for security reasons (OperationLocks is set to "LockReason" : "security").
InstanceNotInSecurityGroup	The instance not in the group.	403	The error message returned when the instance is not in the specified security group.

Error code	Error message	HTTP status code	Description
InvalidInstanceId.NotFound	The specified InstanceId does not exist.	404	The error message returned when the specified instance ID does not exist.
InvalidSecurityGroupId.NotFound	The specified SecurityGroupId does not exist.	404	The error message returned when the specified security group ID does not exist.

2.1.1.11.8. DeleteSecurityGroup

You can call this operation to delete a security group.

When you call this operation, note that:

A security group can be deleted only when it contains no instances or when it is not referenced by the security rules of any other groups.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteSecurityGroup.
SecurityGroupId	String	Yes	The ID of the security group to be deleted.
RegionId	String	Yes	The ID of the region to which the security group belongs.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist or when you are not authorized to access the region.

Error code	Error message	HTTP status code	Description
DependencyViolation	There is still instance(s) in the specified security group.	403	The error message returned when the specified security group still contains instances.
DependencyViolation	The specified security group has been authorized in another one.	403	The error message returned when the specified security group is referenced by another security group.
DependencyViolation	The specified security group has been authorized in another one of another user account	403	The error message returned when the specified security group is referenced by a security group of another user.

Examples

Sample requests

```
https://ecs.example.com/?Action=DeleteSecurityGroup
&SecurityGroupId=sg-F876FF7BA
&amp;RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

XML format

```
<RevokeSecurityGroupResponse>
    <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</RevokeSecurityGroupResponse>
```

JSON format

```
{
   "RequestId":"CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.1.1.11.9. DescribeSecurityGroupAttribute

You can call this operation to query details about a security group, including its permission rules.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSecurityGroupAttribute.
SecurityGroupId	String	Yes	The ID of the destination security group.
RegionId	String	Yes	The ID of the region to which the destination security group belongs.
NicType	String	No	The network type of the destination security group. Valid values: internet | intranet. Default value: internet.
Direction	String	No	The allowed direction of traffic for the security group to be queried. Valid values: egress | ingress | all. Default value: all.

Response parameters

Response parameter description

Name	Type	Required
SecurityGroupId	String	The ID of the destination security group.
SecurityGroupName	String	The name of the destination security group.
RegionId	String	The ID of the region to which the security group belongs.
Description	String	The description of the security group.
Permissions	PermissionType	A set of PermissionType data indicating the permission rules of the security group.
VpcId	String	The VPC ID. This parameter is only specified if the security group belongs to a VPC.

Error codes

Error code description

Error code	Error message	HTTP status code	Description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist or when you do not have permission to use it.
InvalidSecurityGroupId.NotFound	The SecurityGroupId provided does not exist in our records.	404	The error message returned when the specified security group ID does not exist.
InvalidNicType.ValueNotSupported	The specified NicType does not exist.	400	The error message returned when the specified NicType parameter is invalid.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeSecurityGroupAttribute
&SecurityGroupId=sg-F876FF7BA
&amp;RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

XML format

```
<DescribeSecurityGroupAttributeResponse>
    <RequestId>1651FBB6-4FBF-49FF-A9F5-DF5D696C7EC6</RequestId>
    <RegionId>cn-hangzhou</RegionId>
    <SecurityGroupId>C0003E8B-B930-4F59-ADC0-0E209A9012B0</SecurityGroupId>
    <Description>for demo</Description>
      <Permissions>
       <Permission>
          <IpProtocol>ALL</IpProtocol>
          <PortRange>-1/-1</PortRange>
<SourceGroupId>8dsmf982</SourceGroupId>
<SourceGroupOwnerAccount>test@aliyun.com</SourceGroupOwnerAccount>
          <Policy>Accept</Policy>
          <NicType>intranet</NicType>
       </Permission>
        <Permission>
          <IpProtocol>tcp</IpProtocol>
          <PortRange>1/65535</PortRange>
          <SourceCidrIp>0.0.0.0/0</SourceCidrIp>
          <Policy>accept</Policy>
          <NicType>internet</NicType>
       </Permission>
    </Permissions>
</DescribeSecurityGroupAttributeResponse>
```

JSON format

```
{
   "RequestId": "1651FBB6-4FBF-49FF-A9F5-DF5D696C7EC6",
   "RegionId": "cn-hangzhou",
   "SecurityGroupId": "C0003E8B-B930-4F59-ADC0-0E209A9012B0",
   "Description": "for demo",
   "Permissions": {
      "Permission": [{
         "IpProtocol": "ALL",
         "PortRange": "-1/-1",
"SourceGroupId": "8dsmf982",
"SourceGroupOwnerAccount": "test@aliyun.com"
         "Policy": "Accept",
         "NicType": "intranet"
      },
      {
         "IpProtocol": "tcp",
         "PortRange": "1/65535",
         "SourceCidrIp": "0.0.0.0/0",
         "Policy": "accept",
         "NicType": "internet"
      }]
   }
}
```


2.1.1.11.10. DescribeSecurityGroups

You can call this operation to query the basic information about all user-defined security groups.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSecurityGroups.
RegionId	String	Yes	The ID of the region to which the security group belongs.
VpcId	String	No	The ID of the VPC to which the security group belongs.
Tag.n.Key	String	No	The key of the tag. The value of n ranges from 1 to 5. It cannot be a null string.

Name	Type	Required	Description
Tag.n.Value	String	No	The value of the tag. The value of n ranges from 1 to 5. It can be a null string.
PageNumber	Integer	No	The current page number. Starting value: 1. Default value: 1.
PageSize	Integer	No	The number of entries per page. Maximum value: 50. Default value: 10.

Response parameters

Response parameter description

Name	Type	Description
TotalCount	Integer	The total number of security groups.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of entries per page.
RegionId	String	The ID of the region to which the security group belongs.
SecurityGroups	SecurityGroupItemType	The security group information consisting of SecurityGroupItemType data.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeSecurityGroups
&amp;RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

XML format

```
<DescribeSecurityGroupsResponse>
    <RequestId>94D38899-626D-434A-891F-7E1F77A81525</RequestId>
    <TotalCount>4</TotalCount>
    <PageNumber>1</PageNumber>
    <PageSize>10</PageSize>
    <RegionId>cn-hangzhou</RegionId>
    <SecurityGroups>
        <SecurityGroup>
            <SecurityGroupId>sg-F876FF7BA</SecurityGroupId>
            <Description>Test</Description>
        </SecurityGroup>
        <SecurityGroup>
            <SecurityGroupId>sg-086FFC27A</SecurityGroupId>
            <Description>test00212</Description>
        </SecurityGroup>
        <SecurityGroup>
            <SecurityGroupId>sg-BA4B7975B</SecurityGroupId>
            <Description>cn-hangzhou test group</Description>
        </SecurityGroup>
        <SecurityGroup>
            <SecurityGroupId>sg-35F20777C</SecurityGroupId>
            <Description>cn-hangzhou test group</Description>
        </SecurityGroup>
    </SecurityGroups>
</DescribeSecurityGroupsResponse>
```

JSON format

```
{
  "RequestId": "94D38899-626D-434A-891F-7E1F77A81525",
  "TotalCount": 4,
  "PageSize": "10",
  "RegionId": "cn-hangzhou",
  "PageNumber": "1",
  "SecurityGroups": {
    "SecurityGroup": [{
      "SecurityGroupId": "sg-F876FF7BA",
      "Description": "TestByXcf"
    },
    {
      "SecurityGroupId": "sg-086FFC27A",
      "Description": "test00212"
    },
    {
      "SecurityGroupId": "sg-BA4B7975B",
      "Description": "cn-hangzhou test group"
    },
    {
      "SecurityGroupId": "sg-35F20777C",
      "Description": "cn-hangzhou test group"
    }]
  }
}
```


2.1.1.11.11. DescribeSecurityGroupReferences

You can call this operation to query whether a security group is referenced by other security groups.

When you call this operation, note that:

- Security group authorization includes authorization for inbound and outbound traffic rules.
- A maximum of 100 authorization entries can be queried per call.
- When a security group failed to be deleted, you can call this operation to check whether the security group is authorized by another security group. If the security group to be deleted is authorized by another security group, you must revoke its autothorization before it can be deleted.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSecurityGroupReferences.
SecurityGroupId.n	String	Yes	The ID of the security group that you want to query. Value range of n: [1, 10].
RegionId	String	Yes	The ID of the region to which the security group belongs. You can call DescribeRegions to view available regions.

Response parameters

Name	Type	Description
SecurityGroupReferences	SecurityGroupReference	The information about references between security groups.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeSecurityGroupReferences
&RegionId=cn-hangzhou
&SecurityGroupId. 1=sg-1133aa
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeSecurityGroupReferencesResponse>
<RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
<SecurityGroupReferences>
<SecurityGroupReference>
<SecurityGroupId>sg-1133aa</SecurityGroupId>
<ReferencingSecurityGroups>
<ReferencingSecurityGroup>
<SecurityGroupId>sg-2255cc</SecurityGroupId>
<AliUid>123</AliUid>
</ReferencingSecurityGroup>
<ReferencingSecurityGroup>
<SecurityGroupId>sg-2255dd</SecurityGroupId>
<AliUid>123</AliUid>
</ReferencingSecurityGroup>
</ReferencingSecurityGroups>
</SecurityGroupReference>
</SecurityGroupReferences>
</DescribeSecurityGroupReferencesResponse>
```

JSON format

```
{
"RequestId": "CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
"SecurityGroupReferences":[
{
"SecurityGroupId":"sg-1133aa",
"SecurityReferencingGroups":[
{
"AliUid":123,
"SecurityGroupId":"sg-2255cc"
},
{
"AliUid":123,
"SecurityGroupId":"sg-2255dd"
}
]
}
]
}
```

Error codes

Error code	Error message	HTTP status code	Description
Abs.GroupNos.Malformed	The specified parameter SecurityGroupId is essential and size should less than 10.	400	The error message returned when the SecurityGroupId.n is not specified or when the value of n is greater than 10.
InvalidSecurityGroupId.NotFound	The specified SecurityGroupId does not exist.	400	The error message returned when the specified security group ID does not exist.
InvalidRegionId.NotFound	The specified RegionId does not exist.	404	The error message returned when the specified region ID does not exist.

2.1.1.11.12. ModifySecurityGroupAttribute

You can call this operation to modify attributes of a security such as its name and description.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifySecurityGroupAttribute.
RegionId	String	Yes	The ID of the region to which the security group belongs.
SecurityGroupId	String	Yes	The ID of the security group.
SecurityGroupName	String	No	The name of the security group. If not specified, this parameter is null. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It is displayed in Apsara Stack console. It cannot start with `http://` or `https://`.
Description	String	No	The description of the security group. The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified RegionId parameter does not exist.
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required RegionId parameter is not specified.
MissingParameter	The input parameter SecurityGroupId that is mandatory for processing this request is not supplied.	400	The error message returned when the required SecurityGroupId parameter is not specified.
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist or when you are not authorized to access the region.
InvalidSecurityGroupName.Malformed	Specified security group name is not valid.	400	The error message returned when the format of the SecurityGroupName parameter is invalid.
InvalidDescription.Malformed	The specified parameter Description is not valid.	400	The error message returned when the format of the DescriptionName parameter is invalid.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifySecurityGroupAttribute
&SecurityGroupId=sg-F876FF7BA
&RegionId=cn-hangzhou
&SecurityGroupName=NewName
&Common request parameters
```

Sample responses

XML format

```
<ModifySecurityGroupAttributeResponse>
    <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</ModifySecurityGroupAttributeResponse>
```

JSON format

```
{
  "RequestId":"CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.1.1.11.13. ModifySecurityGroupPolicy

You can call this operation to modify the intranet communication policy of a security group.

When you call this operation, note that:

- When the value of the InnerAccessPolicy parameter is Accept, all instances within the security group are accessible from each other. The Accept policy has the highest priority of all rules, and other user-defined security group rules are ignored.
- When the value of the InnerAccessPolicy parameter is Drop, all instances within the security group are isolated from each other. In this case, user-defined security group rules have a higher priority and can be used to change the intranet access policy. For example, you can call AuthorizeSecurityGroup to enable two ECS instances in the security group to access each other.
- You can call DescribeSecurityGroupAttribute to query the intranet communication policy of the security group.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifySecurityGroupPolicy.
SecurityGroupId	String	Yes	The ID of the security group.
RegionId	String	Yes	The ID of the region to which the security group belongs. You can call DescribeRegions to view available regions.

Name	Type	Required	Description
InnerAccessPolicy	String	Yes	The intranet communication policy of the security group. Valid values: • Accept: All instances within the security group can communicate with each other. • Drop: All instances within the security group are isolated from each other. The values are case-insensitive.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifySecurityGroupPolicy
&RegionId=cn-hangzhou
&SecurityGroupId=sg-1133aa
&InnerAccessPolicy=Drop
&<Common request parameters>
```

Sample responses

XML format

```
<ModifySecurityGroupPolicyResponse>
<RequestId>CEF72CEB-54B6-4AE8-B225-F876xxxxxxxx</RequestId>
</ModifySecurityGroupPolicyResponse>
```

JSON format

```
{
"RequestId": "CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

Error codes

Error code	Error message	HTTP status code	Description

Error code	Error message	HTTP status code	Description
InvalidPolicy.Malformed	The InnerAccessPolicy is invalid. Only Accept and Drop are supported.	400	The error message returned when the InnerAccessPolicy parameter is not specified or is invalid.
InvalidSecurityGroupId.Malformed	The SecurityGroupId is invalid. Only letters, numbers and underscores are supported. The maximum length of this parameter is 100 characters.	400	The error message returned when the SecurityGroupId parameter is not specified or is invalid.
InvalidRegionId.NotFound	The RegionId provided does not exist.	404	The error message returned when the specified RegionId parameter does not exist.

2.1.1.11.14. ModifySecurityGroupRule

You can call this operation to modify the inbound rules of a security group.

You can call AuthorizeSecurityGroup to add a security group rule. You can determine an inbound rule by specifying one of the following groups of parameters. You cannot determine a security group rule by specifying only one parameter.

- Grant access permissions to a specified range of IP addresses: IpProtocol, PortRange, SourcePortRange (optional), NicType, Policy, DestCiderIp and SourceCidrIp (optional).
- Grant access permissions to other security groups: IpProtocol, PortRange, SourcePortRange (optional), NicType, Policy, DestCiderIp (optional), DestGroupOwnerAccount, and DestGroupId.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifySecurityGroupRule.
RegionId	String	Yes	The ID of the region to which the destination security group belongs. You can call DescribeRegions to view latest regions.
SecurityGroupId	String	Yes	The ID of the security group.
Description	String	Yes	The description of the security group rule. The description must be 1 to 512 characters in length.

Name	Type	Required	Description
IpProtocol	String	Yes	The transport layer protocol. The parameter value is not case-sensitive. Valid values: • ICMP • GRE • TCP • UDP • all: All protocols are supported.
PortRange	String	Yes	The range of destination port numbers relevant to the transport layer protocol. Valid values: • When IpProtocol is set to TCP or UDP, the port number range is 1 to 65535. Separate the starting port and the ending port with a forward slash (/). Correct example: 1/200. Incorrect example: 200/1. • When IpProtocol is set to ICMP, the port number range is -1/-1, indicating that all values are valid. • When IpProtocol is set to GRE, the port number range is -1/-1, indicating that all values are valid. • When IpProtocol is set to all, the port number range is -1/-1, indicating that all values are valid.
SourcePortRange	String	No	The range of source port numbers relevant to the transport layer protocol. Valid values: • When IpProtocol is set to TCP or UDP, the port number range is 1 to 65535. Separate the starting port and the ending port with a forward slash (/). Correct example: 1/200. Incorrect example: 200/1. • When IpProtocol is set to ICMP, the port number range is -1/-1, indicating that all values are valid. When IpProtocol is set to GRE, the port number range is -1/-1, indicating that all values are valid. • When IpProtocol is set to all, the port number range is -1/-1, indicating that all values are valid.

Name	Type	Required	Description
NicType	String	No	The NIC type. Valid values: • internet: Internet NIC • intranet: intranet NIC This parameter must be set to intranet in mutual security group authorizations where the DestGroupId parameter is specified and the DestCidrIp parameter is not. Default value: internet.
Policy	String	No	The access permission. Valid values: • accept: grants access. • drop: denies access and returns no responses. Default value: accept.
DestCidrIp	String	No	The destination IP address range. CIDR blocks and IPv4 addresses are supported. Default value: 0.0.0.0/0.
SourceCidrIp	String	No	The source IP address range. CIDR blocks and IPv4 addresses are supported. Default value: 0.0.0.0/0.
SourceGroupId	String	No	The ID of the source security group to which you want to grant access permissions. Either the SourceGroupId parameter or the SourceCidrIp parameter must be specified. If the SourceGroupId parameter is specified, but the SourceCidrIp parameter is not, the NicType parameter can only be set to intranet. If both the SourceGroupId and SourceCidrIp parameters are set, the SourceCidrIp value takes precedence by default.

Name	Type	Required	Description
SourceGroupOwnerAccount	String	No	The Apsara Stack tenant account of the source security group when you set security group rules for different tenant accounts. If neither the SourceGroupOwnerAccount parameter nor the SourceGroupOwnerID parameter is specified, the access permissions of other security groups are used. If the SourceCidrIp parameter is specified, the SourceGroupOwnerAccount parameter will be ignored.
SourceGroupOwnerId	String	No	The Apsara Stack tenant account ID of the source security group when you set security group rules for different tenant accounts. If neither the SourceGroupOwnerAccount parameter nor the SourceGroupOwnerID parameter is specified, the access permissions of other security groups are used. If the SourceCidrIp parameter is specified, the SourceGroupOwnerId parameter will be ignored.
Priority	String	No	The priority of the security group rule. Valid values: [1, 100]. Default value: 1.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifySecurityGroupRule
&SecurityGroupId=sg-F876FF7BA
&SourceGroupId=sg-1651FBB64
&SourceGroupOwnerAccount=test@aliyun.com
&IpProtocol=tcp
&PortRange=80/80
&Policy=allow
&Description=This is a new security group rule.
&<Common request parameters>
```

Sample responses

XML format

```
<ModifySecurityGroupRuleResponse>
<RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</ModifySecurityGroupRuleResponse>
```

JSON format

```
<ModifySecurityGroupRuleResponse>
<RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</ModifySecurityGroupRuleResponse>
```

Error codes

Error code	Error message	HTTP status code	Description
InvalidIpProtocol.Malformed	The specified parameter IpProtocol is not valid.	400	The error message returned when the specified IpProtocol parameter is invalid.
InvalidNicType.Mismatch	Specified nic type conflicts with the authorization record.	400	The error message returned when the specified NIC type does not match the security group rule.
InvalidNicType.ValueNotSupported	The specified NicType does not exist.	400	The error message returned when the specified NIC type does not exist.

Error code	Error message	HTTP status code	Description
InvalidPolicy.Malformed	The specified parameter Policy is not valid.	400	The error message returned when the specified Policy parameter is invalid.
InvalidPriority.Malformed	The specified parameter Priority is not valid.	400	The error message returned when the specified Priority parameter is invalid.
InvalidPriority.ValueNotSupported	The specified Priority is invalid.	400	The error message returned when the specified Priority parameter is invalid.
InvalidSecurityGroupDiscription.Malformed	The specified security group rule description is not valid.	400	The error message returned when the specified Description parameter is invalid.
InvalidSourceCidrIp.Malformed	The specified parameter SourceCidrIp is not valid.	400	The error message returned when the specified SourceCidrIp parameter is invalid.
InvalidSourceGroup.NotFound	The specified SourceGroupId does not exist.	400	The error message returned when the specified source group ID does not exist.
InvalidSourceGroupId.Mismatch	Specified security group and source group are not in the same VPC.	400	The error message returned when the specified destination security group and source security group do not belong to the same VPC.
OperationDenied	The specified IpProtocol does not exist or IpProtocol and PortRange do not match.	400	The error message returned when the specified IP protocol does not exist or the specified IP protocol and port number range do not match.
InvalidParamter.Conflict	The specified SecurityGroupId should be different from the SourceGroupId.	403	The error message returned when the specified SecurityGroupId and SourceGroupId values are the same.

Error code	Error message	HTTP status code	Description
InvalidSourceGroupId.Mismatch	NicType is required or NicType expects intranet.	403	The error message returned when the NicType parameter is not specified or is not set to intranet.
MissingParameter	The input parameter SourceGroupId or SourceCidrIp cannot be both blank.	403	The error message returned when either the SourceGroupId parameter or the SourceCidrIp parameter is not specified.
InvalidRegionId.NotFound	The specified RegionId does not exist.	404	The error message returned when the specified region ID does not exist.
InvalidSecurityGroupId.NotFound	The specified SecurityGroupId does not exist.	404	The error message returned when the specified security group ID does not exist.
InvalidSourceGroupId.NotFound	The SourceGroupId provided does not exist in our records.	404	The error message returned when the specified source group ID does not exist.

2.1.1.12. SSH key pairs

2.1.1.12.1. CreateKeyPair

You can call this operation to create an SSH key pair. The system stores the public key and returns the unencrypted private key. The key pair is encoded by using PEM and is in the `PKCS#8` format. You must store the private key on your own and ensure its confidentiality.

Description

In addition to calling CreateKeyPair, you can create a key pair through other key pair generators and upload the key pair (ImportKeyPair) to a region.

Up to 500 key pairs can be created in each region.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateKeyPair.

Name	Type	Required	Description
RegionId	String	Yes	The ID of the region to which the key pair belongs. You can call DescribeRegions to view latest regions.
KeyPairName	String	Yes	The name of the key pair. The name must be unique. • The name must be 2 to 128 characters in length. • It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). • It supports all character set encoding formats. • It cannot start with http:// or https://.

Response parameters

Name	Type	Description
KeyPairName	String	The name of the key pair.
KeyPairFingerPrint	String	The fingerprint of the key pair. The public key fingerprint format is defined in RFC 4716 and uses the MD5 message digest algorithm. For more information, go to RFC 4716.
PrivateKeyBody	String	The private key of the key pair. The private key is encoded by using PEM and is in PKCS#8 format. For more information, see OpenSSLPKCS#8.

Examples

Sample requests

```
https://ecs.example.com/?Action=CreateKeyPair
&RegionId=cn-qingdao
&KeyPairName=test
&<Common request parameters>
```

Sample responses

XML format

```
<CreateKeyPairResponse>
   <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
   <KeyPairName>test</KeyPairName>
   <KeyPairFingerPrint>89:f0:ba:62:ac:b8:aa:e1:61:5e:fd:81:69:86:6d:6b:f0:c0:5a:d7</KeyPairFingerPri
nt>
   <PrivateKeyBody>xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx</PrivateKeyBody>
</CreateKeyPairResponse>
```

JSON format

```
{
   "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
   "KeyPairName": "test"
   "KeyPairFingerPrint": "89:f0:ba:62:ac:b8:aa:e1:61:5e:fd:81:69:86:6d:6b:f0:c0:5a:d7"
   "PrivateKeyBody": "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"
}
```

Error codes

The following table lists the error codes specific to this operation. For more information, go to API Error Center.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required `RegionId` parameter is not specified.
InvalidKeyPairName.Malformed	Specified Key Pair name is not valid.	400	The error message returned when the `KeyPairName` parameter is invalid or already exists.
QuotaExceed.KeyPair	The key pair quota exceeds.	403	The error message returned when the number of key pairs in a region has already reached 500.
InvalidRegionId.NotFound	The specified region does not exist.	404	The error message returned when the specified `RegionId` parameter does not exist.

2.1.1.12.2. ImportKeyPair

You can call this operation to import the public key of an RSA-encrypted key pair that was created by other key pair generators. After the public key is imported, you must store the private key on your own and ensure its confidentiality.

Description

When you call this operation, note that:

- Up to 500 key pairs can be created in each region.
- You can use any of the following encryption methods for your key pair:
  - rsa
  - dsa
  - ssh-rsa
  - ssh-dss
  - ecdsa
  - ssh-rsa-cert-v00@openssh.com
  - ssh-dss-cert-v00@openssh.com
  - ssh-rsa-cert-v01@openssh.com
  - ssh-dss-cert-v01@openssh.com
  - ecdsa-sha2-nistp256-cert-v01@openssh.com
  - ecdsa-sha2-nistp384-cert-v01@openssh.com
  - ecdsa-sha2-nistp521-cert-v01@openssh.com

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ImportKeyPair.
RegionId	String	Yes	The ID of the region to which the SSH key pair belongs. You can call DescribeRegions to view latest regions.
PublicKeyBody	String	Yes	The public key of the key pair to be imported.

Name	Type	Required	Description
KeyPairName	String	Yes	The name of the key pair to be imported. The name must be unique within its region. • The name must be 2 to 128 characters in length. • It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). • It supports all character set encoding formats. • It cannot start with http:// or https://.

Response parameters

Name	Type	Description
KeyPairName	String	The name of the key pair.
KeyPairFingerPrint	String	The fingerprint of the key pair. The public key fingerprint format is defined in RFC 4716 and uses the MD5 message digest algorithm. For more information, see RFC 4716.

Examples

Sample requests

```
https://ecs.example.com/?Action=ImportKeyPair
&RegionId=cn-qingdao
&PublicKeyBody=xxxxxxxxxxxxxx
&KeyPairName=test
&<Common request parameters>
```

Sample responses

XML format

```
<ImportKeyPairResponse>
   <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
   <KeyPairName>test</KeyPairName>
   <KeyPairFingerPrint> 89:f0:ba:62:ac:b8:aa:e1:61:5e:fd:81:69:86:6d:6b:f0:c0:5a:d7</KeyPairFingerPri
nt>
</ImportKeyPairResponse>
```

JSON format

```
{
   "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
   "KeyPairName": "test"
   "KeyPairFingerPrint": "89:f0:ba:62:ac:b8:aa:e1:61:5e:fd:81:69:86:6d:6b:f0:c0:5a:d7"
}
```

Error codes

The following table lists the error codes specific to this operation. For more information, go to API Error Center.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the required `RegionId` parameter is not specified.
InvalidPublicKeyBody.Malformed	The PublicKeyBody format is not supported.	400	The error message returned when the format of the `PublicKeyBody` parameter is incorrect.
InvalidKeyPairName.Malformed	Specified Key Pair name is not valid.	400	The error message returned when the `KeyPairName` parameter is invalid or already exists.
InvalidRegionId.NotFound	The specified region does not exist.	404	The error message returned when the specified `RegionId` parameter does not exist.

2.1.1.12.3. AttachKeyPair

You can call this operation to attach an SSH key pair to one or more Linux instances.

Description

When you call this operation, note that:

- SSH key pairs cannot be bound to Windows instances.
- By default, the username and password authentication method is disabled after you attach an SSH key pair.
- If an instance is in the **Running** state, call RebootInstance to restart the instance for the operation to take effect.
- If the instance is in the **Stopped** state, call StartInstance to start the instance for the operation to take effect.
- If an instance already has an SSH key pair attached, the new SSH key pair will automatically replace the former one.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AttachKeyPair.
RegionId	String	Yes	The ID of the region to which the target SSH key pair belongs. You can call DescribeRegions to view latest regions.
KeyPairName	String	Yes	The names of the target SSH key pairs.
InstanceIds	String	Yes	The IDs of instances to which you want to attach the SSH key pair. The value can contain a JSON array consisting of up to 50 instance IDs. Different instance IDs are separated with commas (,) and displayed in the format of ["i-xxxxxxxxx", "i-yyyyyyyyy", ... "i-zzzzzzzzz"].

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=AttachKeyPair
&RegionId=cn-qingdao
&KeyPairName=test
&InstanceIds=["i-XXXXX"]
&<Common request parameters>
```

Sample responses

XML format

```
<AttachKeyPairResponse>
  <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</AttachKeyPairResponse>
```

JSON format

```
{
  "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

Error codes

The following table lists the error codes specific to this operation. For more information, see API Error Center.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the `RegionId` parameter is not specified or when you are not authorized to use the resources in the specified region.
DependencyViolation.WindowsInstance	The instance creating this window, cannot use ssh key pair to login.	403	The error message returned when you are trying to attach an SSH key pair to Windows instances.

Error code	Error message	HTTP status code	Description
InvalidKeyPairName.NotFound	The specified KeyPairName does not exist in our records.	404	The error message returned when the specified `KeyPairName` parameter does not exist.
InvalidRegionId.NotFound	The specified RegionId does not exist.	404	The error message returned when the specified `RegionId` parameter does not exist.

2.1.1.12.4. DetachKeyPair

You can call this operation to detach an SSH key pair from one or more Linux instances.

Description

When you call this operation, note that:

- For the operation to take effect, you must call RebootInstance to restart the instance after you detach an SSH key pair.
- By default, the username and password authentication method is used after you detach an SSH key pair.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DetachKeyPair.
RegionId	String	Yes	The ID of the region to which the target SSH key pair belongs. You can call DescribeRegions to view latest regions.
KeyPairName	String	Yes	The name of the target SSH key pair.

Name	Type	Required	Description
InstanceIds	String	No	The IDs of instances from which you want to detach the SSH key pair. The value can contain a JSON array consisting of up to 50 instance IDs. Different instance IDs are separated with commas (,) and displayed in the format of ["i-xxxxxxxxx", "i-yyyyyyyyy", ... "i-zzzzzzzzz"].

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=DetachKeyPair
&RegionId=cn-qingdao
&InstanceIds=["i-xxxxxxx", "i-yyyyyyy"]
&KeyPairName=test
&<Common request parameters>
```

Sample responses

XML format

```
<DetachKeyPairResponse>
  <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</DetachKeyPairResponse>
```

JSON format

```
{
  "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

Error codes

The following table lists the error codes specific to this operation. For more information, see API Error Center.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the `RegionId` parameter is not specified or when you are not authorized to use the resources in the specified region.
DependencyViolation.WindowsInstance	The instance creating is windows, cannot use ssh key pair to login.	403	The error message returned when you are trying to detach an SSH key pair from Windows instances.
InvalidKeyPairName.NotFound	The specified KeyPairName does not exist.	404	The error message returned when the specified `KeyPairName` parameter does not exist.
InvalidRegionId.NotFound	The specified RegionId does not exist.	404	The error message returned when the specified `RegionId` parameter does not exist.

2.1.1.12.5. DeleteKeyPairs

You can call this operation to delete one or more SSH key pairs. The entry of a deleted SSH key pair is removed from the database. However, the instances that are attached to the SSH key pair can still use it. You can still view the name of the SSH key pair in the instance details list.

Description

When you call this operation, note that:

- You cannot call DescribeKeyPairs to query a deleted SSH key pair.
- When you call DescribeInstances to query instance information, the SSH key pair name (KeyPairNames) is still returned, but without any other information.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteKeyPairs.

Name	Type	Required	Description
RegionId	String	Yes	The ID of the region to which the target SSH key pairs belong. You can call DescribeRegions to view latest regions.
KeyPairNames	String	Yes	The names of the target SSH key pairs. The value can contain a JSON array consisting of up to 100 SSH key pairs. Different key pair names are separated with commas (,) and displayed in the format of ["key-xxxxxxxxx", "key-yyyyyyyyy", ... "key-zzzzzzzzz"].

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Examples

Sample requests

```
https://ecs.example.com/?Action=DeleteKeyPairs
&RegionId=cn-qingdao
&KeyPairNames=test
&<Common request parameters>
```

Sample responses

XML format

```
<DeleteKeyPairsResponse>
    <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</DeleteKeyPairsResponse>
```

JSON format

```
{
    "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```

Error codes

The following table lists the error codes specific to this operation. For more information, see API Error Center.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the `RegionId` parameter is not specified or when you are not authorized to use the resources in the specified region.
MissingParameter	The input parameter KeyPairName that is mandatory for processing this request is not supplied.	400	The error message returned when the `KeyPairName` parameter is not specified.
InvalidRegionId.NotFound	The specified RegionId does not exist.	404	The error message returned when the specified `RegionId` parameter does not exist.

2.1.1.12.6. DescribeKeyPairs

You can call this operation to query one or more SSH key pairs.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeKeyPairs.
RegionId	String	Yes	The ID of the region to which the target SSH key pairs belong. You can call DescribeRegions to view latest regions.

Name	Type	Required	Description
KeyPairFingerPrint	String	No	The fingerprint of the key pair. The fingerprint uses the MD5 algorithm based on the public key fingerprint format defined in RFC 4716. For more information, see RFC4716.
KeyPairName	String	No	The names of the target key pairs. The asterisks (`*`) symbol can be used as a wildcard with regular expressions to query key pairs by fuzzy match. Sample patterns: • `*SshKey` : queries key pair names that end with *SshKey*, including *SshKey*. • `SshKey*` : queries key pair names that start with *SshKey*, including *SshKey*. • `*SshKey*` : queries key pair names that contain *SshKey*, including *SshKey*. • `SshKey` : queries key pairs names that match *SshKey* exactly.
PageNumber	Integer	No	The page number to be queried in the SSH key pair list. Starting value: 1. Default value: 1.
PageSize	Integer	No	The number of entries to be displayed per page. Maximum value: 50. Default value: 10.

Response parameters

Name	Type	Description
TotalCount	Integer	The total number of key pairs.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of entries per page.
RegionId	String	The ID of the region to which the SSH key pair belongs.
KeyPairs	KeyPairItemType	A set of key pairs.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeKeyPairs
&RegionId=cn-qingdao
&KeyPairFingerPrint=xxxxxxxxxx
&KeyPairName=test
&PageNumber=1
&PageSize=20
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeKeyPairsResponse>
  <PageNumber>1</PageNumber>
  <PageSize>2</PageSize>
  <TotalCount>1</TotalCount>
  <KeyPairs>
    <KeyPair>
      <KeyPairName>test</KeyPairName >
      <KeyPairFingerPrint>xxxxxxxxxx</KeyPairFingerPrint>
    </KeyPair>
  </KeyPairs>
  <RequestId>473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E</RequestId>
</DescribeKeyPairsResponse>
```

JSON format

```
{
  "PageNumber": 1,
  "PageSize": 2,
  "TotalCount": 1,
  "KeyPairs": {
    "KeyPair":[{
      "KeyPairName": "test",
      "KeyPairFingerPrint": "xxxxxxxxxx"
    }]
  }
  "RequestId": "473469C7-AA6F-4DC5-B3DB-A3DC0DE3C83E"
}
```


Error codes

The following table lists the error codes specific to this operation. For more information, see API Error Center.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the `RegionId` parameter is not specified.
InvalidParameter	The specified parameter "PageNumber" is not valid.	400	The error message returned when the specified `PageNumber` value is invalid.
InvalidParameter	The specified parameter "PageSize" is not valid.	400	The error message returned when the specified `PageSize` value is invalid.

2.1.1.13. Elastic network interfaces

2.1.1.13.1. CreateNetworkInterface

You can call this operation to create an Elastic Network Interface (ENI).

When you call this operation, note that:

- An ENI can only be attached to a VPC-type ECS instance, and the ENI must belong to the same VPC as the ECS instance.
- After an ENI is created, it can be attached to an instance. The ENI can also be detached and

attached to a different instance. The attributes of an ENI do not change when it is attached to or detached from an instance.

- When you transfer an ENI from one instance to another, network traffic will be redirected to the new instance.
- A newly created ENI is in the Available state.
- You can create a maximum of 100 ENIs within a region.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateNetworkInterface.
RegionId	String	Yes	The ID of the region to which the ECS instance will belong. You can callDescribeRegions to view available regions.
VSwitchId	String	Yes	The VSwitch ID of the specified VPC.
PrimaryIpAddress	String	No	The primary private IP address to be given to the ENI. The specified IP address must be idle within the CIDR block of the VSwitch. If an IP address is not specified, an idle IP address of the VSwitch will be selected at random.
NetworkInterfaceName	String	No	The name to be given to the ENI. • The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). • The ENI name is displayed in the console. • It cannot start with http:// or https://. • If not specified, this parameter is null. Default value: null.
SecurityGroupId	String	Yes	The ID of the security group to which the ENI will belong. The security group must belong to the same VPC as the ENI.
Description	String	No	The description of the ENI. • The description must be 2 to 256 characters in length. • It cannot start with http:// or https://. • If not specified, this parameter is null. Default value: null.
ClientToken	String	No	A client token. It is used to guarantee the idempotency of requests. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotency.

Response parameters

Response parameter description

Name	Type	Description
NetworkInterfaceId	String	The ID of the ECS instance. The ID is automatically generated by the system and acts as a global unique identifier.

Error codes

Error code	Error message	HTTP status code	Description
Abs.InvalidAccount.NotFound	The Account is not found or ak is expired.	403	The error message returned when the specified Apsara Stack tenant account does not exist or when your AccessKey is expired.
Forbidden.NotSupportRAM	This action does not support accessed by RAM mode.	403	The error message returned when the operation you are trying to perform does not allow RAM users.
UnsupportedParameter	The parameters is unsupported.	400	The error message returned when the specified parameter does not exist or is not supported.
Forbidden.SubUser	The specified action is not available for you.	403	The error message returned when the operation you are trying to perform does not allow RAM users.
MissingParameter	The input parameter that is mandatory for processing this request is not supplied.	400	The error message returned when a required parameter is not specified.
InvalidEcsId.NotFound	The specified server is not found.	404	The error message returned when the specified instance ID does not exist.
InvalidVSwitchId.NotFound	The specified VSwitchId is not found.	404	The error message returned when the specified VSwitch ID does not exist.

Error code	Error message	HTTP status code	Description
InvalidSecurityGroupId.NotFound	The specified SecurityGroupId is not found.	404	The error message returned when the specified security group ID does not exist.
MaxEniCountExceeded	The number of ENI exceeds the limit per region.	403	The error message returned when the number of ENIs in the specified region has reached the upper limit.
InvalidOperation.AvailabilityZoneMismatch	The VPC VSwitch of the specified ENI and ECS instance are not in the zone.	403	The error message returned when the specified VSwitch, ENI and ECS instance are not in the same zone.
InvalidOperation.VpcMismatch	The VPC of the specified ENI and security group are not in the same VPC.	403	The error message returned when the specified ENI and security group do not belong to the same VPC.
SecurityGroupInstanceLimitExceed	The maximum number of instances in a security group is exceeded.	403	The error message returned when the number of instances in the specified security group has reached the upper limit.
InvalidSecurityGroupId.NotVpc	The specified SecurityGroupId not in VPC.	403	The error message returned when the specified security group is not of the VPC type.

Examples

Sample requests

```
https://ecs.example.com/?Action=CreateNetworkInterface
&RegionId=cn-hangzhou
&VSwitchId=[vswitchid]
&SecurityGroupId=sg-c0003exxxxx
&Common request parameters
```

Sample responses

XML format

```
<CreateNetworkInterfaceResponse>
  <RequestId>04F0F334-1335-436C-A1D7-6C044FExxxxx</RequestId>
  <NetworkInterfaceId>eni-eniIxxxxx</NetworkInterfaceId>
</CreateNetworkInterfaceResponse>
```

JSON format

```
{
  "RequestId": "04F0F334-1335-436C-A1D7-6C044FExxxxx",
  "NetworkInterfaceId": "eni-enixxxxx"
}
```

2.1.1.13.2. AttachNetworkInterface

You can call this operation to attach an Elastic Network Interface (ENI) to an ECS instance in a VPC.

When you call this operation, note that:

- The ENI must be in the Available state.
- The ECS instance must be in the Stopped state.
- An ENI can only be attached to a VPC-type ECS instance, and the ENI must belong to the same VPC as the ECS instance.
- One ENI can only be attached to one ECS instance.
- However, an ECS instance can be attached to multiple ENIs at the same time. For more information, see Instance types.
- Because a VSwitch of a VPC can only be located in a single zone, ensure that the ECS instance to be attached to an ENI is in the same zone as the VSwitch to which the ENI belongs.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AttachNetworkInterface.
RegionId	String	Yes	The ID of the region to which the target ECS instance belongs. You can call DescribeRegions to view available regions.
NetworkInterfaceId	String	Yes	The ID of the ENI to be attached.
InstanceId	String	Yes	The ID of the target ECS instance.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code	Error message	HTTP status code	Description
Abs.InvalidAccount.NotFound	The Account is not found or ak is expired.	403	The error message returned when the specified Apsara Stack tenant account does not exist or when your AccessKey is expired.
Forbidden.NotSupportRAM	This action does not support accessed by RAM mode.	403	The error message returned when the operation you are trying to perform does not allow RAM users.
UnsupportedParameter	The parameters is unsupported.	400	The error message returned when the specified parameter does not exist or is not supported.
Forbidden.SubUser	The specified action is not available for you.	403	The error message returned when the operation you are trying to perform does not allow RAM users.
InvalidOperation.InvalidEcsState	The operation is not allowed in the current ECS state.	400	The error message returned when the specified operation is not supported in the current ECS instance status.
InvalidOperation.DetachPrimaryEniNotAllowed	Detaching primary ENI from ECS instance is not allowed.	400	The error message returned when you are trying to unbind a primary NIC from an ECS instance.
MissingParameter	The input parameter that is mandatory for processing this request is not supplied.	400	The error message returned when a required parameter is not specified.
InvalidEcsId.NotFound	The specified EcsId is not found.	404	The error message returned when the specified instance ID does not exist.

Error code	Error message	HTTP status code	Description
EniPerInstanceLimitExceeded	The number of ENI exceeds the limit for the type of instance you are trying to launch.	403	The error message returned when the number of ENIs exceeds the upper limit for the specified ECS instance type.
InvalidOperation.VpcMismatch	The VPC of the specified ENI and security group are not in the same VPC.	403	The error message returned when the specified ENI and security group do not belong to the same VPC.
SecurityGroupInstanceLimitExceed	The maximum number of instances in a security group is exceeded.	403	The error message returned when the number of instances in the specified security group has reached the upper limit.
InvalidOperation.InvalidEniType	The operation is not allowed in the current ENI type.	403	The error message returned when the specified operation is not supported by the current ENI type.

Examples

Sample requests

```
https://ecs.example.com/?Action=AttachNetworkInterface
&RegionId=cn-hangzhou
&NetworkInterfaceId=[networkInterfaceId]
&InstanceId=AY121018033933eae8xxxxx
&Common request parameters
```

Sample responses

XML format

```
<AttachNetworkInterfaceResponse>
   <RequestId>04F0F334-1335-436C-A1D7-6C044FExxxxx</RequestId>
</AttachNetworkInterfaceResponse>
```

JSON format

```
{
  "RequestId": "04F0F334-1335-436C-A1D7-6C044FExxxxx"
}
```

2.1.1.13.3. DescribeNetworkInterfaces

You can call this operation to query available ENIs.

When you call this operation, note that:

- You can specify attribute values to filter the results.
- If no attribute values are specified, all ENIs are returned.
- You can query a maximum of 100 ENIs at a time.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeNetworkInterfaces.
RegionId	String	Yes	The ID of the region in which you want to query ENIs.
VSwitchId	String	No	The ID of the VSwitch associated with the ENIs to be queried.
PrimaryIpAddress	String	No	The primary private IP address of the ENIs to be queried.
SecurityGroupId	String	No	The ID of the security group to which the target ENIs belong.
NetworkInterfaceName	String	No	The name of the ENI.
Type	String	No	The category of the ENI. Valid values: • Primary • Secondary
InstanceId	String	No	The ID of the ECS instance to which the ENI is attached.
NetworkInterfaceId.N	String	No	The ID of the ENI. You can query a maximum of 100 ENIs at a time.
PageNumber	Integer	No	The page number of the queried result. The parameter value is a positive integer. Default value: 1.
PageSize	Integer	No	The number of entries on each page. Valid values: [1,100]. Default value: 10.

Response parameters

Response parameter description

Name	Type	Description
NetworkInterfaceSet	NetworkInterfaceSet	A set of ENIs.
TotalCount	Integer	The total number of instances.
PageNumber	Integer	The page number that you query in the instance list.
PageSize	Integer	The number of entries per page.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
Abs.InvalidAccount.NotFound	The Account is not found or ak is expired.	403	The error message returned when your Apsara Stack tenant account does not exist or your AccessKey is expired.
UnsupportedParameter	The parameters is unsupported.	400	The error message returned when the specified parameter does not exist or is not supported.
MissingParameter	The required input parameter for processing this request is not provided.	400	The error message returned when a required parameter is not specified.
InvalidEcsId.NotFound	The specified server is not found.	404	The error message returned when the specified instance ID does not exist.
InvalidVSwitchId.NotFound	The specified VSwitchId is not found.	404	The error message returned when the specified VSwitch ID does not exist.

Error code	Error message	HTTP status code	Description
InvalidSecurityGroupId.NotFound	The specified SecurityGroupId is not found.	404	The error message returned when the specified security group ID does not exist.
InvalidOperation.AvailabilityZoneMismatch	The VPC VSwitch of the specified ENI and ECS instance are not in the same availability zone.	403	The error message returned when the specified VSwitch, ENI and ECS instance are not in the same zone.
InvalidOperation.VpcMismatch	The VPC of the specified ENI and security group are not in the same VPC.	403	The error message returned when the specified ENI and security group are not in the same VPC.
InvalidSecurityGroupId.NotVpc	The specified SecurityGroupId not in VPC.	403	The error message returned when the specified security group is not of the VPC type.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeNetworkInterfaces
&RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

XML format

```
<DescribeNetworkInterfacesResponse>
  <NetworkInterfaceSets>
    <NetworkInterfaceSet>
      <AssociatedPublicIp />
      <CreationTime>2017-11-24T06:14:22Z</CreationTime>
      <InstanceId>AY121018033933eaxxxxx</InstanceId>
      <MacAddress>00:16:3e:0f:XX:XX</MacAddress>
      <NetworkInterfaceId>eni-bp17pdijfczaxZZZZxxxxx</NetworkInterfaceId>
      <PrivateIpAddress>XXX.XXX.XX.XX</PrivateIpAddress>
      <PrivateIpSets>
        <PrivateIpSet>
          <AssociatedPublicIp />
          <Primary>true</Primary>
          <PrivateIpAddress>XXX.XXX.XX.XX</PrivateIpAddress>
        </PrivateIpSet>
      </PrivateIpSets>
      <SecurityGroupIds>
        <SecurityGroupId>sg-bp144yr32sx6ndwxxxxx</SecurityGroupId>
      </SecurityGroupIds>
      <Status>Available</Status>
      <Type>Secondary</Type>
      <VpcId>vpc-bp1j7w3gc1cexjqdxxxxx</VpcId>
      <VSwitchId>vsw-bp16usj2p27htro3xxxxx</VSwitchId>
      <ZoneId>cn-hangzhou-e</ZoneId>
    </NetworkInterfaceSet>
  </NetworkInterfaceSets>
  <PageNumber>1</PageNumber>
  <PageSize>100</PageSize>
  <RequestId>CEE5C347-0B64-4535-A061-95BE95Axxxxx</RequestId>
  <TotalCount>1</TotalCount>
</DescribeNetworkInterfacesResponse>
```

JSON format

```
{
  "NetworkInterfaceSets": {
    "NetworkInterfaceSet": [
      {
        "AssociatedPublicIp": {
        },
        "CreationTime": "2017-11-24T06:14:22Z",
        "InstanceId": "AY121018033933eaxxxxx",
        "MacAddress": "00:16:3e:0f:XX:XX",
        "NetworkInterfaceId": "eni-bp17pdijfczaxZZZZxxxxx",
        "PrivateIpAddress": "XXX.XXX.XX.XX",
        "PrivateIpSets": {
          "PrivateIpSet": [
            {
              "AssociatedPublicIp": {
              },
              "Primary": true,
              "PrivateIpAddress": "XXX.XXX.XX.XX"
            }
          ]
        },
        "SecurityGroupIds": {
          "SecurityGroupId": [
            "sg-bp144yr32sx6ndwxxxxx"
          ]
        },
        "Status": "Available",
        "Type": "Secondary",
        "VpcId": "vpc-bp1j7w3gc1cexjqdxxxxx",
        "VSwitchId": "vsw-bp16usj2p27htro3xxxxx",
        "ZoneId": "cn-hangzhou-e"
      }
    ]
  },
  "PageNumber": 1,
  "PageSize": 100,
  "RequestId": "CEE5C347-0B64-4535-A061-95BE95Axxxxx",
  "TotalCount": 1
}
```

2.1.1.13.4. DetachNetworkInterface

You can call this operation to detach an ENI from an ECS instance.

When you call this operation, note that:

- The primary ENI of an ECS instance cannot be detached.
- The ENI must be in the In_use state.
- The ECS instance must be in the Stopped state.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DetachNetworkInterface.
RegionId	String	Yes	The ID of the region to which the instance belongs.
NetworkInterfaceId	String	Yes	The ID of the ENI.
InstanceId	String	Yes	The ID of the instance.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code	Error message	HTTP status code	Description
Abs.InvalidAccount.NotFound	The Account is not found or ak is expired.	403	The error message returned when your Apsara Stack tenant account does not exist or your AccessKey is expired.
Forbidden.NotSupportRAM	This action does not support accessed by RAM mode.	403	The error message returned when you try to perform this operation as a RAM user.
UnsupportedParameter	The parameters is unsupported.	400	The error message returned when the specified parameter does not exist or is not supported.

Error code	Error message	HTTP status code	Description
Forbidden.SubUser	The specified action is not available for you.	403	The error message returned when you try to perform this operation as a RAM user.
InvalidOperation.InvalidEcsState	The operation is not allowed in the current ECS state.	400	The error message returned when the specified operation is not supported in the current ECS instance status.
InvalidOperation.DetachPrimaryEniNotAllowed	Detaching primary ENI from ECS instance is not allowed.	400	The error message returned when you attempt to detach the primary ENI from an ECS instance.
MissingParameter	The required input parameter for processing this request is not provided. supplied.	400	The error message returned when a required parameter is not specified.
InvalidEcsId.NotFound	The specified server is not found.	404	The error message returned when the specified instance ID does not exist.
EniPerInstanceLimitExceeded	The number of ENI exceeds the limit for the type of instance you are trying to launch.	403	The error message returned when the number of ENIs exceeds upper limit supported by the specified instance type.
InvalidOperation.InvalidEniType	The operation is not allowed in the current ENI type.	403	The error message returned when the operation is not supported by the current ENI type.

Examples

Sample requests

```
https://ecs.example.com/?Action=DetachNetworkInterface
&RegionId=cn-hangzhou
&NetworkInterfaceId=[networkInterfaceId]
&InstanceId=AY121018033933eaxxxxx
&Common request parameters
```

Sample responses

XML format

```
<DetachNetworkInterfaceResponse>
  <RequestId>04F0F334-1335-436C-A1D7-6C044FExxxxx</RequestId>
</DetachNetworkInterfaceResponse>
```

JSON format

```
{
  "RequestId": "04F0F334-1335-436C-A1D7-6C044FExxxxx",
}
```

2.1.1.13.5. DeleteNetworkInterface

You can call this operation to delete an ENI.

When you call this operation, note that:

- The ENI must be in the Available state.
- If the ENI is attached to an ECS instance, you must first call DetachNetworkInterface before you can delete the ENI.
- After the ENI is deleted:
  - The primary private IP address of the ENI (PrimaryIpAddress) will be released automatically.
  - The deleted ENI is automatically removed from its security group.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteNetworkInterface.
RegionId	String	Yes	The ID of the region to which the ENI belongs.
NetworkInterfaceId	String	Yes	The ID of the ENI.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code	Error message	HTTP status code	Description
Abs.InvalidAccount.NotFound	The Account is not found or ak is expired.	403	The error message returned when your Apsara Stack tenant account does not exist or your AccessKey is expired.
Forbidden.NotSupportRAM	This action does not support accessed by RAM mode.	403	The error message returned when you try to perform this operation as a RAM user.
UnsupportedParameter	The parameters is unsupported.	400	The error message returned when the specified parameter does not exist or is not supported.
Forbidden.SubUser	The specified action is not available for you.	403	The error message returned when you try to perform this operation as a RAM user.
InvalidOperation.DetachPrimaryEniNotAllowed	Detaching primary ENI from ECS instance is not allowed.	400	The error message returned when you attempt to detach the primary ENI from an ECS instance.
MissingParameter	The required input parameter for processing this request is not provided. supplied.	400	The error message returned when a required parameter is not specified.
InvalidOperation.InvalidEniType	The operation is not allowed in the current ENI type.	403	The error message returned when the operation is not supported by the current ENI type.

Examples

Sample requests

```
https://ecs.example.com/?Action=DeleteNetworkInterface
&RegionId=cn-hangzhou
&NetworkInterfaceId=[networkInterfaceId]
&Common request parameters
```

Sample responses

XML format

```
<DetachNetworkInterface>
   <RequestId>04F0F334-1335-436C-A1D7-6C044FExxxxx</RequestId>
</DetachNetworkInterface>
```

JSON format

```
{
   "RequestId": "04F0F334-1335-436C-A1D7-6C044FExxxxx",
}
```

2.1.1.13.6. ModifyNetworkInterfaceAttribute

You can call this operation to modify the attributes of an ENI.

When you call this operation, note that:

- This operation can only modify the attributes of an elastic NIC.
- Only one ENI can have its attributes modified at a time.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyNetworkInterfaceAttribute.
RegionId	String	Yes	The ID of the region to which the target instance belongs.
NetworkInterfaceId	String	Yes	The ID of the ENI.
SecurityGroupId.N	String	No	The ID of the security group to which the ENI is to be assigned to. The new security group will replace the previous security group that the ENI belongs to. The security group must be in the same VPC as the ENI.

Name	Type	Required	Description
NetworkInterfaceName	String	No	The name of the ENI. • The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, underscores (_), and hyphens (-). • The ENI name is displayed in Apsara Stack console. • It cannot start with http:// or https://. • If not specified, this parameter is null. Default value: null.
Description	String	No	The description of the ENI. • The description must be 2 to 256 characters in length. • It cannot start with http:// or https://. • If not specified, this parameter is null. Default value: null.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Error codes

Error code	Error message	HTTP status code	Description
Abs.InvalidAccount.NotFound	The Account is not found or ak is expired.	403	The error message returned when your Apsara Stack tenant account does not exist or your AccessKey is expired.
Forbidden.NotSupportRAM	This action does not support accessed by RAM mode.	403	The error message returned when you try to perform this operation as a RAM user.
UnsupportedParameter	The parameters is unsupported.	400	The error message returned when the specified parameter does not exist or is not supported.
Forbidden.SubUser	The specified action is not available for you.	403	The error message returned when you try to perform this operation as a RAM user.

Error code	Error message	HTTP status code	Description
MissingParameter	The required input parameter for processing this request is not provided. supplied.	400	The error message returned when a required parameter is not specified.
InvalidVSwitchId.NotFound	The specified VSwitchId is not found.	404	The error message returned when the specified VSwitch ID does not exist.
InvalidSecurityGroupId.NotFound	The specified SecurityGroupId is not found.	404	The error message returned when the specified security group ID does not exist.
InvalidOperation.AvailabilityZoneMismatch	The VPC VSwitch of the specified ENI and ECS instance are not in the same availability zone.	403	The error message returned when the specified VSwitch, ENI, and instance do not belong to the same zone.
InvalidOperation.VpcMismatch	The VPC of the specified ENI and security group are not in the same VPC.	403	The error message returned when the specified ENI and security group do not belong to the same VPC.
SecurityGroupInstanceLimitExceed	The maximum number of instances in a security group is exceeded.	403	The error message returned when the number of instances in the specified security group exceeds the upper limit.
InvalidSecurityGroupId.NotVpc	The specified SecurityGroupId not in VPC.	403	The error message returned when the specified security group is not of the VPC type.
InvalidOperation.InvalidEniType	The operation is not allowed in the current ENI type.	403	The error message returned when the operation is not supported by the current ENI type.

Examples

Sample requests

```
https://ecs.example.com/?Action=ModifyNetworkInterfaceAttribute
&RegionId=cn-hangzhou
&NetworkInterfaceId=[networkInterfaceId]
&Common request parameters
```

Sample responses

XML format

```
<DetachNetworkInterfaceResponse>
   <RequestId>04F0F334-1335-436C-A1D7-6C044FExxxxx</RequestId>
</DetachNetworkInterfaceResponse>
```

JSON format

```
{
   "RequestId": "04F0F334-1335-436C-A1D7-6C044FExxxxx",
}
```

2.1.1.14. Regions and zones

2.1.1.14.1. DescribeRegions

You can call this operation to query available regions.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeRegions.

Response parameters

Response parameter description

Name	Type	Description
Regions	RegionType	A set of RegionType data.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeRegions
&Common request parameters
```

Sample responses

XML format

```
<DescribeRegionsResponse>
   <RequestId>611CB80C-B6A9-43DB-9E38-0B0AC3D9B58F</RequestId>
   <Regions>
      <Region>
         <RegionId>cn-hangzhou</RegionId>
      </Region>
      <Region>
         <RegionId>cn-qingdao</RegionId>
      </Region>
   </Regions>
</DescribeRegionsResponse>
```

JSON format

```
{
   "RequestId": "611CB80C-B6A9-43DB-9E38-0B0AC3D9B58F",
   "Regions": {
      "Region": [{
         "RegionId": "cn-hangzhou "
      },
      {
         "RegionId": "cn-qingdao"
      }]
   }
}
```

2.1.1.14.2. DescribeZones

You can call this operation to query available zones.

Request parameters

Request parameter description

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeZones.
RegionId	String	Yes	The region ID.

Response parameters

Response parameter description

Name	Type	Description
Zones	ZoneType	A set of ZoneType data.

Error codes

This operation returns only common errors.

Examples

Sample requests

```
https://ecs.example.com/?Action=DescribeZones
&amp;RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

XML format

```
<DescribeZonesResponse>
  <Zones>
    <Zone>
      <AvailableResourceCreation>
        <ResourceTypes>Instance</ResourceTypes>
        <ResourceTypes>Disk</ResourceTypes>
      </AvailableResourceCreation>
      <LocalName></LocalName>
      <ZoneId>cn-hangzhou-d</ZoneId>
      <AvailableDiskCategories>
        <DiskCategories>cloud</DiskCategories>
      </AvailableDiskCategories>
    </Zone>
    <Zone>
      <AvailableResourceCreation>
        <ResourceTypes>Instance</ResourceTypes>
        <ResourceTypes>Disk</ResourceTypes>
      </AvailableResourceCreation>
      <LocalName></LocalName>
      <ZoneId>cn-hangzhou-b</ZoneId>
      <AvailableDiskCategories>
        <DiskCategories>cloud</DiskCategories>
      </AvailableDiskCategories>
    </Zone>
  </Zones>
  <RequestId>6DB97BCC-92BA-424D-A7C8-3F6486612BAE</RequestId>
</DescribeZonesResponse>
```

JSON format

```
{
 "RequestId": "A347EF0E-BBCC-4EFA-BD79-27AA3ACFD1BF",
 "Zones": {
  "Zone": [
   {
    "AvailableDiskCategories": {
     "DiskCategories": [
      "cloud"
     ]
    },
    "AvailableResourceCreation": {
     "ResourceTypes": [
      "Instance",
      "Disk"
     ]
    },
    "LocalName": "",
    "ZoneId": "cn-hangzhou-d"
   },
   {
    "AvailableDiskCategories": {
     "DiskCategories": [
      "cloud"
     ]
    },
    "AvailableResourceCreation": {
     "ResourceTypes": [
      "Instance",
      "Disk"
     ]
    },
    "LocalName": "",
    "ZoneId": "cn-hangzhou-b"
   }
  ]
 }
}
```


2.1.1.15. Tags

2.1.1.15.1. AddTags

When you call this operation, note that:

- You can create tags for ECS instances, disks, snapshots, images, and security groups.
- You can bind up to 10 tags to each resource.
- If the key of the tag you want to bind already exists in the specified resource, the value of the tag will be overwritten.
- Tag.n.key and Tag.n.Value must match based on the value of n.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AddTags.
RegionId	String	Yes	The ID of the region to which the target resource belongs.
ResourceId	String	Yes	The ID of the resource to which you want to bind a tag.
ResourceType	String	Yes	The resource type. Valid values: • image • instance • snapshot • disk • securitygroup All values are in lowercase.
Tag.n.Key	String	Yes	The key of the tag. The value of n ranges from 1 to 5. The key must be 1 to 64 characters in length. It cannot start with aliyun. It cannot start with http:// or https://. It cannot be a null string.
Tag.n.Value	String	Yes	The value of the tag. The value of n ranges from 1 to 5. The tag value must be 1 to 128 characters in length. It cannot start with aliyun. It cannot start with http:// or https://. It can be a null string.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidResourceId.NotFound	The specified ResourceId is not found in our records.	404	The error message returned when the specified region ID does not exist.
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.
InvalidResourceType.NotFound	The ResourceType provided does not exist in our records.	404	The error message returned when the specified resource type does not exist.
InvalidTagKey.Malformed	The specified Tag.n.Key is not valid.	400	The error message returned when the specified Tag.n.Key is invalid.
InvalidTagValue.Malformed	The specified Tag.n.Value is not valid.	400	The error message returned when the specified Tag.n.Value is invalid.
OperationDenied.QuotaExceed	The quota of tags on resource is beyond permitted range.	400	The error message returned when 10 tags have already been bound to the resource.
InvalidTag.Mismatch	The specified Tag.n.Key and Tag.n.Value are not match.	400	The error message returned when Tag.n.Key and Tag.n.Value do not match.
InvalidTagCount	The specified tags are beyond the permitted range.	400	The error message returned when more than five tags are specified.

Error code	Error message	HTTP status code	Description
InvalidResourceId.NotSupported	The specified ResourceId does not support tagging.	403	The error message returned when the specified resource ID cannot be bound to tags.

Examples

Sample requests

```
https://ecs.example.com/?Action=AddTags
&ResourceId=s-946ntx4wr
&ResourceType=snapshot
&RegionId=cn-shanghai
&Tag. 1. Key=test
&Tag. 1. Value=api
&Common request parameters
```

Sample responses

XML format

```
<AddTagsResponse>
   <RequestId>C46FF5A8-C5F0-4024-8262-B16B639225A0</RequestId>
</AddTagsResponse>
```

JSON format

```
{
 "RequestId": "C46FF5A8-C5F0-4024-8262-B16B639225A0"
}
```

2.1.1.15.2. RemoveTags

You can call this operation to unbind tags from a resource such as an instance, disk, snapshot, image, or security group by specifying tags and a resource ID.

Request parameters

Request parameter description

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RemoveTags.
RegionId	String	Yes	The ID of the region to which the target resource belongs.
ResourceId	String	Yes	The ID of the resource from which you want to unbind the tag.
ResourceType	String	Required	The resource type. Valid values: • image • instance • snapshot • disk • securitygroup All values are in lowercase.
Tag.n.Key	String	No	The key of the tag. It must be 1 to 64 characters in length. The value of n can be from 1 to 5.
Tag.n.Value	String	No	The value of the tag. It must be 1 to 128 characters in length. The value of n can be from 1 to 5. If this parameter is not specified, any tag whose key matches the specified Tag.n.Key will be unbound from the specified resource.

Response parameters

Response parameter description

Name	Type	Description
RequestId	String	The request ID.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter "ResourceId" that is mandatory for processing this request is not supplied.	400	The error message returned when the ResourceId parameter is not specified.

Error code	Error message	HTTP status code	Description
InvalidResourceId.NotFound	The specified ResourceId is not found in our records	404	The error message returned when the specified resource ID does not exist.
MissingParameter	The input parameter "RegionId" that is mandatory for processing this request is not supplied.	400	The error message returned when the RegionId parameter is not specified.
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.
InvalidResourceType.NotFound	The ResourceType provided does not exist in our records.	404	The error message returned when the specified resource type does not exist.
InvalidTagCount	The specified tags are beyond the permitted range	400	The error message returned when more than five tags are specified.

Examples

Sample requests

```
https://ecs.example.com/?Action=RemoveTags
&ResourceId=s-946ntx4wr
&ResourceType=snapshot
&RegionId=cn-shanghai
&Tag. 1. Key=test
&Tag. 1. Value=api
&Common request parameters
```

Sample responses

XML format

```
<RemoveTagsResponse>
   <RequestId>6A2C8AB5-E15D-478C-B56A-CF3DAF060028</RequestId>
</RemoveTagsResponse>
```

JSON format

```
{
 "RequestId": "6A2C8AB5-E15D-478C-B56A-CF3DAF060028"
}
```

2.1.1.15.3. DescribeTags

When you call this operation, note that:

- You can query any tags by specifying conditions such as resource type, resource ID, tag key, and tag value.
- The relationship between specified conditions is AND. Only TagSetItem data that meet all of the specified conditions will be returned.
- If a tag key is specified but no tag values are specified, all tags related to the tag key will be returned.
- If a tag key-value pair is specified, only tags that exactly match the key-value pair will be returned.

Request parameters

Request parameter description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeTags.
RegionId	String	Yes	The ID of the region to which the target tags belong.
ResourceId	String	No	The ID of a resource assocaited with target tags.
ResourceType	String	No	The resource type. Valid values: • image • instance • snapshot • disk • securitygroup All values are in lowercase.
Tag.n.Key	String	No	The key of the tag. The value of n ranges from 1 to 5.
Tag.n.Value	String	No	The value of the tag. The value of n ranges from 1 to 5.
PageSize	Integer	No	Default value: 50. Maximum value: 100.
PageNumber	Integer	No	The page number that you query in the tag list. Starting value: 1. Default value: 1.

Response parameters

Response parameter description

Name	Type	Description
RequestId	String	The request ID.
Tags	TagSetItem	The struct list of the returned content.
PageSize	Integer	Default value: 50. Maximum value: 100.
PageNumber	Integer	The page number that you query in the tag list. Starting value: 1. Default value: 1.
TotalCount	Integer	The total number of instances.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned when the specified region ID does not exist.
InvalidResourceType.NotFound	The ResourceType provided does not exist in our records.	404	The error message returned when the specified resource type does not exist.
InvalidTagCount	The specified tags are beyond the permitted range.	400	The error message returned when more than five tags are specified.
InvalidTagKey.Malformed	The parameter Tag.n.Key is illegal.	400	The error message returned when the specified Tag.n.Key is invalid.
InvalidTagValue.Malformed	The parameter Tag.n.Value is illegal.	400	The error message returned when the specified Tag.n.Value is invalid.

Examples

Sample requests

```
https://ecs.example.com/?Action=AddTags
&ResourceId=s-946ntx4wr
&ResourceType=snapshot
&RegionId=cn-shanghai
&Tag. 1. Key=test
&Tag. 1. Value=api
&Common request parameters
```

Sample responses

XML format

```
<DescribeTagsResponse>
  <RequestId>B04B8CF3-4489-432D-83BA-6F128E4F2295</RequestId>
  <PageNumber>1</PageNumber>
  <PageSize>50</PageSize>
  <Tags>
    <Tag>
      <TagKey>test</TagKey>
      <TagValue>api</TagValue>
    </Tag>
  </Tags>
  <TotalCount>1</TotalCount>
</DescribeTagsResponse>
```

JSON format

```
{
 "PageNumber": 1,
 "PageSize": 50,
 "RequestId": "B04B8CF3-4489-432D-83BA-6F128E4F2295",
 "Tags": {
  "Tag": [
   {
    "TagKey": "test",
    "TagValue": "api"
   }
  ]
 },
 "TotalCount": 1
}
```

2.1.1.16. Other operations

2.1.1.16.1. DescribeTasks

You can call this operation to query existing tasks.

Request parameters

Request parameter description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this value to DescribeTasks.
RegionId	String	Yes	The ID of the region to query.
TaskAction	String	No	The operation name of the task. Valid values: • ImportImage • ExportImage • ImportSnapshot • ExportSnapshot
TaskIds	String	No	The task IDs to query. You can specify a maximum of 100 task IDs separated by commas (,).
TaskStatus	String	No	The status of the task. Valid values: • Finished • Processing • Pending • Deleted • Paused Default value: null.
StartTime	String	No	The beginning of the time range where the data is queried. Specify the time in the ISO 8601 standard in the YYYY-MM-DDThh:mmZ format. The time must be in UTC.
EndTime	String	No	The end of the time range where the data is queried. Specify the time in the ISO 8601 standard in the YYYY-MM-DDThh:mmZ format. The time must be in UTC.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 1 to 100. Default value: 10.

Response parameters

Response parameter description

Parameter	Type	Description
TaskSet	TaskType	A set of tasks.
RegionId	String	The ID of the region.
TotalCount	Integer	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of entries on the current page.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	An input parameter "RegionId" that is mandatory for processing the request is not supplied.	400	The error message returned because the required RegionId parameter is not specified.
InvalidRegionId.NotFound	The specified region not found.	400	The error message returned because the specified region ID does not exist.

Examples

Sample requests

```
https://ecs.example.com/
? Action=DescribeTasks&RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

XML format

```
<DescribeTasksResponse>
 <PageNumber>1</PageNumber>
 <TotalCount>2</TotalCount>
 <PageSize>2</PageSize>
 <RegionId>cn-hangzhou</RegionId>
 <RequestId>E5C82807-5588-4661-9A96-350B206A7623</RequestId>
 <TaskSet>
  <Task>
   <CreationTime>2015-11-24T12:50Z</CreationTime>
   <FinishedTime>2015-11-24T12:50Z</FinishedTime>
   <SupportCancel>true</SupportCancel>
   <TaskAction>IMPORT_IMAGE</TaskAction>
   <TaskStatus>Finished</TaskStatus>
   <TaskId>t-23mo8zf9w</TaskId>
  </Task>
  <Task>
   <CreationTime>2015-11-23T15:10Z</CreationTime>
   <FinishedTime>2015-11-23T15:16Z</FinishedTime>
   <SupportCancel>true</SupportCancel>
   <TaskAction>IMPORT_IMAGE</TaskAction>
   <TaskStatus>Finished</TaskStatus>
   <TaskId>t-23sgu0dyj</TaskId>
  </Task>
 </TaskSet>
</DescribeTasksResponse>
```

JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 2,
  "PageSize": 2,
  "RegionId": "cn-hangzhou",
  "RequestId": "F746C690-D9EA-4F87-AF31-8E1910FAB541",
  "TaskSet": {
    "Task": [
      {
        "CreationTime": "2015-11-24T12:50Z",
        "FinishedTime": "2015-11-24T12:50Z",
        "SupportCancel": true,
        "TaskAction": "ImportImage",
        "TaskStatus": "Finished",
        "TaskId": "t-23mo8zf9w"
      },
      {
        "CreationTime": "2015-11-23T15:10Z",
        "FinishedTime": "2015-11-23T15:16Z",
        "SupportCancel": true,
        "TaskAction": "ImportImage",
        "TaskStatus": "Finished",
        "TaskId": "t-23sgu0dyj"
      }
    ]
  }
}
```


2.1.1.16.2. DescribeTaskAttribute

You can call this operation to query the details of a task.

Request parameters

Request parameter description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this value to DescribeTaskAttribute.
RegionId	String	Yes	The ID of the region to query.
TaskId	String	Yes	The ID of the task to query.

Response parameters

Response parameter description

Parameter	Type	Description
TaskId	String	The ID of the task.
TaskAction	String	The operation name of the task. Valid values: • ImportImage • ExportImage • ImportSnapshot • ExportSnapshot
RegionId	String	The ID of the region.
TaskStatus	String	The status of the task.
Taskprocess	String	The progress of the task.
SupportCancel	String	Indicates whether the task can be canceled. Valid values: • True • False
SuccessCount	Integer	The number of tasks that are completed successfully.
FailedCount	Integer	The number of tasks that failed to execute.
CreationTime	String	The time the task was created. The time follows the ISO 8601 standard in the YYYY-MM-DDThh:mmZ format. The time is displayed in UTC.
FinishedTime	String	The time the task was completed. The time follows the ISO 8601 standard in the YYYY-MM-DDThh:mmZ format. The time is displayed in UTC.

Error codes

N/A

Examples

- **Sample requests**

  ```
  https://ecs.example.com/?Action=DescribeTaskAttribute&RegionId=cn-hangzhou &TaskId=t-23ym6mvro &Common request parameters
  ```

- **Sample responses**

  XML format

```
<DescribeTaskAttributeResponse>
 <CreationTime>2015-11-23T02:13Z</CreationTime>
 <OperationProgressSet>
  <OperationProgress>
   <RelatedItemSet>
    <RelatedItem>
     <Name>OSSBucket</Name>
     <Value>image-temp</Value>
    </RelatedItem>
    <RelatedItem>
     <Name>OSSObject</Name>
     <Value>MYOSSPRE_m-23f8tcp8y_t-23ym6mvro.vhd</Value>
    </RelatedItem>
    <RelatedItem>
     <Name>ImageFormat</Name>
     <Value>vhd</Value>
    </RelatedItem>
   </RelatedItemSet>
   <ErrorMsg/>
   <ErrorCode/>
   <OperationStatus>Success</OperationStatus>
  </OperationProgress>
 </OperationProgressSet>
 <FinishedTime>2015-11-23T02:19Z</FinishedTime>
 <FailedCount>0</FailedCount>
 <SupportCancel>true</SupportCancel>
 <TotalCount>1</TotalCount>
 <SuccessCount>1</SuccessCount>
 <RequestId>EF0C5969-279B-49C8-AD83-BACCC74DD38C</RequestId>
 <RegionId>cn-hangzhou</RegionId>
 <TaskAction>ExportImage</TaskAction>
 <TaskStatus>Finished</TaskStatus>
 <TaskProcess>100%</TaskProcess>
 <TaskId>t-23ym6mvro</TaskId>
</DescribeTaskAttributeResponse>
```

JSON format

```
{
  "CreationTime": "2015-11-23T02:13Z",
  "OperationProgressSet": {
    "OperationProgress": [
      {
        "RelatedItemSet": {
          "RelatedItem": [
            {
              "Name": "OSSBucket",
              "Value": "image-temp"
            },
            {
              "Name": "OSSObject",
              "Value": "MYOSSPRE_m-23f8tcp8y_t-23ym6mvro.vhd"
            },
            {
              "Name": "ImageFormat",
              "Value": "vhd"
            }
          ]
        },
        "ErrorMsg": "",
        "ErrorCode": "",
        "OperationStatus": "Success"
      }
    ]
  },
  "FinishedTime": "2015-11-23T02:19Z",
  "FailedCount": 0,
  "SupportCancel": true,
  "TotalCount": 1,
  "SuccessCount": 1,
  "RequestId": "4BE2C7FE-C7A4-4675-A153-174E032AABFB",
  "RegionId": "cn-hangzhou",
  "TaskAction": "ExportImage",
  "TaskStatus": "Finished",
  "TaskProcess": "100%",
  "TaskId": "t-23ym6mvro"
}
```

2.1.1.16.3. CancelTask

You can call this operation to cancel a running task.

This operation supports the following task types:

- ImportImage
- ExportImage
- ImportSnapshot
- ExportSnapshot

Request parameters

Request parameter description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this value to CancelTask.
RegionId	String	Yes	The ID of the region.
TaskId	String	Yes	The ID of the task.

Response parameters

This operation returns only common response parameters. For more information, see Common parameters.

Error codes

Error code description

Error code	Error message	HTTP status code	Description
MissingParameter	An input parameter "RegionId" that is mandatory for processing the request is not supplied.	400	The error message returned because the required RegionId parameter is not specified.
MissingParameter	An input parameter "TaskId" that is mandatory for processing the request is not supplied.	400	The error message returned because the required TaskId parameter is not specified.
InvalidRegionId.NotFound	The specified region not found.	400	The error message returned because the specified region ID does not exist.

Error code	Error message	HTTP status code	Description
InvalidTaskId.NotFound	The specified "TaskId" is not found.	400	The error message returned because the specified task ID does not exist.
InvalidTaskId.Task-ActionNotSupport	The specified task action not support.	403	The error message returned because the specified task cannot be canceled.
InvalidTaskId.Incorrect-TaskStatus	The specified task status is not invalid.	403	The error message returned because the specified task is in a state that does not support this operation.
CancelTaskFailed	The task is failed to cancel, Please contact the administrator.	403	The error message returned because the task failed to be canceled. Contact the administrator.

Examples

Sample requests

```
https://ecs.example.com/?Action=CancelTask&RegionId=cn-hangzhou&TaskId=t-23ym6mvro&Common request parameters
```

Sample responses

XML format

```
<CancelTaskResponse>
    <RequestId>4BE2C7FE-C7A4-4675-A153-174E032AABFB</RequestId>
</CancelTaskResponse>
```

JSON format

```
{"RequestId": "4BE2C7FE-C7A4-4675-A153-174E032AABFB"}
```

2.1.1.17. Data types

2.1.1.17.1. AvailableResourceCreationType

Description

The types of available resources.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
ResourceTypes	String	You can create the following types of resources: • Instance: instances • IoOptimized: I/O optimized instances • Disk: disks • VSwitch: VPCs

2.1.1.17.2. AvailableDiskCategoriesType

Description

The available disk categories.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
DiskCategories	String	Disk category • cloud: basic cloud disks and independent basic cloud disks • cloud_ssd: cloud SSD disks

2.1.1.17.3. BandwidthPackageItemType

Description

The information about shared bandwidth packages.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
BandwidthPackageId	String	The ID of a bandwidth package, such as bwp-xxoo123.
RegionId	String	The region ID.
Name	String	The instance name. The name must be 2 to 128 characters in length. It must start with an English character and can contain numbers, periods (.), underscores (_), and hyphens (-). It cannot start with `http://` or `https://`.
Description	String	The description of the instance. The description must be 2 to 256 characters in length. It is displayed in Apsara Stack console. If not specified, this parameter is null. Default value: null. It cannot start with `http://` or `https://`.
ZoneId	String	The zone ID.
GatewayId	String	The ID of the NAT Gateway associated with the bandwidth package.
Bandwidth	String	The bandwidth value. Valid values: 5 to 5000. Unit: Mbit/s.
ISP	String	Only BGP is supported.
PublicIpAddresses	PublicIpAddressSetType	A list of IP addresses. Each IP address has a unique AllocatedId attribute and an IP address attribute.
BusinessStatus	String	• Normal • SecurityLocked (locked because of security risk control).
CreationTime	String	The creation time of the shared bandwidth package. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ.

2.1.1.17.4. DiskItemType

Description

Contains disk information.

Node name

Disk

Subnodes

Node description

Name	Type	Description
DiskId	String	The disk ID.
RegionId	String	The ID of the region to which the disk belongs.
ZoneId	String	The ID of the zone to which the disk belongs.
DiskName	String	The name of the disk.
Description	String	The description of the disk.
Type	String	The type of the disk. Valid values: • system: system disk • data: data disk
Category	String	The category of the disk. Valid values: • cloud: basic cloud disk • cloud_efficiency: ultra cloud disk • cloud_ssd: SSD cloud disk
Size	Integer	The size of the disk. Unit: GB.
ImageId	String	The ID of the image from which the disk is created. It is null unless the disk was created from an image. This value will remain unchanged throughout the lifecycle of the disk.
SourceSnapshotId	String	The ID of the snapshot used to create the disk. It is null if no snapshots are used to create the disk. This value will remain unchanged throughout the lifecycle of the disk.
Portable	String	Indicates whether the disk is detachable. • true: The disk is an independent basic cloud disk that can be attached to and detached from instances within a zone. • false: The disk is not an independent basic cloud disk, and is created and released together with the instance that it is attached to. To attach or detach a disk, you must first check that this attribute of the disk is true. This attribute is set to false for the system disks of the basic cloud disk type and SSD cloud disk type. This attribute cannot be modified.
Status	String	The disk status. Valid values: In_use | Available | Attaching | Detaching | Creating | ReIniting.
OperationLocks	OperationLocksType	The reason why the disk is locked.

Name	Type	Description
InstanceId	String	The ID of the instance to which the disk belongs. It is null unless the disk is in the In_use state.
Device	String	The device information of the instance to which a disk belongs, such as /dev/xvdb. It is null unless the disk is in the In_use state.
DeleteWithInstance	String	• true: When the instance is released, the disk will be released together with it. • false: When the instance is released, the disk will be retained.
DeleteAutoSnapshot	String	Indicates whether automatic snapshots are deleted when a disk is released. Valid values: true | false. Snapshots created by the CreateSnapshot operation or in the console are retained permanently and cannot be deleted based on the value of this parameter.
EnableAutoSnapshot	String	Indicates whether an automatic snapshot policy is enabled for the disk. Valid values: true | false. • true • false
CreationTime	String	The creation time of the disk. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ.
AttachedTime	String	The time when the disk is attached. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ. This parameter is valid only when the disk is in the In_use state.
DetachedTime	String	The time when the disk is detached. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ. This parameter is valid only when the disk is in the Available state.

2.1.1.17.5. DiskSetType

Description

The disk information.

Node name

Disks

Subnodes

Node description

Name	Type	Description
Disk	DiskItemType	A set of DiskItemType data.

2.1.1.17.6. ImageType

Description

The image information.

Node name

Image

Subnodes

Node description

Name	Type	Description
ImageId	String	The image ID.
ImageVersion	String	The image version.
OSType	String	The operating system type. Valid values: • Windows • Linux
Platform	String	The release version of the operating system.
Architecture	String	The system architecture. Valid values: i386 | x86_64.
ImageName	String	The name of the image.
Description	String	The description of the image.
Size	Integer	The size of the image.
ImageOwnerAlias	String	The alias of the image owner. Valid values: • system: public system images • self: custom images • others: images shared by other users
OSName	String	The name of the operating system.
DiskDeviceMappings	DiskDeviceMapping	The description of the system, including disks and snapshots under the image.
Progress	String	The image creation progress. Unit: percent (%).

Name	Type	Description
Status	String	The status of the image. Valid values: • Unavailable • Available • Creating • CreateFailed
CreationTime	String	The creation time of the image. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ.
Usage	String	The referenced resource type. Valid values: instance | none.
IsCopied	String	Indicates whether the image is copied. Valid values: true | false.

2.1.1.17.7. InstanceMonitorDataType

Description

Contains instance monitoring data.

Node name

InstanceMonitorData

Subnodes

Node description

Name	Type	Description
InstanceId	String	The ID of the ECS instance.
CPU	Integer	The CPU utilization. Unit: percent (%).
IntranetRX	Integer	The amount of intranet data traffic received by the ECS instance. Unit: Kbit/s.
IntranetTX	Integer	The amount of intranet data traffic sent by the ECS instance. Unit: Kbit/s.
IntranetBandwidth	Integer	The intranet bandwidth of the ECS instance. Unit: Kbit/s.
InternetRX	Integer	The amount of Internet data traffic received by the ECS instance. Unit: Kbit/s.
InternetTX	Integer	The amount of Internet data traffic sent by the ECS instance. Unit: Kbit/s.
InternetBandwidth	Integer	The Internet bandwidth of the ECS instance. Unit: Kbit/s.

Name	Type	Description
IOPSRead	Integer	The amount of system disk I/O reads. Unit: times/s.
IOPSWrite	Integer	The amount of system disk I/O writes. Unit: times/s.
BPSRead	Integer	The amount of system disk read bandwidth. Unit: Byte/s.
BPSWrite	Integer	The amount of system disk write bandwidth. Unit: Byte/s.
TimeStamp	String	The timestamp generated when the traffic is queried. The timestamp uses UTC and complies with the ISO 8601 standard. The timestamp format is YYYY-MM-DDThh:mmZ.

2.1.1.17.8. InstanceStatusItemType

Description

A set of instance status items.

Node name

InstanceStatus

Subnodes

Node description

Name	Type	Description
InstanceId	String	The ID of the instance.
Status	String	The status of the instance.

2.1.1.17.9. InstanceTypeItemType

Description

The instance type information.

Node name

InstanceType

Subnodes

Node description

Name	Type	Description
InstanceTypeId	String	The ID of the instance type.
CpuCoreCount	Integer	The number of CPU cores.

Name	Type	Description
MemorySize	Double	The memory capacity. Unit: GiB.
InstanceTypeFamily	String	The instance type family.

2.1.1.17.10. IpAddressSetType

Description

Contains a set of IP addresses.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
IpAddress	String	The IP address.

2.1.1.17.11. InstanceStatusSetType

Description

A set of instance status items.

Node name

InstanceStatuses

Subnodes

Node description

Name	Type	Description
InstanceStatus	InstanceStatusItemType	A set of InstanceStatusItemType data.

2.1.1.17.12. NetworkInterfaceType

Description

The information about an ENI.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
NetworkInterfaceId	String	The ID of an ENI.
PrimaryIpAddress	String	The primary private IP address of the ENI.
MacAddress	String	The MAC address of the ENI.

2.1.1.17.13. NetworkInterfaceSet

Description

A set of ENIs.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
NetworkInterfaceId	String	The ID of the ENI.
Status	String	The status of the ENI.
Type	String	The category of the ENI.
VpcId	String	The ID of the VPC.
VSwitchId	String	The VSwitch ID of the specified VPC.
ZoneId	String	The ID of the zone.
AssociatedPublicIp	AssociatedPublicIp	The public IP address of the ENI.
PrivateIpAddress	String	The primary private IP address of the ENI.
PrivateIpSet	PrivateIpSet	A set of private IP addresses.
MacAddress	String	The MAC address of the ENI.
SecurityGroupIds	SecurityGroupIdSetType	The ID of the security group to which the ENI belongs.

Name	Type	Description
NetworkInterfaceName	String	The name of the ENI.
Description	String	The description of the ENI.
InstanceId	String	The ID of the ECS instance to which the ENI is attached.
CreationTime	String	The creation time of the ENI. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ.

2.1.1.17.14. OperationLocksType

Description

The reason why a resource is locked.

Node name

OperationLock

Subnodes

Node description

Name	Type	Description
LockReason	String	The reason why a resource is locked, such as security.

2.1.1.17.15. PermissionSetType

Description

A set of security group rules.

Node name

Permissions

Subnodes

Node description

Name	Type	Description
Permision	PermissionType	A set of PermissionType data.

2.1.1.17.16. PermissionType

Description

The security group rule information.

Node name

Permission

Subnodes

Node description

Name	Type	Description
IpProtocol	String	The IP protocol.
PortRange	String	The port number range.
SourceCidrIp	String	The source IP address segment for Ingress authorization.
SourceGroupId	String	The source security group for ingress authorization.
SourceGroupOwnerAccount	String	The Apsara stack tenant account to which the source security group belongs.
DestCidrIp	String	The destination IP address segment for Egress authorization.
DestGroupId	String	The destination security group for Egress authorization.
DestGroupOwnerAccount	String	The Apsara stack tenant account to which the destination security group belongs.
Policy	String	The authorization policy.
NicType	String	The network type.
Priority	String	The rule priority.
Direction	String	The allowed direction of traffic.
Description	String	The description.

2.1.1.17.17. RegionType

Description

The region information.

Node name

Region

Subnodes

Node description

Name	Type	Description
RegionId	String	The region ID.
LocalName	String	The region name.

2.1.1.17.18. SnapshotType

Description

The snapshot information.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
Snapshotid	String	The snapshot ID.
SnapshotName	String	The name of the snapshot. This parameter is returned only if a snapshot name was specified during creation.
Description	String	The description of the snapshot.
Progress	String	The snapshot creation progress. Unit: percent (%).
SourceDiskId	String	The ID of the source disk. It is retained after the source disk of the snapshot is deleted.
SourceDiskSize	Integer	The capacity of the source disk. Unit: GB.
SourceDiskType	String	The type of the source disk. Valid values: System | Data.
CreationTime	String	The creation time of the source disk. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ.
Status	String	The status of the snapshot. Valid values: progressing | accomplished | failed.

Name	Type	Description
Usage	String	The referenced resource type. Valid values: image | disk | image_disk | none.

2.1.1.17.19. SecurityGroupIdSetType

Description

A set of security group IDs.

Node name

SecurityGroupIds

Subnodes

Node description

Name	Type	Description
SecurityGroupId	String	The ID of the security group.

2.1.1.17.20. SecurityGroupSetType

Description

A set of security groups.

Node name

SecurityGroups

Subnodes

Node description

Name	Type	Description
SecurityGroup	SecurityGroupItemType	A set of SecurityGroupItemType data.

2.1.1.17.21. SecurityGroupItemType

Description

The security group information.

Node name

SecurityGroups

Subnodes

Node description

Name	Type	Description
SecurityGroupId	String	The ID of the security group.
SecurityGroupName	String	The name of the security group.
Description	String	The description of the security group.
VpcId	String	The ID of the VPC to which the security group belongs.
CreationTime	String	The creation time of the security group. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ.

2.1.1.17.22. AutoSnapshotPolicyType

Description

Contains information about automatic snapshot policies.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
AutoSnapshotPolicyId	String	The ID of the automatic snapshot policy.
RegionId	String	The ID of the region to which the automatic snapshot policy belongs.
AutoSnapshotPolicyName	String	The name of the automatic snapshot policy.
TimePoints	String	The point in time at which the snapshot is automatically created. The smallest unit you can specify is hour. Valid values: 0 to 23, corresponding to the 24 hours within the range of 00:00 to 23:00. For example, 1 indicates 01:00. You can specify multiple points in time. The parameter is a JSON-formatted array: ["0", "1", ... "23"]. You can specify a maximum of 24 points in time. Separate multiple time points with commas (,).

Name	Type	Description
RepeatWeekdays	String	The repeat date for the automatic snapshot. This parameter specifies which day of the week that the automatic snapshot is created on. Valid values: 1 to 7, corresponding to the days of the week, with 1 indicating Monday. You can specify multiple dates. The parameter is a JSON-formatted array: ["1", "2", ... "7"].
RetentionDays	Integer	The retention period of the automatic snapshot. Unit: day. • -1: The automatic snapshot is retained permanently. • 1-65536: The automatic snapshot is retained for the specified number of days.
DiskNums	Integer	The number of disks on which the policy is enabled.
OperationLocks	OperationLocksType	The reason why the snapshot is locked.
Status	String	The status of the automatic snapshot policy. Valid values: Creating | Available.
CreationTime	String	The creation time of the automatic snapshot policy. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ.

2.1.1.17.23. AutoSnapshotExecutionStatusType

Description

Returns information about the most recent execution of an automatic snapshot policy.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
SystemDiskExecutionStatus	String	The status of the last execution. Valid values: Standby | Executed | Failed. • Standby: The automatic snapshot policy is configured but no snapshots have been created, or the automatic snapshot policy for system disks is disabled. • Executed: The execution succeeded. • Failed: The execution failed.

Name	Type	Description
DataDiskExecutionStatus	String	The status of the last execution. Valid values: Standby | Executed | Failed. • Standby: The automatic snapshot policy is configured but no snapshots have been created, or the automatic snapshot policy for data disks is disabled. • Executed: The execution succeeded. • Failed: The execution failed.

2.1.1.17.24. DiskDeviceMapping

Description

A list of the mappings between images and snapshots.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
Snapshotid	String	The snapshot ID.
Size	String	The size of the created disk.
Device	String	The device information of the created disk, such as /dev/xvdb.
Format	String	The image format.
ImportOSSBucket	String	The OSS bucket where an imported image is stored.
Importossobject	String	The OSS object corresponding to an imported image file.

2.1.1.17.25. VpcSetType

Description

A set of VPCs.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
VpcId	String	The ID of a VPC.
RegionId	String	The ID of the region to which the VPC belongs.
Status	String	The status of the VPC. Valid values: Pending | Available.
VpcName	String	The name of the VPC. If not specified, this parameter is null. Default value: null. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-). It is displayed in Apsara Stack console. It cannot start with `http://` or `https://`.
VSwitchIds	String	A list of VSwitch IDs.
CidrBlock	String	The CIDR block of the VPC.
VRouterId	String	The ID of the VRouter.
Description	String	The description of the VPC. If not specified, this parameter is null. Default value: null. The description must be 2 to 256 characters in length. It cannot start with `http://` or `https://`.
CreationTime	String	The creation time of the VPC. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ.
IsDefault	Boolean	Indicates whether the VPC is the default private network in the region. Valid values: true | false.
UserCidrs	String	A list of CIDR blocks available to the user.

2.1.1.17.26. EipAddressAssociateType

Description

The EIP binding information.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
AllocationId	String	The ID of an EIP instance.

Name	Type	Description
IpAddress	String	An EIP address.
Bandwidth	Integer	The Internet bandwidth limit of the EIP. Default value: 5 Mbit/s.

2.1.1.17.27. EipAddressSetType

Description

Contains information about elastic IP addresses (EIPs).

Node name

The node name depends on the API that uses the current data type.

Subnodes

Name	Type	Description
RegionId	String	The ID of the region to which the EIP belongs.
IpAddress	String	The EIP.
AllocationId	String	The ID of the EIP instance.
Status	String	The current status of the EIP. Valid values: Associating | Unassociating | InUse | Available.
InstanceType	String	Valid values: EcsInstance | HaVip. The value is null if no resource is bound.
InstanceId	String	The ID of the instance bound to the EIP. If no instances are bound to the EIP, this value is null.
Bandwidth	Integer	The Internet bandwidth limit of the EIP. Default value: 5 Mbit/s.
OperationLocks	OperationLocksType	An array consisting of LockReason strings. If no logs are active, no subnodes will exist.
AllocationTime	String	The time at which the EIP is assigned. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mm:ssZ.

2.1.1.17.28. InstanceAttributesType

Description

Contains information about ECS instance attributes.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
InstanceId	String	The ID of the ECS instance.
InstanceName	String	The name of the ECS instance.
Description	String	The description of the ECS instance.
ImageId	String	The image ID.
RegionId	String	The ID of the region to which the ECS instance belongs.
ZoneId	String	The ID of the zone to which the ECS instance belongs.
CPU	Integer	The number of CPU cores.
Memory	Integer	The memory capacity. Unit: MB.
InstanceType	String	The instance type.
InstanceTypeFamily	String	The instance type family.
HostName	String	The name of the host where the ECS instance resides.
SerialNumber	String	The serial number of the host where the ECS instance resides.
Status	String	The instance status.
SecurityGroupIds	SecurityGroupIdSetType	A set of security groups to which the ECS instance belongs.
PublicIpAddress	IpAddressSetType	The public IP address of the ECS instance. For more information, see IpAddressSetType.
InternetMaxBandwidthIn	Integer	The maximum inbound bandwidth from the Internet.
InternetMaxBandwidthOut	Integer	The maximum outbound bandwidth to the Internet.
CreationTime	String	The creation time of the ECS instance. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mm:ssZ.
VpcAttributes	VpcAttributesType	A set of VPC attributes.
EipAddress	EipAddressAssociateType	A set of EIPs.

Name	Type	Description
InnerIpAddress	IpAddressSetType	The internal IP address of the ECS instance. For more information, see IpAddressSetType.
InstanceNetworkType	String	The network type of the ECS instance.
OperationLocks	OperationLocksType	The operation locks.
DeviceAvailable	String	Indicates whether a new disk can be mounted to the instance. Valid values: True | False.
IoOptimized	String	Indicates whether the ECS instance is I/O optimized. Valid values: True | False.

2.1.1.17.29. VpcAttributesType

Description

Contains the VPC-related attributes of an ECS instance.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
VpcId	String	The ID of the VPC.
VSwitchId	String	The ID of the VSwitch.
PrivateIpAddress	IpAddressSetType	A set of private IP addresses.
NatIpAddress	String	The IP address of the NAT Gateway. This address is used for ECS instances in different networks to communicate with each other.

2.1.1.17.30. DiskMonitorDataType

Description

Contains disk monitoring data.

Node name

DiskMonitorData

Subnodes

Node description

Name	Type	Description
DiskId	String	The disk ID.
IOPSRead	Integer	The disk I/O read operation. Unit: times/s.
IOPSWrite	Integer	The disk I/O write operation. Unit: times/s.
IOPSTotal	Integer	The disk I/O read and write operations. Unit: times/s.
BPSRead	Integer	The disk read bandwidth. Unit: Byte/s.
BPSWrite	Integer	The disk write bandwidth. Unit: Byte/s.
BPSTotal	Integer	The total disk read and write bandwidth. Unit: Byte/s.
TimeStamp	String	The timestamp of the query. The timestamp uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mm:ssZ.

2.1.1.17.31. AccountType

Description

Contains account information.

Node name

Account

Subnodes

Node description

Name	Type	Description
AliyunId	String	The account ID.

2.1.1.17.32. ShareGroupType

Description

Contains information about shared groups.

Node name

ShareGroup

Subnodes

Node description

Name	Type	Description
Group	String	The shared group.

2.1.1.17.33. TagSetItem

Node description

Name	Type	Description
TagKey	String	The key of the tag.
TagValue	String	The value of the tag.
ResourceTypeCount	Array	The number of resources that are bound to the tag. For more information, see ResourceTypeCountItem.

2.1.1.17.34. ResourceTypeCountItem

Node description

Name	Type	Description
ResourceType	String	The resource type.
Count	String	The number of resources of the type that are bound to a specific tag.

2.1.1.17.35. AvailableInstanceTypesType

Description

Contains information about available instance types.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
InstanceTypes	Array	The instance types.

2.1.1.17.36. InstanceTypeFamilyItemType

Description

Contains information about instance type families.

Node name

InstanceTypeFamily

Subnodes

Node description

Name	Type	Description
InstanceTypeFamilyId	String	The ID of the instance type family.
Generation	String	The generation of the instance type family.

2.1.1.17.37. AvailableResourcesType

Description

Contains information about available resources.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
IoOptimized	String	Indicates whether the ECS instance is I/O optimized.
NetworkTypes	String	The supported network types.
InstanceGenerations	Array	The supported instance generations.
InstanceTypeFamilies	Array	The supported families of instance types.
SystemDiskCategories	Array	An array consisting of supported system disk categories.
DataDiskCategories	Array	An array consisting of supported data disk categories.
InstanceTypes	Array	An array consisting of supported instance types.

2.1.1.17.38. TaskType

Description

Contains information about tasks.

Node name

TaskSetType

Subnodes

Node description

Name	Type	Description
TaskId	String	The ID of the task.
Action	String	The operation that you want to perform.
TaskStatus	String	The status of the task. Valid values: • Finished • Processing
SupportCancel	String	Indicates whether a task can be canceled. Valid values: • True • False
CreationTime	String	The creation time of the task. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mm:ssZ.
FinishedTime	String	The completion time of the task. The time uses UTC and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mm:ssZ.

2.1.1.17.39. KeyPairSetType

A set of SSH key pairs.

Node name

The node name depends on the parameter that uses the current data type.

Subnodes

Name	Type	Description
KeyPair	KeyPairItemType	An SSH key pair of the `KeyPairItemType` type.

2.1.1.17.40. KeyPairItemType

The SSH key pair information.

Node name

KeyPairs

Subnodes

Name	Type	Description
KeyPairName	String	The name of the SSH key pair.
KeyPairFingerPrint	String	The fingerprint of the SSH key pair.

2.1.1.17.41. OperationProgressType

Description

The implementation details of an operation task on a resource.

Node name

OperationProgress

Subnodes

Node description

Name	Type	Description
RelatedItemSet	RelatedItemSetType	The resource type information.
OperationStatus	String	The operation status. Valid values: • Processing • Success • Failed
ErrorCode	String	The error code. This parameter is null unless OperationStatus is Failed.
ErrorMsg	String	The error message. This parameter is null unless OperationStatus is Failed.

2.1.1.17.42. RelatedItemType

Description

The related item information.

Node name

RelatedItem

Subnodes

Node description

Name	Type	Description
Name	String	The related item name.
Value	String	The related item value.

2.1.1.17.43. AccessPointSetType

Description

Contains a set of APs. The parameter value is a list of AccessPointType data.

Node name

The node name depends on the API that uses the current data type.

Subnodes

AccessPointType.

2.1.1.17.44. AccessPointType

Description

The access point (AP) information.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
AccessPointId	String	The access point ID.
Type	String	The AP type. Valid value: VPC. A VPC AP allows access to a VPC network through physical connection.

Name	Type	Description
Status	String	The status of the AP. Valid values: • Recommended: The AP is in good state and is recommended for connection. • Hot: The AP is in a normal state, but is connected by a large number of users. • Full: The AP is unavailable for connection because the number of connected users has reached the upper limit.
Name	String	The name of the AP.
Description	String	The description of the AP.
AttachedRegionId	String	The ID of the region where the AP is physically located. If this parameter is not specified, the AP does not belong to any region.
Location	String	The physical location of the AP.
HostOperator	String	The operator of the data center where the AP is located.

2.1.1.17.45. BandwidthPackageSetType

Description

The list of shared bandwidth packages.

Node name

The node name depends on the API that uses the current data type.

Subnodes

An array consisting of BandwidthPackageItemType data.

2.1.1.17.46. ForwardEntrySetType

Description

The list of port forwarding rules.

Node name

The node name depends on the API that uses the current data type.

Subnodes

An array consisting of ForwardEntryItemType data.

2.1.1.17.47. ForwardEntryItemType

Description

The information about port forwarding rules.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
ForwardTableId	String	The ID of the forwarding table to which an entry belongs.
ForwardEntryId	String	The ID of the forwarding entry.
ExternalIp	String	The forwarded IP address. This address must be a public IP address on a NAT Gateway.
ExternalPort	String	The forwarded port number. Valid values: 1 to 65535 | Any.
IpProtocol	String	The protocol type for message forwarding. Valid values: TCP | UDP | Any.
InternalIp	String	The destination IP address for message forwarding. This address must be a private IP address.
InternalPort	String	The destination port number for message forwarding. Valid values: 1 to 65535 | Any.
Status	String	The status of a forwarding entry. Valid values: Pending | Available | Modifying.

2.1.1.17.48. PublicIpAddressSetType

Description

The list of public IP addresses in a shared bandwidth package.

Node name

The node name depends on the API that uses the current data type.

Subnodes

An array consisting of PublicIpAddressItemType data.

2.1.1.17.49. PublicIpAddressItemType

Description

The information about public IP addresses in a shared bandwidth package.

Node name

The node name depends on the API that uses the current data type.

Subnodes

Node description

Name	Type	Description
AllocationId	String	The ID of the public IP address, which is globally unique.
IpAddress	String	The public IP address.

2.1.1.17.50. ZoneType

Description

The zone information.

Node name

Zone

Subnodes

Node description

Name	Type	Description
ZoneId	String	The zone ID.
LocalName	String	The name of the zone in the local language.
AvailableResources	AvailableResourcesType	The available resources. It is an array consisting of AvailableResourcesType data.
AvailableInstanceTypes	AvailableInstanceTypesType	The types of instances that can be created.
AvailableResourceCreation	AvailableResourceCreationType	The types of resources that can be created.
AvailableDiskCategories	AvailableDiskCategoriesType	The available disk categories.

2.1.1.18. Appendix

2.1.1.18.1. Instance types

An instance is the smallest unit in ECS that is capable of providing computing services. The computing capabilities vary with instance type.

The instance type defines the CPU and memory configuration of an instance and determines properties such as CPU model and processing frequency. However, you must combine the instance type with disk category, image, and network type to uniquely identify an instance. The following table describes all instance type families.

Instance type family	Type code	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues	ENIs (including one primary ENI)
n4	ecs.n4.small	1	2.0	None	0.5	5	1	1
	ecs.n4.large	2	4.0	None	0.5	10	1	1
	ecs.n4.xlarge	4	8.0	None	0.8	15	1	2
	ecs.n4.2xlarge	8	16.0	None	1.2	30	1	2
	ecs.n4.4xlarge	16	32.0	None	2.5	40	1	2
	ecs.n4.8xlarge	32	64.0	None	5.0	50	1	2
mn4	ecs.mn4.small	1	4.0	None	0.5	5	1	1
	ecs.mn4.large	2	8.0	None	0.5	10	1	1
	ecs.mn4.xlarge	4	16.0	None	0.8	15	1	2
	ecs.mn4.2xlarge	8	32.0	None	1.2	30	1	2
	ecs.mn4.4xlarge	16	64.0	None	2.5	40	1	2
	ecs.mn4.8xlarge	32	128.0	None	5.0	50	2	8
xn4	ecs.xn4.small	1	1.0	None	0.5	5	1	1
	ecs.e4.small	1	8.0	None	0.5	5	1	1
	ecs.ce4.xlarge	2	16.0	None	0.5	10	1	1

Instance type family	Type code	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues	ENIs (including one primary ENI)
e4	ecs.ce4.xlarge	4	32.0	None	0.8	15	1	2
	ecs.e4.2xlarge	8	64.0	None	1.2	30	1	3
	ecs.e4.4xlarge	16	128.0	None	2.5	40	1	8
sn1ne	ecs.sn1ne.large	2	4.0	None	1.0	30	2	2
	ecs.sn1ne.xlarge	4	8.0	None	1.5	50	2	3
	ecs.sn1ne.2xlarge	8	16.0	None	2.0	100	4	4
	ecs.sn1ne.3xlarge	12	24.0	None	2.5	130	4	6
	ecs.sn1ne.4xlarge	16	32.0	None	3.0	160	4	8
	ecs.sn1ne.6xlarge	24	48.0	None	4.5	200	6	8
	ecs.sn1ne.8xlarge	32	64.0	None	6.0	250	8	8
	ecs.sn2ne.large	2	8.0	None	1.0	30	2	2
	ecs.sn2ne.xlarge	4	16.0	None	1.5	50	2	3
	ecs.sn2ne.2xlarge	8	32.0	None	2.0	100	4	4

Instance type family	Type code	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues	ENIs (including one primary ENI)
sn2ne	ecs.sn2ne.3xlarge	12	48.0	None	2.5	130	4	6
	ecs.sn2ne.4xlarge	16	64.0	None	3.0	160	4	8
	ecs.sn2ne.6xlarge	24	96.0	None	4.5	200	6	8
	ecs.sn2ne.8xlarge	32	128.0	None	6.0	250	8	8
	ecs.sn2ne.14xlarge	56	224.0	None	10.0	450	14	8
se1ne	ecs.se1ne.large	2	16.0	None	1.0	30	2	2
	ecs.se1ne.xlarge	4	32.0	None	1.5	50	2	3
	ecs.se1ne.2xlarge	8	64.0	None	2.0	100	4	4
	ecs.se1ne.3xlarge	12	96.0	None	2.5	130	4	6
	ecs.se1ne.4xlarge	16	128.0	None	3.0	160	4	8
	ecs.se1ne.6xlarge	24	192.0	None	4.5	200	6	8
	ecs.se1ne.8xlarge	32	256.0	None	6.0	250	8	8

Instance type family	Type code	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues	ENIs (including one primary ENI)
	ecs.se1ne.14xlarge	56	480.0	None	10.0	450	14	8
se1	ecs.se1.large	2	16.0	None	0.5	10	1	2
	ecs.se1.xlarge	4	32.0	None	0.8	20	1	3
	ecs.se1.2xlarge	8	64.0	None	1.5	40	1	4
	ecs.se1.4xlarge	16	128.0	None	3.0	50	2	8
	ecs.se1.8xlarge	32	256.0	None	6.0	80	3	8
	ecs.se1.14xlarge	56	480.0	None	10.0	120	4	8
ebmg5	ecs.ebmg5.24xlarge	96	384.0	None	10.0	400	8	32
i2	ecs.i2.xlarge	4	32.0	1 × 894	1.0	50	2	3
	ecs.i2.2xlarge	8	64.0	1 × 1,788	2.0	100	2	4
	ecs.i2.4xlarge	16	128.0	2 × 1,788	3.0	150	4	8
	ecs.i2.8xlarge	32	256.0	4 × 1,788	6.0	200	8	8
	ecs.i2.16xlarge	64	512.0	8 × 1788	10.0	400	16	8
	ecs.d1.2xlarge	8	32.0	4 × 5,500	3.0	30	1	4
	ecs.d1.3xlarge	12	48.0	6 × 5,500	4.0	40	1	6

Instance type family	Type code	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues	ENIs (including one primary ENI)
d1	ecs.d1.4xlarge	16	64.0	8 × 5,500	6.0	60	2	8
	ecs.d1.6xlarge	24	96.0	12 × 5,500	8.0	80	2	8
	ecs.d1-c8d3.8xlarge	32	128.0	12 × 5,500	10.0	100	4	8
	ecs.d1.8xlarge	32	128.0	16 × 5,500	10.0	100	4	8
	ecs.d1-c14d3.14xlarge	56	160.0	12 × 5,500	17.0	180	6	8
	ecs.d1.14xlarge	56	224.0	28 × 5,500	17.0	180	6	8
sccg5ib	ecs.sccg5ib.24xlarge	96	384.0	None	10.0	450	8	32
scch5ib	ecs.scch5ib.16xlarge	64	192.0	None	10.0	450	8	32
re5	ecs.re5.15xlarge	60	990.0	None	10.0	100	16	8
	ecs.re5.30xlarge	120	1980.0	None	15.0	200	16	15
	ecs.re5.45xlarge	180	2,970.0	None	30.0	450	16	15
	ecs.sn1.medium	2	4.0	None	0.5	10	1	2
	ecs.sn1.large	4	8.0	None	0.8	20	1	3
	ecs.sn1.xlarge	8	16.0	None	1.5	40	1	4

sn1 Instance type family	Type code	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues	ENIs (including one primary ENI)
	ecs.sn1.3xlarge	16	32.0	None	3.0	50	2	8
	ecs.sn1.7xlarge	32	64.0	None	6.0	80	3	8
sn2	ecs.sn2.medium	2	8.0	None	0.5	10	1	2
	ecs.sn2.large	4	16.0	None	0.8	20	1	3
	ecs.sn2.xlarge	8	32.0	None	1.5	40	1	4
	ecs.sn2.3xlarge	16	64.0	None	3.0	50	2	8
	ecs.sn2.7xlarge	32	128.0	None	6.0	80	3	8
	ecs.sn2.14xlarge	56	224.0	None	10.0	120	4	8

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues	ENIs (including one primary ENI)	FPGA
	ecs.f1-c8f1.2xlarge	8	60.0	None	3.0	40	4	4	Intel ARRIA 10 GX 1150

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues	ENIs (including one primary ENI)	FPGA
f1	ecs.f1-c8f1.4xlarge	16	120.0	None	5.0	100	4	8	2 × Intel ARRIA 10 GX 1150
	ecs.f1-c28f1.7xlarge	28	112.0	None	5.0	200	8	8	Intel ARRIA 10 GX 1150
	ecs.f1-c28f1.14xlarge	56	224.0	None	10.0	200	14	8	2 × Intel ARRIA 10 GX 1150
f3	ecs.f3-c16f1.4xlarge	16	64.0	None	5.0	100	4	8	1 × Xilinx VU 9P
	ecs.f3-c16f1.8xlarge	32	128.0	None	10.0	200	8	8	2 × Xilinx VU 9P
	ecs.f3-c16f1.16xlarge	64	256.0	None	20.0	200	16	8	4 × Xilinx VU 9P

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.gn5-c4g1.xlarge	4	30.0	440	3.0	30	1
	ecs.gn5-c8g1.2xlarge	8	60.0	440	3.0	40	1

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.gn5-c4g1.2xlarge	8	60.0	880	5.0	100	2
	ecs.gn5-c8g1.4xlarge	16	120.0	880	5.0	100	4

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
gn5	ecs.gn5-c28g1.7xlarge	28	112.0	440	5.0	100	8
	ecs.gn5-c8g1.8xlarge	32	240.0	1,760	10.0	200	8

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.gn5-c28g1.14xlarge	56	224.0	880	10.0	200	14
	ecs.gn5-c8g1.14xlarge	54.	480.0	3,520	25.0	400	14

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.gn4-c4g1.xlarge	4	30.0	None	3.0	30	1
	ecs.gn4-c8g1.2xlarge	8	30.0	None	3.0	40	1

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
gn4	ecs.gn4.8xlarge	32	48.0	None	6.0	80	3
	ecs.gn4-c4g1.2xlarge	8	60.0	None	5.0	50	1

gn4

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.gn4-c8g1.4xlarge	16	60.0	None	5.0	50	1
	ecs.gn4.14xlarge	56	96.0	None	10.0	120	4

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.ga1.xlarge	4	10.0	1 × 87	1.0	20	1
	ecs.ga1.2xlarge	8	20.0	1 × 175	1.5	30	1

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
ga1	ecs.ga1.4xlarge	16	40.0	1 × 350	3.0	50	2
	ecs.ga1.8xlarge	32	80.0	1 × 700	6.0	80	3

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.ga1.14xlarge	56	160.0	1 × 1,400	10.0	120	4
	ecs.gn5i-c2g1.large	2	8.0	None	1.0	10	2

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.gn5i-c4g1.xlarge	4	16.0	None	1.5	20	2
	ecs.gn5i-c8g1.2xlarge	8	32.0	None	2.0	40	4

gn5i Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.gn5i-c16g1.4xlarge	16	64.0	None	3.0	80	4
	ecs.gn5i-c16g1.8xlarge	32	128.0	None	6.0	120	8

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.gn5i-c28g1.14xlarge	56	224.0	None	10.0	200	14
	ecs.gn5e-c11g1.3xlarge	10	58.0	None	2.0	15	1

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
gn5e	ecs.gn5e-c11g1.5xlarge	22	116.0	None	4.0	30	1
	ecs.gn5e-c11g1.11xlarge	44	232.0	None	6.0	60	2

Instance type family	Instance type	CPU (core)	Memory (GiB)	Local storage (GiB)	Bandwidth (inbound or outbound in Gbit/s)	Network packet processing (inbound or outbound in 10,000 PPS)	NIC queues
	ecs.gn5e-c11g1.22xlarge	88	464.0	None	10.0	120	4

The following instance types are only applicable to environments that are upgraded from Apsara Stack V2 to V3.

Instance type family	Instance type	CPU (core)	Memory (GiB)
n1	ecs.n1.tiny	1	1.0
	ecs.n1.small	1	2.0
	ecs.n1.medium	2	4.0
	ecs.n1.large	4	8.0
	ecs.n1.xlarge	8	16.0

Instance type family	Instance type	CPU (core)	Memory (GiB)
	ecs.n1.3xlarge	16	32.0
	ecs.n1.7xlarge	32	64.0
n2	ecs.n2.small	1	4.0
	ecs.n2.medium	2	8.0
	ecs.n2.large	4	16.0
	ecs.n2.xlarge	8	32.0
	ecs.n2.3xlarge	16	64.0
	ecs.n2.7xlarge	32	128.0
e3	ecs.e3.small	1	8.0
	ecs.e3.medium	2	16.0
	ecs.e3.large	4	32.0
	ecs.e3.xlarge	8	64.0
	ecs.e3.3xlarge	16	128.0
c1	ecs.c1.small	8	8.0
	ecs.c1.large	8	16.0
c2	ecs.c2.medium	16	16.0
	ecs.c2.large	16	32.0
	ecs.c2.xlarge	16	64.0
m1	ecs.m1.medium	4	16.0
	ecs.m1.xlarge	8	32.0
m2	ecs.m2.medium	4	32.0
s1	ecs.s1.small	1	2.0
	ecs.s1.medium	1	4.0
	ecs.s1.large	1	8.0
s2	ecs.s2.small	2	2.0
	ecs.s2.large	2	4.0
	ecs.s2.xlarge	2	8.0

Instance type family	Instance type	CPU (core)	Memory (GiB)
	ecs.s2.2xlarge	2	16.0
s3	ecs.s3.medium	4	4.0
	ecs.s3.large	4	8.0
t1	ecs.t1.small	1	1.0

2.1.1.18.2. Glossary

This topic describes the terms that you may encounter in ECS API operations.

Terms

Description

Term	Definition	Description
Instance	ECS instance, instance for short	An ECS instance is a virtual computer that is emulated on a physical server.
Region	Region	A region is the geographic location where resources are located. Each region contains a group of zones.
Zone	Zone	A zone is a physical area that operates an independent network and has its own power supply. The network latency is shorter for communication between ECS instances in the same zone. Zones within the same region can access each other, but faults which occur in one zone are isolated from other zones.
Image	Image file, image for short	An image file contains data for an operating system and applications. You can select an image to initialize an ECS instance. Before you create an instance, ensure that available images exist. All of the system disk contents of a newly created instance, including its OS and software configurations, are copied from the image. To create instances of different operating systems, you must select different image files.
Disk	Disk	A disk is the storage device used by an instance.
Snapshot	Snapshot	A snapshot is a backup copy of data on a disk for a certain point in time. A snapshot can be used to restore disk data and create custom images.
IP	IP address	A public IP address on the Internet.
SecurityGroup	Security group	A security group is a group of instances to which a set of security policies will be applied to. An instance must belong to at least one security group. The security policies of a security group apply to all instances in the group.

Term	Definition	Description
CIDR	Classless Inter-Domain Routing (CIDR)	CIDR is an Internet address allocation scheme. Compared with the Class A, B, and C addressing schemes, CIDR is much more efficient. For example, to convert the IP address segment 125.203.96.0 - 125.203.127.255 into CIDR format, find the same first 19 bits: 125.203.0110 0000.0000 0000 to 125.203.0111 1111.1111 1111, which can be represented in 125.203.96.0/19.

Limits

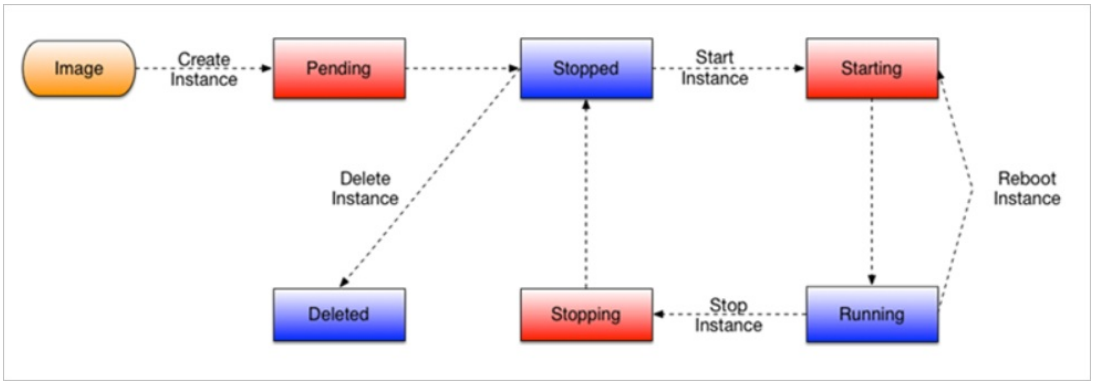
- In ECS, the number of instances, security groups, and other resources that can be used by each user is limited.
- Specifications such as the instance type, number of disks that can be mounted on each instance, disk capacity, and number of disk snapshots are also limited.

2.1.1.18.3. Instance statuses

Statuses

Status	Description
Pending	The instance is being created.
Stopped	The instance is stopped.
Starting	The instance is starting.
Running	The instance is running.
Stopping	The instance is being stopped.

Instance state diagram



2.1.1.18.4. Common errors

Error codes

Error code	HTTP status code	Error message
IdempotentParameterMismatch	400	The request is retried with updated parameters.
IllegalTimestamp	400	The input parameter "Timestamp" that is mandatory for processing this request is not supplied.
IncompleteSignature	400	The request signature does not conform to Aliyun standards.
InvalidAccessKeyId.NotFound	400	The Access Key ID provided does not exist in our records.
InvalidOwner	400	OwnerId and OwnerAccount can't be used at one API access.
InvalidOwnerId	400	The specified OwnerId is not valid.
InvalidOwnerAccount	400	The specified OwnerAccount is not valid.
InvalidParamater	400	The specified parameter "SignatureMethod" is not valid.
InvalidParamater	400	The specified parameter "SignatureVersion" is not valid.
InvalidParameter	400	The specified parameter "Action or Version" is not valid.
InvalidParameter	400	The specified parameter is not valid.
InvalidParameter.IsNull	400	The required parameter must be not null.
MissingParameter	400	The input parameter "Action" that is mandatory for processing this request is not supplied.
MissingParameter	400	The input parameter "AccessKeyId" that is mandatory for processing this request is not supplied.
MissingParameter	400	An input parameter "Signature" that is mandatory for processing the request is not supplied.
MissingParameter	400	The input parameter "Timestamp" that is mandatory for processing this request is not supplied. supplied.
MissingParameter	400	The input parameter "Version" that is mandatory for processing this request is not supplied.

Error code	HTTP status code	Error message
SignatureNonceUsed	400	The request signature nonce has been used.
Throttling	400	You have made too many requests within a short time; your request is denied due to request throttling.
UnsupportedParameter	400	The parameter is unsupported.
UnknownError	400	The request processing has failed due to some unknown error.
Forbidden.AccessKeyDisabled	403	The Access Key is disabled.
Forbidden.NotSupportRAM	403	This action does not support accessed by RAM mode.
Forbidden.RAM	403	User not authorized to operate the specified resource, or this API doesn't support RAM.
Forbidden.RiskControl	403	This operation is forbidden by Aliyun Risk Control system.
Forbidden.SubUser	403	The specified action is not available for you.
Forbidden.Unauthorized	403	User not authorized to operate on the specified resource.
InvalidAccount.NotFound	403	The specified Account does not exist.
InvalidAction	403	The specified action is not valid.
InvalidIdempotenceParameter.Mismatch	403	The specified parameters are different from before.
InvalidParameter.OwnerAccount	403	OwnerAccount is Invalid.
InvalidParameter.ResourceOwnerAccount	403	ResourceOwnerAccount is Invalid.
LastTokenProcessing	403	The last token request is processing.
MissingParameter	403	The input parameter OwnerId, OwnerAccount that is mandatory for processing this request is not supplied.
RealNameAuthenticationError	403	Your account has not passed the real-name authentication yet.
UnsupportedHTTPMethod	403	This http method is not supported.

Error code	HTTP status code	Error message
InvalidDiskId.NotFound	404	The specified DiskId does not exist.
InvalidImageId.NotFound	404	The specified ImageId does not exist.
InvalidInstanceId.NotFound	404	The specified InstanceId does not exist.
InvalidRegionId.NotFound	404	The specified RegionId does not exist.
InvalidSecurityGroupId.NotFound	404	The specified SecurityGroupId does not exist.
InvalidSnapshotId.NotFound	404	The specified SnapshotId does not exist.
OperationConflict	409	Request was denied due to conflict with a previous request.
InternalError	500	The request processing has failed due to some unknown error, exception or failure.
ServiceUnavailable	500	The request has failed due to a temporary failure of the server.
ServiceUnavailable.RegionMaintaining	503	System maintenance is in progress on the selected region, please wait a few minutes before trying again.

2.1.1.18.5. Disk categories

Disk types

Disk type	Category	Maximum capacity of a disk
Basic disk	cloud	2,000 GiB
Ultra disk	cloud_efficiency	32,768 GiB
SSD disk	cloud_ssd	32,768 GiB

2.1.1.18.6. How to ensure idempotency

If a request timeout or internal server error occurs when you call CreateInstance to create an ECS instance, the client may attempt to resend the request. You can specify the ClientToken parameter to prevent the server from creating redundant instances in these cases. The ClientToken parameter ensures idempotency of the request.

A ClientToken is a unique and case-sensitive string generated by the client. It cannot exceed 64 ASCII characters in length.

If you use the same ClientToken for multiple CreateInstance operations, the server will return identical responses that contain the same InstanceId parameter. Therefore, if an error occurs during an instance creation request, you can retry the creation request using the same ClientToken as the failed request. This ensures that only one ECS instance is created and that it assigned to a specific InstanceId.

If you specify a ClientToken that is in use with different request parameters than previously used, ECS will return the IdempotentParameterMismatch error code. You must change the SignatureNonce, Timestamp, and Signature values when calling the operation again. This is because ECS uses SignatureNonce to prevent replay attacks and Timestamp to mark the time of each request. Each new request must have different SignatureNonce and Timestamp values, which changes the Signature value.

Typically, if a 500 (InternalError) or 503 (ServiceUnavailable) error code is returned or no responses are returned, you must retry operations. If an operation is retried after a response code of 200 is returned, an identical response will be returned but the server status will not be affected. If a 4xx error code is returned and *try it later* does not appear in the error message, attempts to retry the operation will fail.

2.1.1.18.7. API responses when an instance is locked for security reasons

Note: If a disk is in the In_use state, responses of operations related to the disk are subject to the OperationLocks of the instance. In other cases, OperationLocks can be ignored.

When DescribeInstanceAttribution returns the OperationLocks parameter with LockReason: security, the instance is locked for security reasons.

Operations and responses

Operation	Response
AllocatePublicIpAddress	Error
AttachDisk	Error
AuthorizeSecurityGroup	Normal logic
CreateDisk	Normal logic
CreateImage	Normal logic
CreateInstance	-
CreateSecurityGroup	Normal logic
CreateSnapshot	Error (only for disks that are mounted to the current instance and are in the In_use state)
DeleteDisk	Normal logic
DeleteImage	Normal logic
DeleteInstance	Normal logic

Operation	Response
DeleteSecurityGroup	Normal logic
DeleteSnapshot	Normal logic
DescribeAutoSnapshotPolicy	Normal logic
DescribeDisks	Normal logic
DescribeImages	Normal logic
DescribeInstanceAttribute	Normal logic
DescribeInstanceStatus	Normal logic
DescribeInstanceTypes	Normal logic
DescribeRegions	Normal logic
DescribeSecurityGroupAttribute	Normal logic
DescribeSecurityGroups	Normal logic
DescribeSnapshotAttribute	Normal logic
DescribeSnapshots	Normal logic
DescribeZones	Normal logic
DetachDisk	Error
JoinSecurityGroup	Error
LeaveSecurityGroup	Error
ModifyAutoSnapshotPolicy	Normal logic
ModifyDiskAttribute	Normal logic
ModifyInstanceAttribute	Error
RebootInstance	Error
ReInitDisk	Error when the disk is in the In_use state. Normal logic when the disk is in other states.
ReplaceSystemDisk	Normal logic
ResetDisk	Error
RevokeSecurityGroup	Normal logic
StartInstance	Error

Operation	Response
StopInstance	Error

2.1.1.18.8. ISO 8601 date and time formats

ISO 8601 Data elements and interchange formats – Information interchange – Representation of dates and times is an international standard covering the exchange of date- and time-related data. It was issued by the International Organization for Standardization (ISO). ECS open APIs adopt the ISO 8601 standard date and time formats.

2.1.2. SDK reference

2.1.2.1. Java SDK

2.1.2.1.1. Quick start

This topic describes how to obtain and use the *ECS* Java SDK.

Environment preparation

- Before using the Java SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to obtain and view your AccessKey in Apsara Stack console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.
- The Apsara Stack Java SDK requires JDK V1.6 and later.

Install the Java SDK

If you use Apache Maven to manage Java projects, you need only to import the JAR file to *pom.xml* of the project.

To use the SDK, you must install the SDK core library and the service SDK.

The version number of the SDK core library is 3.7.1. The version number of the *ECS* SDK is *3.6.0*.

```
<dependencies>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-sdk-core</artifactId>
      <version>3.7.1</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-core-3.7.1.jar</systemPath>
    </dependency>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-ecs</artifactId>
      <version>2.6.0</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-dfs-1.0.jar</systemPath>
    </dependency>
  </dependencies>
```

Use the Java SDK

The following example shows how to use the Apsara Stack Java SDK:

1. Create a DefaultAcsClient instance and initialize it.
2. Create an API request and configure its parameters.
3. Initiate the request and handle the response or exceptions.

```
package com.testprogram;
 import com.aliyuncs.profile.DefaultProfile;
 import com.aliyuncs.DefaultAcsClient;
 import com.aliyuncs.IAcsClient;
 import com.aliyuncs.exceptions.ClientException;
 import com.aliyuncs.exceptions.ServerException;
 import com.aliyuncs.ecs.model.v20140526.*;
 public class Main {
    public static void main(String[] args) {
       // Create a DefaultAcsClient instance and initialize it.
       DefaultProfile profile = DefaultProfile.getProfile(
          "<your-region-id>",         // Your region ID.
          "<your-access-key-id>",     // Your AccessKey ID.
          "<your-access-key-secret>"); // Your AccessKey Secret.
       // Set the endpoint of the current service.
      profile.addEndpoint("your-region-id", "your-region-id", "product", "endpoint");
       IAcsClient client = new DefaultAcsClient(profile);
       // Create an API request and configure its parameters.
       DescribeInstancesRequest request = new DescribeInstancesRequest();
       request.setPageSize(10);
       // Initiate the request and handle the response or exception.
       DescribeInstancesResponse response;
       try {
          response = client.getAcsResponse(request);
          for (DescribeInstancesResponse.Instance instance:response.getInstances()) {
             System.out.println(instance.getPublicIpAddress());
          }
       } catch (ServerException e) {
          e.printStackTrace();
       } catch (ClientException e) {
          e.printStackTrace();
       }
    }
 }
```

2.1.2.1.2. Use the Java SDK

2.1.2.2. Python SDK

2.1.2.2.1. Quick start

This topic describes how to obtain and use the *ECS* Python SDK.

Environment preparation

- Before using the Python SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey in Apsara Stack console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.

Install the Python SDK

To install the Python SDK, perform the following operations:

1. Install the SDK core library.
   - If you are using Python V2.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core
     ```

   - If you are using Python V3.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core-v3
     ```

2. Install the *ECS* SDK.

   The following code shows how to install the ECS SDK:

   ```
   pip install aliyun-python-sdk-ecs
   ```

Call the Python SDK

The following example shows how to call the Python SDK:

1. Create a client instance. When creating the client instance, you must obtain the Region ID, AccessKey ID, and AccessKey Secret.
2. Create an API request and configure its parameters.
3. Initiate the request and handle the response or exceptions.

```
#! /usr/bin/env python
#coding=utf-8

from aliyunsdkcore import client
from aliyunsdkcore.profile import region_provider
from aliyunsdkecs.request.v20140526 import DescribeInstancesRequest

# global config
region_id = 'xxxxx'
secret_id = 'xxxxx'
secret_key = 'xxxxx'

# product config
product_name = 'ecs'
endpoint = 'ecs.example.com'

# create client
client.region_provider.modify_point(product_name, region_id, endpoint)
clt = client.AcsClient(secret_id, secret_key, region_id)

# setup request
request = DescribeInstancesRequest.DescribeInstancesRequest()
request.set_accept_format('json')

# get response
response = clt.do_action_with_exception(request)

print response
```

2.1.2.2.2. Use the Python SDK

2.1.2.3. PHP SDK

2.1.2.3.1. Quick start

The Apsara Stack PHP SDK allows you to access *ECS* without performing complex programming operations. This topic describes how to obtain and use the Apsara Stack PHP SDK.

Environment preparation

- Before using the PHP SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey in Apsara Stack console, see Obtain an AccessKey pair.

- Obtain the service endpoint. For more information, see Obtain an endpoint.
- The Apsara Stack PHP SDK applies to PHP V5.3, 5.4 5.5, 5.6, 7.0, and 7.1. You can run the **php -v** command to obtain the current PHP version number.

Install the PHP SDK

To install the PHP SDK, perform the following operations:

1. Download the PHP SDK source code from Apsara Stack official website.
2. Add the PHP SDK reference to your code.

   For example, if the PHP SDK is downloaded to `/path/to/aliyun-openapi-php-sdk`, use the following command:

   ```
   require_once '/path/to/aliyun-openapi-php-sdk/aliyun-php-sdk-core/Config.php';
   ```

Use the PHP SDK

The following example shows how to use the Apsara Stack PHP SDK:

1. Create a DefaultAcsClient instance and initialize it.

   When you create and initialize a DefaultAcsClient instance, you must provide the values of Region ID, AccessKey ID, and AccessKey Secret.
2. Create an API request and configure its parameters.
3. Initiate the request and handle the response or exceptions.

```
<?php

use Ecs\Request\V20140526\DescribeInstancesRequest;

# Create a DefaultAcsClient instance and initialize it.
$clientProfile = DefaultProfile::getProfile(
   "<your-region-id>",              # Your region ID.
   "<your-access-key-id>",          #  Your AccessKey ID.
   "<your-access-key-secret>"       # Your AccessKey Secret.
);
$client = new DefaultAcsClient($clientProfile);
# Set the endpoint of the current service.
$profile->endpoint ="your-region-id", "your-region-id", "product", "endpoint";

# Create an API request and configure its parameters.
$request = new DescribeInstancesRequest();
$request->setPageSize(10);

# Initiate the request and handle the response.
try {
   $response = $client->getAcsResponse($request);
   print_r($response);
} catch(ServerException $e) {
   print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
} catch(ClientException $e) {
   print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
}
? >
```

2.1.2.4. Go SDK

2.1.2.4.1. Quick start

The Apsara Stack Go SDK allows you to access *ECS* without performing complex programming operations. This topic describes how to obtain and use the Apsara Stack Go SDK.

Environment preparation

- Before using the Go SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey in Apsara Stack console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.

Install the Go SDK

1. Download the Go SDK source code from Apsara Stack official website.
2. Extract the source code to the directory specified by *GO_PATH*.

Use the Go SDK

The following example shows how to use the Apsara Stack Go SDK:

1. Create a client instance.
2. Create an API request and configure its parameters.
3. Initiate the request and handle the response or exceptions.

```
package main

import (
    "github.com/aliyun/alibaba-cloud-sdk-go/services/ecs"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "fmt"
)

func main() {
    // Create an ecsClient instance.
    ecsClient, err := ecs.NewClientWithAccessKey(
        "<your-region-id>",           // Your region ID.
        "<your-access-key-id>", // Your AccessKey ID.
        "<your-access-key-secret>") // Your AccessKey Secret.
    if err ! = nil {
        // Handle exceptions.
        panic(err)
    }
   // Set the endpoint of the current service.
    request.Domain = "endpoint"
    // Create an API request and configure its parameters.
    request := ecs.CreateDescribeInstancesRequest()
    // Set request.PageSize to 10.
    request.PageSize = requests.NewInteger(10)
    // Initiate the request and handle exceptions.
    response, err := ecsClient.DescribeInstances(request)
    if err ! = nil {
        // Handle exceptions.
        panic(err)
    }
    fmt.Println(response)
}
```

2.1.2.4.2. Use the Go SDK

2.1.2.5. .NET SDK

2.1.2.5.1. Quick start

The Apsara Stack .NET SDK allows you to access *ECS* without performing complex programming operations. This topic describes how to obtain and call the Apsara Stack .NET SDK.

Environment preparation

- Before using the .NET SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey in Apsara Stack Operations Console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.
- The Apsara Stack .NET SDK applies to .NET Framework 4.0 and later.

Install the Apsara Stack .NET SDK

To call the SDK of a service, you must install the SDK core library and the SDK of the service. For example, to call the *ECS* SDK, you must obtain and install both the *ECS* SDK and its core library. You can use one of the following methods to install the .NET SDK:

- Add DLL reference
  i. Download the compressed package containing a DLL file from .NET SDK release list, and decompress it to obtain the DLL file.
  ii. Right-click your project in Solution Explorer of Visual Studio and choose **Reference** from the shortcut menu.
  iii. In the shortcut menu, click **Add Reference**.
  iv. In the dialog box that appears, click **Browse**. Then select the downloaded DLL file and click **Confirm**.
- Add project reference
  i. Visit Apsara Stack official website to download the .NET SDK source code.
  ii. Find the *aliyun-net-openapi-XXX* subfolder in the downloaded folder, and then locate the \ *.*csproj* file. It is the .NET project file. For example, in the `aliyun-net-openapi-ecs` sub-folder, there is a file named `aliyun-net-sdk-ecs.csproj` .
  iii. In Visual Studio, right-click your solution.
  iv. Choose **Add** > **Existing Projects**.
  v. In the dialog box that appears, select the .NET project file (such as `aliyun-net-sdk-ecs.csproj`) from the downloaded source code, and click **Open**.
  vi. Right-click your project and choose **Reference** > **Add reference** from the shortcut menu.

Call the .NET SDK

The following code shows how to call the .NET SDK:

1. Create a DefaultAcsClient instance and initialize it.

2. Create an API request and set its parameters.
3. Initiate the request and process the response or exceptions.

```
using Aliyun.Acs.Core;
using Aliyun.Acs.Core.Profile;
using Aliyun.Acs.Core.Exceptions;
using Aliyun.Acs.Ecs.Model.V20140526;

class TestProgram
{
   static void Main(string[] args)
   {
      // Create a client to initiate a request.
      IClientProfile profile = DefaultProfile.GetProfile(
         "<your-region-id>",
         "<your-access-key-id>",
         "<your-access-key-secret>");
// Set the endpoint of the current service.
     profile.setEndpoint("your-region-id", "your-region-id", "product", "endpoint");
 DefaultAcsClient client = new DefaultAcsClient(profile);
      try
      {
         // Create a request.
         DescribeInstancesRequest request = new DescribeInstancesRequest();
         request.PageSize = 10;
         // Initiate the request and obtain the response.
         DescribeInstancesResponse response = client.GetAcsResponse(request);
         System.Console.WriteLine(response.TotalCount);
      }
      catch (ServerException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
      catch (ClientException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
   }
}
```

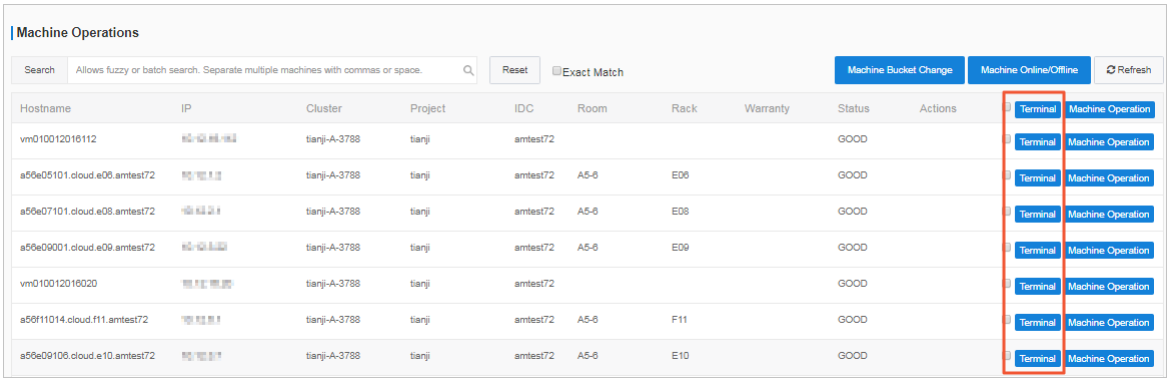
2.1.2.5.2. Use the .NET SDK

2.1.3. Obtain an endpoint

You can obtain the product endpoint in Apsara Stack Operations.

Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms > Apsara Stack Operations > Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. Choose **Operations > Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the command **curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration"** to obtain JSON data.

7. Obtain the *ECS* endpoint based on the ID (*ecs-yaochi*) and the key value (*ecs.openapi.endpoint*) of *ECS*.

2.1.4. Obtain an AccessKey pair

You can obtain the AccessKey pair on the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**. The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.2. Container Service

2.2.1. Container Service API invocation

2.2.1.1. Overview

To use the APIs provided by Container Service, you can send HTTP requests to the endpoint of Container Service APIs and include specific parameters in the requests. The system returns a response after processing the request.

1. Common parameters
2. Request structure
3. Response parameters
4. Sign API requests

2.2.1.2. Common parameters

Common request headers

Common parameters are required in all API calls.

Name	Description	Required
Authorization	The authentication information used to check the authenticity of a request. Format: `AccessKeyId:Signature`.	Yes
Content-Length	The length of the request content defined by RFC 2616.	Yes
Content-Type	The type of the request content defined by RFC 2616.	Yes
Content-MD5	The 128-bit MD5 hash value of the request body represented as a base64 string. We recommend that you specify this parameter to prevent request tampering.	Yes
Date	The timestamp when the request was sent. Currently, only GMT format is supported. If the difference between the timestamp when the request was sent and the timestamp when the request was received exceeds 15 minutes, the request is deemed invalid.	Yes
Host	The target host of the request. For example, *diku.aliyuncs.com*.	Yes
Accept	The return value type required by the client. Valid values: *application/json* or *application/xml*.	Yes
x-acs-version	The API version. The current version is *2015-12-15*.	Yes
x-acs-region-id	The region where the Container Service server is located.	Yes
x-acs-signature-nonce	A unique random number. This parameter is used to prevent replay attacks. A different random number is required for each request.	Yes
x-acs-signature-method	The signature algorithm. Currently, only *HMAC-SHA1* is supported.	Yes

Example

```
GET /clusters HTTP/1.1
Host: cs.aliyuncs.com
Accept: application/json
User-Agent: cs-sdk-python/0.0.1 (Darwin/15.2.0/x86_64;2.7.10)
x-acs-signature-nonce: f63659d4-10ac-483b-99da-ea8fde61eae3
Authorization: acs <yourAccessKeyId>:<yourSignature>
x-acs-signature-version: 1.0
Date: Wed, 16 Dec 2015 11:18:47 GMT
x-acs-signature-method: HMAC-SHA1
Content-Type: application/json;charset=utf-8
X-Acs-Region-Id: cn-beijing
Content-Length: 0
```

Common response headers

Each time you send an API request, Container Service returns a unique identifier, RequestId, no matter whether the API call is successful or not.

Example

XML example:

```
<? xml version="1.0" encoding="UTF-8"? >
<!—Response Root Node-->
<API Name + Response>
| <!—Request ID-->
| <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
| <!—Response Data-->
</API Name + Response>
```

JSON example:

```
{
   "RequestId": "4C467B38-3910-447D-87BC-AC049166F216"
   /* Response Data */
}
```

2.2.1.3. Request structure

Endpoint

The endpoint of Container Service APIs is cs.aliyuncs.com.

Protocols

HTTP and HTTPS are supported. We recommend that you send requests through HTTPS for enhanced security.

Request methods

The following HTTP methods are supported: PUT, POST, GET, and DELETE.

Request parameters

Each request must contain common request parameters and parameters unique to specific operations.

Request encoding

Requests and responses are encoded using UTF-8.

2.2.1.4. Response parameters

The response data is returned in a unified format. If status code `2xx` is returned, it indicates that the API call is successful. If status code `4xx` or `5xx` is returned, it indicates that the API call has failed. For successful API calls, response data is returned in XML or JSON format. You can pass a parameter to specify the format when you call the API. The default format is XML.

The following example is formatted for readability. The actual result is not formatted with line feeds or indentation.

2.2.1.5. Sign API requests

Introduction

Apsara Stack issues an AccessKey pair, consisting of an AccessKey ID and AccessKey Secret, to each Apsara Stack tenant account. The AccessKey ID verifies the identity of the user. The AccessKey Secret is used to sign API requests and verify signatures. You must keep your AccessKey confidential. You can create and manage AccessKey pairs on the Apsara Stack official website.

Container Service verifies every request it receives. All requests to Container Service must contain signature information. Container Service performs symmetric encryption by using the AccessKey ID and AccessKey Secret to verify the identity of the requester. Container Service only accepts requests that are validated by verification codes. Invalid requests are rejected and an HTTP 403 error is returned.

You can add an Authorization header to every HTTP request and include the signature in the header.

Container Service requires that the signature be included in the HTTP Header in the following format: `Authorization: acs [Access Key Id]:[Signature]` .

The `Signature` is calculated as follows:

```
Signature = base64(hmac-sha1(VERB + "\n"
        + ACCEPT + "\n"
        + Content-MD5 + "\n"
        + Content-Type + "\n"
        + Date + "\n"
        + CanonicalizedHeaders + "\n"
        + CanonicalizedResource))
```

- `VERB` indicates the HTTP method. For example, `PUT`.
- `Accept` indicates the return value type required by the client. Valid values: application/json and application/xml.
- `Content-MD5` indicates the MD5 value of the request content.
- `Content-Type` indicates the type of the request content.
- `Date` indicates the timestamp when the request was sent. Required. The Date must be in GMT format. If the difference between the timestamp when the request was sent and the timestamp when the request was received exceeds 15 minutes, the request is deemed invalid and a 400 error code is returned. For more information about error codes, see part 5 of this topic. For example, `Thu, 17 Mar 2012 18:49:58 GMT`.
- `CanonicalizedHeaders` indicates the header fields prefixed with `x-acs-` in the request.
- `CanonicalizedResource` indicates the Uniform Resource Identifier (URI) of the requested resource. For example, `/clusters? name=my-clusters&resource=new`.

> **Note** `CanonicalizedHeaders`, header fields prefixed with `x-acs-`, must meet the following requirements:

1. Header field names starting with `x-acs-` must be in lowercase. For example, you need to convert `X-ACS-Meta-Name: TaoBao` to `x-acs-meta-name: TaoBao`. Header field names are case-insensitive. We recommend that you use lowercase letters.
2. If a header field value is too long, replace delimiters such as `\t`, `\n`, `\r`, or `\f`, with spaces.
3. Sort HTTP headers in ascending lexicographic order.
4. Delete any space between the header field names and values. For example, convert `x-acs-meta-name: TaoBao,Alipay` to `x-acs-meta-name:TaoBao,Alipay`.
5. Join all header fields with the `\n` delimiter to form CanonicalizedHeaders.

> **Note** The format of `CanonicalizedResource` is as follows: `CanonicalizedResource` indicates the URIs of the requested resources. You need to sort sub-resources in ascending lexicographic order and join them with the `&` delimiter to form a string. In the following example, the string following the question mark `?` indicates CanonicalizedResource.

```
http://cs.aliyuncs.com/clusters?name=my-clusters&resource=new
```

`CanonicalizedResource` is as follows:

```
/clusters? name=my-clusters&resource=new
```

Example

Overview

The following example demonstrates how to sign an API request.

`access_key_id` and `access_key_secret` indicate the AccessKey ID and AccessKey Secret respectively. We recommend that you use your own program to construct an API request. You can then calculate the signature by following the example.

The example request is as follows:

```
POST http://cs.aliyuncs.com/clusters?param1=value1&param2=value2 HTTP/1.1
Accept-Encoding: identity
Content-Length: 210
Content-MD5: 6U4ALMkKSj0PYbeQSHqgmA==
x-acs-version: 2015-12-15
Accept: application/json
User-Agent: cs-sdk-python/0.0.1 (Darwin/15.2.0/x86_64;2.7.10)
x-acs-signature-nonce: fbf6909a-93a5-45d3-8b1c-3e03a7916799
x-acs-signature-version: 1.0
Date: Wed, 16 Dec 2015 12:20:18 GMT
x-acs-signature-method: HMAC-SHA1
Content-Type: application/json;charset=utf-8
X-Acs-Region-Id: cn-beijing
Authorization: acs <yourAccessKeyId>:<yourSignature>
{"password": "Just$****","instance_type": "ecs.m2.medium","name": "my-test-cluster-9708****","size": 1,"n
etwork_mode": "vpc","data_disk_category": "cloud","data_disk_size": 10,"ecs_image_id": "m-253l****l"}
```

Construct the request

Calculate `Content-Length` and `Content-MD5`.

`Content-Length` indicates the length of the content body.

> **Note** No space or line feed at the beginning of the body.

```
body: {"password": "Just$****","instance_type": "ecs.m2.medium","name": "my-test-cluster-9708****","size
": 1,"network_mode": "vpc","data_disk_category": "cloud","data_disk_size": 10,"ecs_image_id": "m-253ll***
*"}
Content-Length: 210
```

`Content-MD5` : The MD5 value is calculated as follows.

```
body: {"password": "Just$****","instance_type": "ecs.m2.medium","name": "my-test-cluster-9708****","size
": 1,"network_mode": "vpc","data_disk_category": "cloud","data_disk_size": 10,"ecs_image_id": "m-253ll***
*"}
# Calculate the MD5 value of the body
md5(body): e94e002cc90a4a3d0f61b790487aa098
# Convert the MD5 value to a byte array. Convert every two hexadecimal digits to one byte.
# Example: e9 -> 11111111111111111111111111101001 -> -23
bytes(md5(body)): {[-23], [78], [0], [44], [-55], [10], [74], [61], [15], [97], [-73], [-112], [72], [122], [-96], [-104]}
# Convert the byte array to a base64 string
base64(bytes(md5(body))): 6U4ALMkKSj0PYbeQSHqgmA==
Content-MD5: 6U4ALMkKSj0PYbeQSHqgmA==
```

Convert `CanonicalizedHeaders` as follows:

```
# List all header fields prefixed with 'x-acs-'
x-acs-version: 2015-12-15
x-acs-signature-nonce: ca480402-7689-43ba-acc4-4d2013d9d8d4
x-acs-signature-version: 1.0
x-acs-signature-method: HMAC-SHA1
X-Acs-Region-Id: cn-beijing
# Convert the header field name to lowercase, delete the spaces at the start and end of each line, and s
ort the header fields in lexicographical order. Delete any space between the header field names and val
ues.
# Note: No line feed in the last line.
x-acs-region-id:cn-beijing
x-acs-signature-method:HMAC-SHA1
x-acs-signature-nonce:fbf6909a-93a5-45d3-8b1c-3e03a7916799
x-acs-signature-version:1.0
x-acs-version:2015-12-15
```

Calculate `CanonicalizedResource` as follows:

In this example, the length of `CanonicalizedResource` is 27.

> **Note** A line feed `\n` exists at the end of the first line.

```
/clusters? param1=value1&param2=value2
```

Calculate `Signature` as follows:

Construct `SignatureString`. In this example, the length of the signature string is 307. Apart from the last line, each line has a line feed `\n` at the end.

```
POST
application/json
6U4ALMkKSj0PYbeQSHqgmA==
application/json;charset=utf-8
Wed, 16 Dec 2015 12:20:18 GMT
x-acs-region-id:cn-beijing
x-acs-signature-method:HMAC-SHA1
x-acs-signature-nonce:fbf6909a-93a5-45d3-8b1c-3e03a7916799
x-acs-signature-version:1.0
x-acs-version:2015-12-15
/clusters? param1=value1&param2=value2
```

Calculate `Signature` as follows:

```
# Use the AccessKeySecret to encrypt SignatureString. In this example, access_key_secret is the Access KeySecret.
hmac-sha1(SignatureString): fee03d405e421ebaf514adec881038c4b313584d
# Similar to calculating Content-MD5, convert the encrypted string to a byte array.
# Convert the byte array to a base64 string. The output is the signature string.
base64(bytes(hmac-sha1(SignatureString))): ZmVlMDNkNDA1ZTQyMWViYWY1MTRhZGVjODgxMDM4YzRiMzEzNTg0ZA==
Signature: ZmVlMDNkNDA1ZTQyMWViYWY1MTRhZGVjODgxMDM4YzRiMzEzNTg0ZA==
```

The signature calculation is complete.

Add other header fields and the complete HTTP request is as follows:

```
POST http://cs.aliyuncs.com/clusters?param1=value1&param2=value2 HTTP/1.1
Accept-Encoding: identity
Content-Length: 210
Content-MD5: 6U4ALMkKSj0PYbeQSHqgmA==
x-acs-version: 2015-12-15
Accept: application/json
User-Agent: cs-sdk-python/0.0.1 (Darwin/15.2.0/x86_64;2.7.10)
x-acs-signature-nonce: fbf6909a-93a5-45d3-8b1c-3e03a7916799
x-acs-signature-version: 1.0
Date: Wed, 16 Dec 2015 12:20:18 GMT
x-acs-signature-method: HMAC-SHA1
Content-Type: application/json;charset=utf-8
X-Acs-Region-Id: cn-beijing
Authorization: acs <yourAccessKeyId>:<yourSignature>
{"password": "Just$****","instance_type": "ecs.m2.medium","name": "my-test-cluster-9708****","size": 1,"n
etwork_mode": "vpc","data_disk_category": "cloud","data_disk_size": 10,"ecs_image_id": "m-253ll****"}
```

2.2.2. Cluster API list

2.2.2.1. Download cluster certificates

Download the certificate for the cluster where you are logged in.

Request

Request format

```
GET /clusters/:clusterid/certs
```

Custom request headers

None. See Common request headers.

Response

Response format

```
HTTP/1.1 200 OK
```

Custom response headers

None. See Common response headers.

Response body

```
{
   "config": "string"
}
```

Response body parameters

Name	Type	Description
config	string	The kubeconfig file that contains information about the current user.

Example

Sample request

```
GET /clusters/C5b5e80b0b64a4bf6939d2d8fbbc5ded7/certs HTTP/1.1
<Common request header>
```

Sample response

```
HTTP/1.1 200 OK
<Common response header>
{
    "config": "xxxxxxxx"
}
```

2.2.2.2. Create Kubernetes clusters

Create a Kubernetes cluster and add nodes to the cluster.

Request

Request format

```
POST /clusters HTTP/1.1
```

Custom request headers

None. See Common request headers.

Request body

```
{
   "disable_rollback": "whether to roll back when the operation fails",
   "name": "cluster name",
   "timeout_mins": "cluster creation timeout",
   "cluster_type": "cluster type. Kubernetes",
```

```
    "region_id": "region",
    "vpcid": "VPC ID",
    "zoneid": "zone",
    "vswitchid": "VSwitch ID",
    "container_cidr": "POD CIDR Block",
    "service_cidr": "Service CIDR Block",
    "ssh_flags": "whether to allow public access through SSH",
    "cloud_monitor_flags":"whether to install the CloudMonitor agent",
    "login_password": "SSH logon password. Select one between SSH authentication and key pair authent
ication",
    "key_pair":"key pair name. Select one between SSH authentication and key pair authentication",
    "master_instance_charge_type":"billing method of the Master node. PostPaid or PrePaid",
    "master_period_unit":"unit of the subscription duration of the Master node. Month or Year. This para
meter only takes effect when parameter master_instance_charge_type is set to PrePaid",
    "master_period":"duration of the subscription of the Master node. This parameter only takes effect w
hen parameter master_instance_charge_type is set to PrePaid",
    "master_auto_renew":"whether auto renewal is enabled for the Master node",
    "master_auto_renew_period":"renewal cycle of the Master node",
    "master_instance_type": "instance type of the Master node",
    "master_system_disk_category": "system disk type of the Master node",
    "master_system_disk_size":"system disk size of the Master node",
    "master_data_disk":"whether a data disk is attached to the Master node",
    "master_data_disk_category":"type of the data disk attached to the Master node",
    "master_data_disk_size":"size of the data disk attached to the Master node",
    "worker_instance_charge_type":"billing method of Worker nodes. PrePaid or PostPaid",
    "worker_period_unit":"unit of the subscription duration of Worker nodes. Month or Year. This paramet
er only takes effect when parameter worker_instance_charge_type is set to PrePaid",
    "worker_period":"subscription duration of Worker nodes. This parameter only takes effect when para
meter worker_instance_charge_type is set to PrePaid",
    "worker_auto_renew":"whether auto renewal is enabled for worker nodes. Valid values: true and fals
e",
    "worker_auto_renew_period":"renewal cycle of worker nodes",
    "worker_instance_type": "instance type of Worker nodes",
    "worker_system_disk_category": "system disk type of Worker nodes",
    "worker_system_disk_size": "system disk size of Worker nodes",
    "worker_data_disk":"whether data disks are attached to Worker nodes",
    "worker_data_disk_category":"type of the data disks attached to Worker nodes",
    "worker_data_disk_size":"size of the data disks attached to Worker nodes",
    "num_of_nodes": "number of Worker nodes",
    "snat_entry": "whether to configure SNAT entries",
    "public_slb":"whether to allow public access to the API Server"
}
```

```
}
```

Request body parameters

Name	Type	Required	Description
disable_rollback	bool	No	Whether to roll back when the operation fails. • A value of true indicates no. • A value of false indicates yes. Default value: true. If you choose to roll back when the operation fails, resources created during the operation are released. We recommend that you choose true.
name	string	Yes	The cluster name. The name can contain uppercase and lowercase letters, Chinese characters, numbers, and hyphens (-).
timeout_mins	int	No	The maximum time in minutes during which the cluster creation operation must be completed. Default: 60.
region_id	string	Yes	The ID of the region where the cluster is located.
zoneid	string	Yes	The zone of the region.
vpcid	string	No	The ID of the VPC network where the cluster is deployed. Optional. If this parameter is not specified, the system automatically creates a VPC network with CIDR block 192.168.0.0/16. Note Parameter vpcid and vswitchid must be used together.
vswitchid	string	No	The ID of the VSwitch associated with the cluster. Optional. If this parameter is not specified, the system automatically creates a VSwitch with CIDR block 192.168.0.0/16.
container_cidr	string	No	The CIDR block associated with the container. This CIDR block must not overlap with that of the VPC network. If the VPC network is automatically created by the system, the container is associated with CIDR block 172.16.0.0/16 by default.

Name	Type	Required	Description
service_cidr	string	No	The service CIDR block. This CIDR block must not overlap with that of the VPC network or container. If the VPC network is automatically created by the system, the service CIDR block is set to 172.19.0.0/20 by default.
master_instance_charge_type	string	Yes	The billing method of the Master node. Default value: PostPaid. Valid values: • A value of PrePaid indicates that a subscription-based billing method is used. • A value of PostPaid indicates that a pay-as-you-go billing method is used.
master_period_unit	string	No	The unit of the subscription duration. This parameter is required when parameter master_instance_charge_type is set to PrePaid. Valid values: • A value of Week indicates that the subscription duration is measured in weeks. • A value of Month indicates that the subscription duration is measured in months.
master_period	int	No	The duration of the subscription. This parameter is required when parameter master_instance_charge_type is set to PrePaid. • When `PeriodUnit=Week`, the valid values are as follows: 1, 2, 3, and 4. • When `PeriodUnit=Month`, the valid values are as follows: 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 24, 36, 48, and 60.
master_auto_renew	bool	No	Whether auto renewal is enabled for the Master node. This parameter is required when parameter master_instance_charge_type is set to PrePaid. • A value of true indicates that auto renewal is enabled. • A value of false indicates that auto renewal is disabled.

Name	Type	Required	Description
master_auto_renew_period	int	No	The cycle of auto renewal. This parameter is required when parameter master_instance_charge_type is set to PrePaid and parameter master_auto_renew is set to true. • When `PeriodUnit=Week`, the valid values are as follows: 1, 2, and 3. • When `PeriodUnit=Month`, the valid values are as follows: 1, 2, 3, 6, and 12.
master_instance_type	string	Yes	The instance type of the Master node. For more information, choose Elastic Compute Service > Instances and see topic *Instance type families* .
master_system_disk_category	string	Yes	The system disk type of the Master node. Valid values: • A value of cloud_efficiency indicates the ultra cloud disk. • A value of cloud_ssd indicates the SSD cloud disk.
master_system_disk_size	int	Yes	The system disk size of the Master node. Unit: GiB.
master_data_disk	bool	No	Whether a data disk is attached to the Master node. Valid values: • A value of true indicates yes. • A value of false indicates no. Default is false.
master_data_disk_category	string	No	The data disk type of the Master node. This parameter only takes effect when parameter master_data_disk is set to true. Valid values: • A value of cloud indicates the basic cloud disk. • A value of cloud_efficiency indicates the ultra cloud disk. • A value of cloud_ssd indicates the SSD cloud disk.
master_data_disk_size	int	No	The data disk size of the Master node. This parameter only takes effect when parameter master_data_disk is set to true. Unit: GB.

Name	Type	Required	Description
worker_instance_charge_type	string	No	The billing method of Worker nodes. Default value: PostPaid. Valid values: • A value of PrePaid indicates that a subscription-based billing method is used. • A value of PostPaid indicates that a pay-as-you-go billing method is used.
worker_period_unit	string	No	The unit of the subscription duration. This parameter is required when parameter worker_instance_charge_type is set to PrePaid. Valid values: • A value of Week indicates that the subscription duration is measured in weeks. • A value of Month indicates that the subscription duration is measured in months.
worker_period	int	No	The duration of the subscription. This parameter is required when parameter worker_instance_charge_type is set to PrePaid. • When `PeriodUnit=Week`, the valid values are as follows: 1, 2, 3, and 4. • When `PeriodUnit=Month`, the valid values are as follows: 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 24, 36, 48, and 60.
worker_auto_renew	bool	No	Whether auto renewal is enabled for Worker nodes. Valid values: • A value of true indicates that auto renewal is enabled. • A value of false indicates that auto renewal is disabled.
worker_auto_renew_period	int	No	The cycle of auto renewal. This parameter is required when parameter worker_instance_charge_type is set to PrePaid and parameter worker_auto_renew is set to true. • When `PeriodUnit=Week`, the valid values are as follows: 1, 2, and 3. • When `PeriodUnit=Month`, the valid values are as follows: 1, 2, 3, 6, and 12.

Name	Type	Required	Description
worker_instance_type	string	Yes	The instance type of Worker nodes. For more information, choose Elastic Compute Service > Instances and see topic *Instance type families* .
worker_system_disk_category	string	Yes	The system disk type of Worker nodes.
worker_system_disk_size	int	Yes	The system disk size of Worker nodes. Unit: GB.
worker_data_disk	string	No	Whether data disks are attached to Worker nodes. Valid values: • A value of true indicates yes. • A value of false indicates no.
worker_data_disk_category	int	No	The data disk type of Worker nodes. This parameter only takes effect when parameter worker_data_disk is set to true. Valid values: • A value of cloud indicates the basic cloud disk. • A value of cloud_efficiency indicates the ultra cloud disk. • A value of cloud_ssd indicates the SSD cloud disk.
worker_data_disk_size	string	No	The data disk size of Worker nodes. This parameter only takes effect when parameter worker_data_disk is set to true. Unit: GB.
login_password	string	Yes	The SSH logon password. The password must be 8 to 30 characters in length and contain letters, numbers, and special characters. Select one between login_password and key_pair.
key_pair	string	Yes	The keypair name. Select one between login_password and key_pair.
num_of_nodes	int	Yes	The number of Worker nodes. Valid values: [0, 300]

Name	Type	Required	Description
snat_entry	bool	Yes	Whether to configure SNAT. If the VPC network is automatically created, this parameter must be set to true. If an existing VPC network is used, configure this parameter as follows: • If the VPC network can access the Internet, set this parameter to false. • If the VPC network cannot access the Internet, set this parameter to true to configure SNAT.
ssh_flags	bool	No	Whether to enable SSH. • A value of true indicates that SSH is enabled. • A value of false indicates that SSH is disabled.
cloud_monitor_flags	bool	No	Whether to install the CloudMonitor agent. • A value of true indicates yes. • A value of false indicates no.
public_slb	bool	No	Whether to allow public access to the API Server. • A value of true indicates that public access to the API Server is allowed. Default value: true. • A value of false indicates that public access to the API Server is denied.

Response

Response format

```
HTTP/1.1 202 Accepted
```

Custom response headers

None. See Common response headers.

Response body

```
{
  "cluster_id":"string",
  "request_id":"string",
  "task_id":"string"
}
```

Example

Sample request

```
POST /clusters HTTP/1.1
<Common request header>
{
   "disable_rollback": true,
   "name": "my-test-Kubernetes-cluster",
   "timeout_mins": 60,
   "cluster_type": "Kubernetes",
   "region_id": "cn-beijing",
   "zoneid": "cn-beijing-f",

   "vpcid": "",
   "vswitchid": "",
   "num_of_nodes": 1,
   "container_cidr": "172.16.0.0/16",
   "service_cidr": "172.19.0.0/20",
   "cloud_monitor_flags": true,
   "master_instance_type": "ecs.sn1ne.large",
   "master_system_disk_category": "cloud_efficiency",
   "master_system_disk_size": 40,

   "worker_instance_type": "ecs.sn1ne.large",
   "worker_system_disk_category": "cloud_efficiency",
   "worker_system_disk_size": 40,

   "snat_entry": true,
   "ssh_flags": true,
   "login_password": "Hello1234"

}
```

Sample response

```
HTTP/1.1 202 Accepted
<Common response header>
{
   "cluster_id": "cb95aa626a47740afbf6aa099b650d7ce",
   "request_id": "687C5BAA-D103-4993-884B-C35E4314A1E1",
   "task_id": "T-5a54309c80282e39ea00002f"
}
```

2.2.2.3. Add ECS instances to clusters

Add existing ECS instances to clusters.

> **Note** When you add an ECS instance to a cluster, the system disk of the instance is replaced. We recommend that you back up data in advance.

Request

Request format

```
POST /clusters/{cluster_id}/attach HTTP/1.1
```

Request parameters

Name	Type	Required	Description
cluster_id	string	Yes	The ID of the cluster.

Custom request headers

None. See Common request headers.

Request body

```
{
   "password": "root password of the ECS instance",
   "instances": "instances that you want to add to the cluster",
   "format_disk": "whether to format data disks",
   "key_pair": "instance key pair"
}
```

Request body parameters

Name	Type	Required	Description

Name	Type	Required	Description
password	string	Yes	The password for logging on to the ECS instance. The password must be 8 to 30 characters in length and contain letters, numbers, and special characters.
instances	Array	Yes	The array of existing instances.
format_disk	bool	No	Whether to format data disks.
key_pair	string	No	The name of the key pair. • For Windows instances, ignore this parameter. Default is empty. The *password* parameter takes effect even if this parameter is specified. • For Linux instances, if this parameter is specified, password authentication is disabled.

Response

Response format

```
HTTP/1.1 202 OK
```

Custom response headers

None. See Common response headers.

Response body

```
{
  "list": [
    {
      "code": "200",
      "instanceId": "i-2zee3oiwcyoz7kwdo8bt",
      "message": "successful"
    },
    {
      "code": "200",
      "instanceId": "i-2ze0lgm3y6iylcbtcypf",
      "message": "successful"
    }
  ],
  "task_id": "T-5a544aff80282e39ea000039"
}
```

Example

Sample request

```
POST /clusters/Cccfd68c474454665ace07efce924f75f/attach HTTP/1.1
<Common request header>
{
  "password": "Hello1234",
  "instances": [
    "i-xxxx",
    "i-yyyy"
  ]
}
```

Sample response

```
HTTP/1.1 202 Accepted
<Common response header>
{
   "list": [
      {
         "code": "200",
         "instanceId": "i-xxxx",
         "message": "successful"
      },
      {
         "code": "200",
         "instanceId": "i-yyyy",
         "message": "successful"
      }
   ],
   "task_id": "T-5a544aff80282e39ea000039"
}
```

2.2.2.4. Get kubeconfig files

Get the kubeconfig file that contains information about the current user. kubeconfig files are used to configure access to clusters.

Request

Request format

```
GET /k8s/:clusterid/user_config
```

Custom request headers

None. See Common request headers.

Response

Response format

```
HTTP/1.1 200 OK
```

Custom response headers

None. See Common response headers.

Response body

```
{
   "config": "string"
}
```

Response body parameters

Name	Type	Description
config	string	The kubeconfig file that contains information about the current user.

Example

Sample request

```
GET /k8s/c5b5e80b0b64a4bf6939d2d8fbbc5ded7/user_config HTTP/1.1
<Common request header>
```

Sample response

```
HTTP/1.1 200 OK
<Common response header>
{
   "config": "xxxxxxxx"
}
```

2.2.2.5. View clusters

View cluster details by cluster ID.

Request

Request format

```
GET /clusters/{cluster_id} HTTP/1.1
```

Request parameters

Name	Type	Required	Description
cluster_id	string	Yes	The ID of the cluster.

Custom request headers

None. See Common request headers.

Request body

None.

Response

Response format

```
HTTP/1.1 200 OK
```

Custom response headers

None. See Common response headers.

Response body

```
{
  "agent_version": "string",
  "cluster_id": "string",
  "created": "datetime",
  "external_loadbalancer_id": "string",
  "master_url": "string",
  "name": "string",
  "network_mode": "string",
  "region_id": "string",
  "security_group_id": "string",
  "size": "numbers",
  "state": "string",
  "updated": "datetime",
  "vpc_id": "string",
  "vswitch_id": "string"
}
```

Response body parameters

Cluster details

Name	Type	Description
agent_version	string	The Agent version.
cluster_id	string	The unique identifier of the cluster.
created	string	The timestamp when the cluster is created.
external_loadbalancer_id	string	The ID of the SLB instance deployed in the cluster.

Name	Type	Description
master_url	string	The address of the Master node in the cluster. You can use this address to connect to the cluster. For more information, see *topic* Connect to the Master node through SSH in Container Service User Guide.
name	string	The cluster name that you specified when you created the cluster. The cluster name must be unique under each Apsara Stack tenant account.
network_mode	string	The network type. vpc indicates the VPC network.
region_id	string	The ID of the region where the cluster is located.
security_group_id	string	The ID of the security group.
size	string	The number of nodes in the cluster.
state	string	The state of the cluster.
updated	string	The last update time.
vpc_id	string	The ID of the VPC network where the cluster is deployed.
vswitch_id	string	The ID of the VSwitch associated with the cluster.

Example

Sample request

```
GET /clusters/C5b5e80b0b64a4bf6939d2d8fbbc5ded7 HTTP/1.1
<Common request header>
```

Sample response

```
HTTP/1.1 200 OK
<Common response header>
{
   "agent_version": "0.5-e56dab3",
   "cluster_id": "c978ca3eaacd3409a9437db07598f1f69",
   "created": "2015-12-11T03:52:40Z",
   "external_loadbalancer_id": "1518f2b7e4c-cn-beijing-btc-a01",
   "master_url": "https://182.92.245.56:17589",
   "name": "my-python-cluster-039de960",
   "network_mode": "vpc",
   "region_id": "cn-beijing",
   "security_group_id": "sg-25yqjuxhz",
   "size": 5,
   "state": "running",
   "updated": "2015-12-15T15:01:58Z",
   "vpc_id": "",
   "vswitch_id": ""
}
```

2.2.2.6. Expand Kubernetes clusters

Increase or decrease the number of Worker nodes in the clusters. This operation is only applicable to resources created by ROS.

Request

Request format

```
PUT /clusters/{cluster_id} HTTP/1.1
```

Request parameters

Name	Type	Required	Description
cluster_id	string	Yes	The ID of the cluster.

Custom request headers

None. See Common request headers.

Request body

```
{
   "disable_rollback": "whether to roll back when the operation fails",
   "timeout_mins": "resource creation timeout",
   "worker_instance_type": "Worker instance type",
   "login_password": "node SSH login password",
   "num_of_nodes": "number of Worker nodes"
}
```

Request body parameters

Name	Type	Required	Description
disable_rollback	bool	Yes	Whether to roll back when the operation fails. A value of *true* indicates no. A value of *false* indicates yes. If you choose to roll back when the operation fails, resources created during the operation are released. We recommend that you choose *true*.
timeout_mins	int	Yes	The maximum time in minutes during which a resource creation operation must be completed. Default: *60*.
worker_instance_type	string	Yes	The instance type of Worker nodes. For more information, choose Elastic Compute Service > Instances and see topic *Instance type families* .

Name	Type	Required	Description
login_password	string	Yes	The SSH login password. The password must be 8 to 30 characters in length and contain letters, numbers, and special characters. The password must be the same as the password you specified when you created the cluster. **Note** You can only choose to specify either login_password or num_of_nodes. You must specify the parameter that you specified when you created the cluster.
num_of_nodes	int	Yes	The number of Worker nodes. Valid values: [0,300] To expand the cluster, you must specify a value that is greater than the existing number of Worker nodes. **Note** You can only choose to specify either login_password or num_of_nodes. You must specify the parameter that you specified when you created the cluster.

Response

Response format

```
HTTP/1.1 202 Accepted
```

Custom response headers

None. See Common response headers.

Response body

```
{
   "cluster_id":"string",
   "request_id":"string",
   "task_id":"string"
}
```

Example

Sample request

```
PUT /clusters/Cccfd68c474454665ace07efce924f75f HTTP/1.1
<Common request header>
{
   "disable_rollback": true,
   "timeout_mins": 60,
   "worker_instance_type": "ecs.sn1ne.large",
   "login_password": "Hello1234"
}
```

Sample response

```
HTTP/1.1 202 Accepted
<Common response header>
{
   "cluster_id": "<yourClusterId>",
   "request_id": "687C5BAA-D103-4993-884B-C35E4314A1E1",
   "task_id": "T-5a54309c80282e39ea00002f"
}
```

2.2.2.7. Delete clusters

Delete clusters by cluster ID and release all nodes in the clusters.

Request

Request format

```
DELETE /clusters/{cluster_id} HTTP/1.1
```

Request parameters

Name	Type	Required	Description
cluster_id	string	Yes	The ID of the cluster.

Custom request headers

None. See Common request headers.

Request body

None.

Response

Response format

```
HTTP/1.1 202 Accepted
```

Custom response headers

None. See Common response headers.

Response body

None.

Example

Sample request

```
DELETE /clusters/Cccfd68c474454665ace07efce924f75f HTTP/1.1
<Common request header>
```

Sample response

```
HTTP/1.1 202 Accepted
<Common response header>
```

2.3. Auto Scaling (ESS)

2.3.1. API reference

2.3.1.1. API usage instructions

Before you call ESS API operations, you must be granted the ESS API permissions in the ESS console. If you are not authorized, the following error codes will be returned.

Error code description

Description	Error code	Error message	HTTP status code
The error message returned because ESS is not activated and you are not authorized to call this operation.	Forbidden.Unsubscribed	Do not have permission to access this API.	403
The error message returned because you are not authorized to call ESS API operations.	Forbidden.Unauthorized	A required authorization for the specified action is not supplied.	403

2.3.1.2. Make API requests

Call an ESS API operation, send an HTTP GET request to the ESS API server, and add corresponding parameters to the request based on the description of the corresponding API operation. After the request is processed, the system will return a result.

2.3.1.3. Request structure

This topic introduces the request structure.

- **Endpoint**

  The service address of the Auto Scaling API operations is ess.example.com. For more information, see Obtain an endpoint.

- **Protocols**

  You can send requests over HTTP or HTTPS. We recommend that you send API requests through HTTPS for higher security.

- **Request Method**

  The system allows you to send HTTP GET requests. This requires request parameters to be included in the request URL.

- **Request parameters**

  For each request, you must specify the operation you want to execute as an action parameter, such as CreateScalingGroup. Additionally, each request must contain the common request parameters and specific request parameters of the specified operation.

- **Character encoding**

  Requests and responses are encoded using the UTF-8 character set.

2.3.1.4. Common parameters

2.3.1.4.1. Common request parameters

Common request parameters are request parameters that you must use when you call each API.

Common request parameter description

Parameter	Type	Required	Description
Format	String	No	The type of the returned value. Valid values: JSON and XML. Default value: XML.
Version	String	Yes	The version number of the API. The format is YYYY-MM-DD. The current version is 2014-08-28.
AccessKeyId	String	Yes	The AccessKey ID provided by Apsara Stack for you to access services.
Signature	String	Yes	The signature result string. For more information about signature calculation methods, see the "Sign signatures" topic.
SignatureMethod	String	Yes	The mode of the signature. HMAC-SHA1 is supported currently.
Timestamp	String	Yes	The timestamp of a request. The date format complies with the ISO 8601 standard, and uses UTC time. The format is YYYY-MM-DDThh:mm:ssZ. For example, 2014-08-28T12:00:00Z (20:00:00, August 28, 2014, China Standard Time).
SignatureVersion	String	Yes	The algorithm version of the signature. The current version is 1.0.
SignatureNonce	String	Yes	A unique, randomly generated number used to prevent network replay attacks. You must use different random numbers for different requests.

XML format

```
https://ess.example.com/
? Format=xml
&Version=2014-08-28
&Signature=Pc5WB8gokVn0xfeu%2FZV%2BiNM1****
&SignatureMethod=HMAC-SHA1
&SignatureNonce=1521552885****
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2014-08-28T12:00:00Z
```

2.3.1.4.2. Common response parameters

Each time you call an API, the system returns a globally unique ID (RequestId), regardless of whether the request is successful.

XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<!—The root node of the result-->
<API name+Response>
   <!—The returned request tag-->
   <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
   <!—The response data-->
</API name+Response>
```

JSON format

```
{
   "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
   /* The response data */
}
```

2.3.1.5. Responses

2.3.1.5.1. Successful response examples

After an API is called, the response data is displayed in a uniform format. A returned HTTP status code of 2xx indicates that the call succeeds. A returned HTTP status code of 4xx or 5xx indicates that the call fails. When the call succeeds, the formats of response data are XML and JSON. An external system can set parameters in a request to specify the format of the response data. The default value is XML.

> **Note** The sample responses in this document are formatted in a way that is easier for you to read. The actual response data does not go through line breaks, indentation, or other layouts.

Responses in the XML format include information about whether the request succeeds and specific service data.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-The root node of the result-->
<API name+Response>
   <!-The returned request tag-->
   <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
   <!-The response data-->
</API name+Response>
```

JSON format

```
{
   "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
   /* The response data */
}
```

2.3.1.5.2. Error response examples

When an error occurs during an API call, no response data is returned. You can locate the cause of an error based on the error codes corresponding to each API in Client errors and Server errors.

When an error occurs during a call, an HTTP status code of 4xx or 5xx is returned. The returned message includes the specific error code and message. It also contains a globally unique request ID (RequestId) and the ID of the site you accessed with this request (HostId).

XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<Error>
  <RequestId>8906582E-6722-409A-A6C4-0E7863B733A5</RequestId>
  <HostId>ess.example.com</HostId>
  <Code>UnsupportedOperation</Code>
  <Message>The specified action is not supported. </Message>
</Error>
```

JSON format

```
"RequestId": "8906582E-6722-409A-A6C4-0E7863B733A5",
    "HostId": "ess.example.com",
    "Code": "UnsupportedOperation",
    "Message": "The specified action is not supported."
}
```

2.3.1.6. Request signatures

This topic describes how API requests are signed and authenticated.

You must sign all API requests to ensure security. Alibaba Cloud uses the request signature to verify the identity of the API caller. Auto Scaling implements symmetric encryption with an AccessKey pair to verify the identity of the request sender. An AccessKey pair is an identity credential issued to Apsara Stack tenant accounts and RAM users that is similar to a logon username and password. An AccessKey pair consists of an AccessKey ID and an AccessKey secret. The AccessKey ID is used to verify the identity of the user, while the AccessKey secret is used to encrypt and verify the signature string. You must keep your AccessKey secret strictly confidential. For more information, see Obtain an AccessKey pair.

Perform the following steps to sign an access request:

1. Compose and encode a string-to-sign.
    i. Create a canonicalized query string by arranging the request parameters (including all common and operation-specific parameters except Signature) in alphabetical order. The canonicalized query string is only made up of the parameters and does not include "https://endpoint/?".

    > **Note** When you use the GET method to submit requests, these parameters constitute the parameter field of the request URI following the question mark (?) and connected by the ampersand (&).

    ii. Encode the name and value of each request parameter. Encode the canonicalized query string in UTF-8. The URL encoding rules are as follows:
        - Uppercase letters, lowercase letters, digits, and some special characters such as ampersands (&), hyphens (-), underscores (_), periods (.), and tildes (~) do not need to be encoded.
        - Other characters must be percent encoded in %XY format. XY represents the ASCII code of the characters in hexadecimal notation. For example, double quotation marks (") are encoded as %22.
        - Extended UTF-8 characters are encoded in %XY%ZA... format.
        - Spaces must be encoded as %20. Do not encode spaces as plus signs (+).

        > **Note** Generally, libraries that support URL encoding (for example, the java.net.URLEncoder class in Java) encode strings in compliance with the requirements of the "application/x-www-form-urlencoded" MIME-type. If this encoding method is used, replace the plus signs (+) in the encoded strings with "%20", the asterisks (*) with "%2A", and "%7E" with tildes (~), to conform to the preceding encoding rules.

iii. Connect the encoded parameter names and values with equal signs (=).

iv. Sort the equal sign-connected strings by their parameter names alphabetically and connect them with ampersands (&).

2. Create a string-to-sign from the encoded canonicalized query string. The steps to create a string-to-sign are as follows:

```
StringToSign=
HTTPMethod + "&" +
percentEncode("/") + "&" +
percentEncode(CanonicalizedQueryString)
```

3. Follow RFC 2104 to calculate the HMAC value of the string-to-sign using the AccessKey secret as the key.

> **Note** The key used for calculating the signature is your AccessKey secret followed by an ampersand (&). Use SHA1 as the hashing algorithm.

4. Encode the HMAC value in Base64 to obtain the signature string.
5. Add the signature string to the request as the Signature parameter. The result is the signed API request.

> **Note**
>
> When the obtained signature value is submitted to the ECS server as the final request parameter value, the value must be URL-encoded like other parameters based on rules defined in RFC 3986.
>
> Take DescribeScalingGroups as an example. The request URL to be signed is as follows:
>
> ```
> http://ess.example.com/?TimeStamp=2014-08-15T11%3A10%3A07Z&Format=xml&AccessKeyId=testid&Action=DescribeScalingGroups&SignatureMethod=HMAC-SHA1&RegionId=cn-qingdao&SignatureNonce=1324fd0e-e2bb-4bb1-917c-bd6e437f****&SignatureVersion=1.0&Version=2014-08-28
> ```
>
> Then, the StringToSign is:
>
> ```
> GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeScalingGroups&Format%3Dxml&RegionId%3Dcn-qingdao&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D1324fd0e-e2bb-4bb1-917c-bd6e437f***&SignatureVersion%3D1.0&TimeStamp%3D2014-08-15T11%253A10%253A07Z&Version%3D2014-08-28
> ```
>
> If the Access Key Id is testid and the Access Key Secret is testsecret, the Key used for HMAC calculation is testsecret&. Then, the calculated signature value is SmhZuLUnXmqxSEZ%2FGqyiwGqmf%2BM=.
>
> The signed request URL with signature parameters is as follows:
>
> ```
> http://ess.example.com/?TimeStamp=2014-08-15T11%3A10%3A07Z&Format=xml&AccessKeyId=testid&Action=DescribeScalingGroups&SignatureMethod=HMAC-SHA1&RegionId=cn-qingdao&SignatureNonce=1324fd0e-e2bb-4bb1-917c-bd6e437f****&SignatureVersion=1.0&Version=2014-08-28&Signature=SmhZuLUnXmqxSEZ%2FGqyiwGqmf%****
> ```

2.3.1.7. Scaling groups

2.3.1.7.1. CreateScalingGroup

You can create a scaling group.

Description

You call call this operation to create scaling groups based on input parameters.

- MinSize and MaxSize define the minimum number and maximum number of ECS instances in a scaling group, respectively.
  - When the number of ECS instances currently in the scaling group is smaller than MinSize, ECS instances are automatically created to the group to make the number of instances equal to MinSize.
  - When the number of ECS instances currently in the scaling group is greater than MaxSize, ECS instances are automatically removed from the group to make the number of instances equal to MaxSize.

- DefaultCooldown indicates the default cool-down time of a scaling group.
  - During the cool-down time after a scaling activity (attaching or removing ECS instances) is executed, the scaling group cannot execute any other scaling activities.
  - Currently, this parameter is only valid for scaling activities triggered by CloudMonitor alarms.
- RemovalPolicy is used to filter and remove ECS instances from a scaling group. It allows you to remove instances based on multiple filtering conditions.
  - If an SLB instance is specified for a scaling group, the scaling group automatically added ECS instances to the specified SLB instance.
  - The specified SLB instance must be active.
  - Health check must be enabled on all listener ports configured for the SLB instance. Otherwise, the scaling group fails to be created.
  - If ECS instances of the VPC type have been added to an SLB instance, the SLB instance cannot be specified for a scaling group.
  - The default weight of the ECS instance added to an SLB instance is 50.
- If an RDS instance is specified for a scaling group, the scaling group automatically adds the intranet IP addresses of its ECS instances to the whitelist of the specified RDS instance.
  - The specified RDS instance must be running.
  - The number of IP addresses in the specified RDS instance whitelist cannot be greater than or equal to the upper limit.
- A scaling group does not go into effect after it is created. It must be enabled to trigger scaling rules and execute scaling rules.
- Each scaling group must be in the same region as the SLB instance and RDS instance.
- You can create up to 20 scaling groups.

Request parameters

Request parameter description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateScalingGroup.
RegionId	String	Yes	The ID of the region where the scaling group is located.
MaxSize	Integer	Yes	The maximum number of ECS instances in the scaling group. Valid values: [0, 100].
MinSize	Integer	Yes	The minimum number of ECS instances in the scaling group. Valid values: [0, 100].

Parameter	Type	Required	Description
ScalingGroupName	String	No	The displayed name of the scaling group must be 2 to 40 characters in length. It must start with a letter or number. It can contain numbers, uppercase letters, lowercase letters, underscores (_), hyphens (-), and periods (.). This parameter must be unique in the region it is located and under an Apsara Stack tenant account. If you do not specify this parameter, the default value (ScalingGroupId) is used.
DefaultCooldown	Integer	No	The default cool-down time of the scaling group. Valid values: [0, 86400]. Unit: second. Default value: 300s.
RemovalPolicy.N	String	No	The policy for removing ECS instances from a scaling group. Valid values: • OldestInstance: Remove the ECS instance that was added to the scaling group first. • NewestInstance: Remove the ECS instance that was added to the scaling group last. • OldestScalingConfiguration: Remove ECS instances that were created based on the earliest scaling configuration. Default values: OldestScalingConfiguration and OldestInstance. You can enter up to two values.
LoadBalancerIds	String	No	The SLB instance IDs. The instance IDs are formatted as a JSON array, such as lb-id0, lb-id1, and lb-idz can contain a maximum of five Server Load Balancer instances.
DBInstanceIds	String	No	The RDS instance IDs. The instance IDs are formatted as a JSON array, such as rm-id0, rm-id1, and rm-idz can contain a maximum of eight ApsaraDB RDS instances.
VSwitchId	String	No	The VSwitch ID must be specified when you create a scaling group of the VPC type.

Parameter	Type	Required	Description
VSwitchIds.N	String	No	• If VSwitchIds.N is set, VSwitchId is ignored. • This parameter enables you to specify a maximum of five VSwitches of one VPC in multiple zones when you create a scaling group. The value range of N is [1, 5]. • The VSwitch priority is indicated by an ascending set of numbers, with 1 indicating the highest priority. • When an ECS instance cannot be created in the zone where the VSwitch with the highest priority resides, the instance will be created in the zone where the VSwitch with the next highest priority resides.

Response parameters

Response parameter description

Parameter	Type	Description
ScalingGroupId	String	The globally unique scaling group ID generated by the system.

Error code

For more information about common error codes, see Client errors or Server errors.

Error code description

Description	Error code	Description	HTTP status code
The error message returned when the scaling group name already exists.	InvalidScalingGroupName.Duplicate	The specified value of parameter `<parameter name>` is duplicated.	400
The error message returned when the number of user scaling groups reaches the upper limit.	QuotaExceeded.ScalingGroup	Scaling group quota exceeded.	400
The error message returned when the specified region does not exist.	InvalidRegionId.NotFound	The specified region does not exist.	404

Description	Error code	Description	HTTP status code
The error message returned when the specified MinSize is greater than MaxSize.	InvalidParameter.Conflict	The values of parameter <parameter name> and parameter <parameter name> are conflict.	400
The error message returned when the specified SLB instance does not exist under this account.	InvalidLoadBalancerId.NotFound	The specified Load Balancer does not exist.	404
The error message returned when the specified SLB instance and scaling group are not in the same region.	InvalidLoadBalancerId.RegionMismatch	The specified Load Balancer and the specified scaling group are not in the same region.	400
The error message returned when the specified SLB instance is not active.	IncorrectLoadBalancerStatus	The current status of the specified load balancer does not support this action.	400
The error message returned when health check is not enabled for the specified SLB instance.	IncorrectLoadBalancerHealthCheck	The current health check type of specified load balancer does not support this action.	400
The error message returned when the network type of the specified SLB instance is private after you specify the VSwitch ID.	InvalidLoadBalancerId.IncorrectAddressType	The current address type of specified Load Balancer does not support this action.	400
The error message returned when the network type of the ECS instance connected to the specified SLB instance is different from that of the scaling group.	InvalidLoadBalancerId.IncorrectInstanceNetworkType	The network type of the instance in specified load balancer does not support this action.	400
The error message returned when the ECS instance connected to the SLB instance of the specified scaling group and the VSwitch are not in the same VPC.	InvalidLoadBalancerId.VPCMismatch	The specified virtual switch and the instance in specified load balancer are not in the same VPC.	400

Description	Error code	Description	HTTP status code
The error message returned when the specified RDS instance does not exist under this account.	InvalidDBInstanceId.NotFound	DB instance "XXX" does not exist.	404
The error message returned when the specified RDS instance and scaling group are not in the same region.	InvalidDBInstanceId.RegionMismatch	DB instance "XXX" and the specified scaling group are not in the same Region.	400
The error message returned when the specified RDS instance is not running.	IncorrectDBInstanceStatus	The current status of DB instance "XXX" does not support this action.	400
The error message returned when the number of IP addresses in the specified RDS instance whitelist reaches the upper limit.	QuotaExceeded.DBInstanceSecurityIP	Security IP quota exceeded in DB instance "XXX".	400
The error message returned when the specified VSwitch does not exist.	InvalidVSwitchId.NotFound	The specified virtual switch does not exist.	404
The error message returned when the number of private IP addresses of the VSwitch reaches the upper limit.	QuotaExceeded.PrivateIpAddress	Private IP address quota exceeded in the specified virtual switch.	400
The error message returned when the number of instances in the VPC reaches the upper limit.	QuotaExceeded.VPCInstance	Instance quota exceeded in the specified VPC.	400
The error message returned when the VSwitch is unavailable, and instances cannot be created.	IncorrectVSwitchStatus	The current status of virtual switch does not support this operation.	400

Examples

Sample requests

```
http://ess.example.com/?Action=CreateScalingGroup
&RegionId=cn-qingdao
&MaxSize=20
&MinSize=2
&LoadBalancerId=147b46d767c-cn-qingdao-c****
&DBInstanceId. 1=rdszzzyyuny****
&DBInstanceId. 2=rdsia3u3yia****
&<Common request parameter>
```

Response examples

XML format

```
<CreateScalingGroupResponse>
  <RequestId>536E9CAD-DB30-4647-AC87-AA5CC38C5382</RequestId>
  <ScalingGroupId>dP8VqSd9ENXPc0ciVmbc****</ScalingGroupId>
</CreateScalingGroupResponse>
```

XML format

```
{
  "RequestId": "536E9CAD-DB30-4647-AC87-AA5CC38C5382",
  "ScalingGroupId": "dP8VqSd9ENXPc0ciVmbc****"
}
```

2.3.1.7.2. ModifyScalingGroup

You can modify a scaling group.

Description

- You can call this operation to modify the attributes of a scaling group. However, the following attributes cannot be modified:
  - RegionId
  - LoadBalancerId
  - DBInstanceId
- This operation can only be called when the scaling group is in active or inactive state.
- When the specified scaling configuration needs to be modified, the InstanceType of the modified scaling configuration must be the same as the active InstanceType of the scaling configuration.

  After a new scaling configuration is added to the scaling group, the running ECS instances that were created based on the previous scaling configuration will remain unchanged.
- If the number of ECS instances does not meet the requirements of the modified MaxSize and MinSize parameters, ECS instances will be added to or removed from the group, so that the

number of instances is equal to the MaxSize or MinSize parameter.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyScalingGroup.
ScalingGroupId	String	Yes	The ID of a scaling group.
ScalingGroupName	String	No	The displayed name of the scaling group. The name must be 2 to 40 characters in length. It must start with a letter or number. It can contain numbers, uppercase letters, lowercase letters, underscores (_), hyphens (-), and periods (.). The name of the scheduled task must be unique to an Alibaba Cloud account in the region it is located.
ActiveScalingConfigurationId	String	No	The ID of the active scaling configuration in the scaling group.
MinSize	Integer	No	The minimum number of ECS instances in the scaling group. Valid values: [0, 100].
MaxSize	Integer	No	The maximum number of ECS instances in the scaling group. Valid values: [0, 100].
DefaultCooldown	Integer	No	The default cool-down time of the scaling group. Valid values: [0, 86400]. Unit: second.

Parameter	Type	Required	Description
RemovalPolicy.N	String	No	The ECS instance removal policy for the scaling group. Valid values: • OldestInstance: Remove the ECS instance that was added to the scaling group first. • NewestInstance: Remove the ECS instance that was added to the scaling group last. • OldestScalingConfiguration : Remove ECS instances that were created based on the earliest scaling configuration. A maximum of two values can be entered.

Response parameters

For more information, see Common response parameters.

Error code

For more information about common error codes, see Client errors or Server errors.

Description	Error code	Description	HTTP status code
The error message returned when the specified scaling group does not exist under this account.	InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404
The error message returned when the scaling group name already exists.	InvalidScalingGroupName.Duplicate	The specified value of parameter `<parameter name>` is duplicated.	400

Description	Error code	Description	HTTP status code
The error message returned when the specified scaling configuration does not exist in the specified scaling group.	InvalidScalingConfigurationId.NotFound	The specified scaling configuration does not exist.	404
The error message returned when the instances types of the specified scaling configuration and the active scaling configuration are different.	InvalidScalingConfigurationId.InstanceTypeMismatch	The specified scaling configuration and existing active scaling configuration have different instance type.	400
The error message returned when the specified MinSize is greater than MaxSize.	InvalidParameter.Conflict	The values of parameter `<Parameter name>` and parameter `<Parameter name>` are conflict.	400

Examples

Sample requests

```
http://ess.example.com/?Action=ModifyScalingGroup
&ScalingGroupId=cqS5QbbhmvGLcJbWoDbW****
&ScalingGroupName=ScalingGroup
&<Common request parameter>
```

Response examples

XML format

```
<ModifyScalingGroupResponse>
  <RequestId>6469DCD0-13AC-487E-85A0-CE4922908FDE</RequestId>
</ModifyScalingGroupResponse>
```

JSON format

```
{
  "RequestId": "6469DCD0-13AC-487E-85A0-CE4922908FDE"
}
```

2.3.1.7.3. EnableScalingGroup

You can call this operation to enable a specified scaling group.

Description

- You can call this operation to enable a specified scaling group.
  - After you enable a scaling group successfully, the scaling group becomes active and the specified Elastic Compute Service (ECS) instances are added to the scaling group.
  - The ECS instances specified by the interface are added to the scaling group. Then, if the number of ECS instances in it is still smaller than MinSize, additional ECS instances are automatically created to make the number equal to MinSize. For example, a scaling group is created with MinSize = 5. Two existing ECS instances are specified in the InstanceId.N parameter when the scaling group is enabled. Then, three additional ECS instances are automatically created after the two ECS instances are added by the Auto Scaling service to the scaling group.
- You can only call the operation when the scaling group is inactive.
- If the scaling group has no active scaling configuration, you must specify a scaling configuration when enabling the scaling group.
  - A single scaling group can only have one active scaling configuration at a time.
  - When you specify a new scaling configuration by using this operation, the current scaling group becomes inactive.
- The restrictions on the added ECS instances are as follows:
  - The added ECS instances must be in the same region as the scaling group.
  - The added ECS instances must have the same instance type as the active scaling configuration.
  - The added ECS instances must be running.
  - The ECS instances to be added cannot be added to another scaling group.
  - If you specify the VswitchID parameter for a scaling group, ECS instances in a classic network or ECS instances in other VPCs cannot be added to the scaling group.
  - If the VswitchID parameter is not specified for the scaling group, ECS instances of the Virtual Private Cloud (VPC) type cannot be added to the scaling group.
- The call fails if the number (total capacity) of instances specified by the interface plus instances in the scaling group is greater than MaxSize.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to EnableScalingGroup.
ScalingGroupId	String	Yes	The ID of the scaling group.
ActiveScalingConfigurationId	String	No	The ID of the scaling configuration to be activated in the scaling group.
InstanceId.N	String	No	The ID of ECS instance N to be added to the enabled scaling group. Valid values of N: 1 to 20.

Response parameters

For more information, see Common response parameters.

Error codes

For more information about errors common to all operations, see Client errors or Server errors.

Description	Error code	Error message	HTTP status code
The error message returned because the specified scaling group does not exist under this account.	InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404
The error message returned because Auto Scaling does not have full authorization with Open API.	Forbidden.Unauthorized	A required authorization for the specified action is not supplied.	403
The error message returned because the specified scaling group is currently being deleted.	IncorrectScalingGroupStatus	The current status of the specified scaling group does not support this action.	400

Description	Error code	Error message	HTTP status code
The error message returned because the specified scaling configuration does not exist in the specified scaling group.	InvalidScalingConfigurationId.NotFound	The specified scaling configuration does not exist.	404
The error message returned because the instance type of the specified scaling configuration is different from that of the active scaling configuration.	InvalidScalingConfigurationId.InstanceTypeMismatch	The specified scaling configuration and existing active scaling configuration have different instance type.	400
The error message returned because no active scaling configuration is specified for the scaling group.	MissingActiveScalingConfiguration	An active scaling configuration for the specified scaling group is not supplied.	400
The error message returned because the specified ECS instance does not exist under this account.	InvalidInstanceId.NotFound	Instance "XXX" does not exist.	404
The error message returned because the specified ECS instance and the scaling group are not in the same region.	InvalidInstanceId. RegionMismatch	Instance "XXX" and the specified scaling group are not in the same Region.	400

Description	Error code	Error message	HTTP status code
The error message returned because the specified ECS instance type is different from that of the active scaling configuration.	InvalidInstanceId.InstanceTypeMismatch	Instance "XXX" and existing active scaling configuration have different instance type.	400
The error message returned because the specified ECS instance is not running.	IncorrectInstanceStatus	The current status of instance "XXX" does not support this action.	400
The error message returned because the network type of the specified ECS instance is different from that of the scaling group.	InvalidInstanceId.NetworkTypeMismatch	The network type of instance "XXX" does not support this action.	400
The error message returned because the added ECS instance and the specified scaling group are not in the same VPC.	InvalidInstanceId.VPCMismatch	Instance "XXX" and the specified scaling group are not in the same VPC.	400
The error message returned because the specified ECS instance is already added to another scaling group.	InvalidInstanceId.InUse	Instance "XXX" is already attached to another scaling group.	400
The error message returned because the specified Server Load Balancer (SLB) instance is not active.	IncorrectLoadBalancerStatus	The current status of the specified load balancer does not support this action.	400

Description	Error code	Error message	HTTP status code
The error message returned because health check is not enabled for the specified SLB instance.	IncorrectLoadBalancerHealthCheck	The current health check type of specified load balancer does not support this action.	400
The error message returned because the network type of the ECS instance connected to the specified SLB instance is different from that of the scaling group.	InvalidLoadBalancerId.IncorrectInstanceNetworkType	The network type of the instance in specified Load Balancer does not support this action.	400
The error message returned because the ECS instance connected to the SLB instance of the specified scaling group and the VSwitch are not in the same VPC.	InvalidLoadBalancerId.VPCMismatch	The specified virtual switch and the instance in specified Load Balancer are not in the same VPC.	400
The error message returned because the specified RDS instance is not running.	IncorrectDBInstanceStatus	The current status of DB instance "XXX" does not support this action.	400
The error message returned because the total number of ECS instances (Total Capacity) exceeds MaxSize after an instance is added to the specified scaling group.	IncorrectCapacity.MaxSize	To attach the instances, the total capacity will be greater than the max size.	400

Examples

Sample requests

```
http://ess.example.com/?Action=EnableScalingGroup
&ScalingGroupId=dmIDKNcyWfzncX9MWX1****
&InstanceId.1=i-283vv****
&<Common request parameters>
```

Sample success responses

XML format

```
< EnableScalingGroupResponse>
   <RequestId>6469DCD0-13AC-487E-85A0-CE4922908FDE</RequestId>
</ EnableScalingGroupResponse>
```

JSON format

```
{
   "RequestId": "6469DCD0-13AC-487E-85A0-CE4922908FDE"
}
```

2.3.1.7.4. DisableScalingGroup

You can disable a specified scaling group.

Description

- The scaling activity that is being executed before this operation is called will be continued until it is completed. Scaling activity requests after this operation is called will be rejected.
- The operation can only be called when the scaling group is active.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DisableScalingGroup.
ScalingGroupId	String	Yes	The ID of the scaling group.

Response parameters

For more information about response parameters, see Common response parameters.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified scaling group does not exist under this account.	InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404

Examples

Sample requests

```
http://ess.example.com/?Action=DisableScalingGroup
&ScalingGroupId=dmIDKNcyWfzncX9MWX1****
&<Common request parameter>
```

Response examples

XML format

```
< DisableScalingGroupResponse>
   <RequestId>6469DCD0-13AC-487E-85A0-CE4922908FDE</RequestId>
</ DisableScalingGroupResponse>
```

JSON format

```
{
   "RequestId": "6469DCD0-13AC-487E-85A0-CE4922908FDE"
}
```

2.3.1.7.5. DeleteScalingGroup

You can delete a specified scaling group.

Description

- ForceDelete indicates whether to forcibly delete a scaling group and remove and release its ECS instances when the scaling group contains ECS instances or is undergoing a scaling activity.
- When ForceDelete is set to false, the scaling group can only be deleted when the following conditions are met:
  - Condition 1: The scaling group is not currently undergoing a scaling activity.
  - Condition 2: The number of ECS instances currently in the scaling group (Total Capacity) is 0.
  - If these two conditions are met, the scaling group can be disabled and deleted.
- If ForceDelete is set to true, we recommend that you perform the following procedure:

  - Disable the scaling group to reject new scaling activity requests. Remove all ECS instances from the scaling group after the ongoing scaling activities are completed and then delete the scaling group. Manually added ECS instances are only removed from the scaling group, whereas automatically created instances are deleted.

- Note that deleting a scaling group also deletes its scaling configurations, rules, activities, and requests.
- The following tasks and instances are not deleted: scheduled tasks, CloudMonitor alarm tasks, Server Load Balancer instances, and ApsaraDB RDS instances.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteScalingGroup.
ScalingGroupId	String	Yes	The ID of the scaling group.
ForceDelete	Bool	No	Indicates whether to forcibly delete a scaling group and remove and release its ECS instances when the scaling group contains ECS instances or is undergoing scaling activity. The default value is false, indicating that the scaling group will not be forcibly deleted.

Response parameters

For more information about response parameters, see Common response parameters.

Error code

Error message	Error code	Description	HTTP status code
The error message returned when the specified scaling group does not exist under this account.	InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404
The error message returned when Auto Scaling does not have full authorization with Open API.	Forbidden.Unauthorized	A required authorization for the specified action is not supplied.	403
The error message returned when the specified scaling group still contains ECS instances.	InstanceInUse	You cannot delete a scaling configuration or scaling group while there is an instance associated with it.	400

Examples

Sample requests

```
http://ess.example.com/?Action=DeleteScalingGroup
&ScalingGroupId=dmIDKNcyWfzncX9MWX1****
&<Common request parameters>
```

Response examples

XML format

```
<DeleteScalingGroupResponse>
    <RequestId>6469DCD0-13AC-487E-85A0-CE4922908FDE</RequestId>
</DeleteScalingGroupResponse>
```

JSON format

```
{
  "RequestId": "6469DCD0-13AC-487E-85A0-CE4922908FDE"
}
```

2.3.1.7.6. DescribeScalingGroups

You can call this operation to query information about scaling groups.

Description

A scaling group can have the following lifecycle status:

- Active: An active scaling group can receive requests to execute scaling rules and trigger scaling activities.
- Inactive: An inactive scaling group cannot receive any requests to execute scaling rules.
- Deleting: The scaling group is currently being deleted and cannot receive any requests to execute scaling rules.

Request parameters

Request parameter description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeScalingGroups.

Parameter	Type	Required	Description
RegionId	String	Yes	The ID of the region where the scaling group is located.
ScalingGroupId.N	String	No	The ID of scaling group N. Valid values of N: 1 to 20. The IDs of inactive scaling groups do not appear in the query result without any error reported.
ScalingGroupName.N	String	No	The name of scaling group N. Valid values of N: 1 to 20. The names of inactive scaling groups do not appear in the query result without any error reported.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: 50. Default value: 10.

Response parameters

Response parameter description

Parameter	Type	Description
TotalCount	Integer	The total number of scaling groups.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of entries returned per page.
ScalingGroups	ScalingGroupSetType	A collection of details about the scaling groups you are querying.

ScalingGroupSetType is a collection of ScalingGroupItemTypes.

Parameter	Type	Description
ScalingGroup	ScalingGroupItemType	The details of a scaling group.

The following table describes the attributes of ScalingGroupItemType.

Parameter	Type	Description
ScalingGroupId	String	The ID of a scaling group.
ScalingGroupName	String	The display name of a scaling group.
ActiveScalingConfigurationId	String	The ID of the active scaling configuration in a scaling group.
RegionId	String	The ID of the region where a scaling group is located.
MinSize	Integer	The minimum number of ECS instances in a scaling group.
MaxSize	Integer	The maximum number of ECS instances in a scaling group.
DefaultCooldown	Integer	The default cooldown time of a scaling group.
RemovalPolicies	RemovalPolicySetType	A collection of scaling group ECS instance removal policies.
LoadBalancerIds	List of LoadBalancerId	The Server Load Balancer instance IDs.
DBInstanceIds	DBInstanceIdSetType	The RDS instance IDs.
VSwitchId	String	The ID of the VSwitch corresponding to a scaling group.
LifecycleState	String	The lifecycle status of a scaling group.
TotalCapacity	Integer	The total number of ECS instances in a scaling group.
ActiveCapacity	Integer	The number of ECS instances that have been added to the scaling group and are running properly.

Parameter	Type	Description
PendingCapacity	Integer	The number of ECS instances that have been added to the group but have not completed relevant configurations.
RemovingCapacity	Integer	The number of ECS instances are currently being removed from the scaling group.
CreationTime	String	The time when a scaling group was created.

RemovalPolicySetType is a collection of strings.

Parameter	Type	Description
RemovalPolicy	String	The ECS instance removal policy for a scaling group.

DBInstanceIdSetType is a collection of strings.

Parameter	Type	Description
DBInstanceId	String	The ID of an RDS instance.

Error codes

For more information about errors common to all operations, see Client errors or Server errors.

Examples

Sample requests

```
http://ess.example.com/?Action=DescribeScalingGroups
&RegionId=cn-qingdao
&PageSize=50
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeScalingGroupsResponse>
  <RequestId>6393C3A8-B611-42F2-AFA6-F080FC45D5D0</RequestId>
  <TotalCount>1</TotalCount>
  <PageNumber>1</PageNumber>
  <PageSize>10</PageSize>
  <ScalingGroups>
  <ScalingGroup>
      <ActiveCapacity>1</ActiveCapacity>
      <ActiveScalingConfigurationId>dyo713cNYIB4ddEVlKbc****</ActiveScalingConfigurationId>
      <DBInstanceIds>
        <DBInstanceId>rdszzzyyuny****</DBInstanceId>
      </DBInstanceIds>
      <VSwitchId>vpc-25j4g****</VSwitchId>
      <DefaultCooldown>20</DefaultCooldown>
      <LifecycleState>Active</LifecycleState>
      <LoadBalancerId>147b46d767c-cn-qingdao-c****</LoadBalancerId>
      <MaxSize>1</MaxSize>
      <MinSize>0</MinSize>
      <PendingCapacity>0</PendingCapacity>
      <RegionId>cn-qingdao</RegionId>
      <RemovingCapacity>0</RemovingCapacity>
      <ScalingGroupId>dyrSuvBOtO1dEdIllbp****</ScalingGroupId>
      <ScalingGroupName>dyrSuvBOtO1dEdIllbp****</ScalingGroupName>
      <RemovalPolicies>
        <RemovalPolicy>OldestScalingConfiguration</RemovalPolicy>
        <RemovalPolicy>OldestInstance</RemovalPolicy>
      </RemovalPolicies>
      <TotalCapacity>1</TotalCapacity>
      <CreationTime>2014-08-14T10:58Z</CreationTime>
    </ScalingGroup>
  </ScalingGroups>
</DescribeScalingGroupsResponse>
```

JSON format

```
{
 "RequestId": "68386699-8B9E-4D5B-BC4C-75A28F6C2A00",
 "TotalCount": 1,
 "PageSize": 10,
 "PageNumber": 1,
 "ScalingGroups": {
  "ScalingGroup": [
   {
    "ScalingGroupId": "b8pYCVbIV5k9cz4PWpbe****",
    "ScalingGroupName": "b8pYCVbIV5k9cz4PWpbe****",
    "RegionId": "cn-qingdao",
    "RemovingCapacity": 0,
    "DefaultCooldown": 300,
    "MinSize": 1,
    "MaxSize": 2,
    "LifecycleState": "Inactive",
    "ActiveScalingConfigurationId": " dyo713cNYIB4ddEVlKbc****",
    "LoadBalancerId": "147b46d767c-cn-qingdao-c****",
    "PendingCapacity": 0,
    "TotalCapacity": 0,
    "ActiveCapacity": 0,
    "CreationTime": "2014-08-14T10:58Z",
    "DBInstanceIds": {
     "DBInstanceId": [
      "rdsia3u3yia****",
      "rdszzzyyuny****"
     ]
    },
    "VSwitchId":"vpc-25j4g****",
    "RemovalPolicies": {
     "RemovalPolicy": [
      "OldestScalingConfiguration",
      "OldestInstance"
     ]
    }
   }
  ]
 }
}
```

2.3.1.7.7. DescribeScalingInstances

You can query ECS instances in a scaling group. You can query ECS instances by specifying the scaling group ID, scaling configuration ID, health status, lifecycle status, and creation type.

Description

- ECS instances in a scaling group can be either automatically created or manually added.
  - Automatically created ECS instances refer to those created by Auto Scaling during scaling based on user-defined scaling configurations and rules.
  - Manually added ECS instances refer to those added to a scaling group manually by you.
- An ECS instance in a scaling group will go through the following status during its lifecycle:
  - Pending: The ECS instance is currently being added to the scaling group. For example, the instance might currently be being created, added to a Server Load Balancer instance, or added to ApsaraDB RDS.
  - InService: The ECS instance has been successfully added to the scaling group and is providing service normally.
  - Removing: The ECS instance is being removed from the scaling group.
- An ECS instance in a scaling group can be in either of the following health status:
  - Healthy: If an ECS instance is running, it is considered as healthy.
  - Unhealthy: If an ECS instance is not in the **Running** status, it will be considered as unhealthy.
- Auto Scaling automatically removes unhealthy ECS instances from the scaling group.
  - Auto Scaling will stop and release automatically created ECS instances that are unhealthy.
  - Auto Scaling will not stop or release manually added ECS instances that are unhealthy.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value DescribeScalingInstances.
RegionId	String	Yes	The ID of the region where the scaling group is located.
ScalingGroupId	String	No	The ID of the scaling group.
ScalingConfigurationId	String	No	The ID of an associated scaling configuration.
InstanceId.N	String	No	The ID of ECS instance N. N ranges from 1 to 20. The IDs of inactive instances are ignored in the query results, and no error is reported.

Parameter	Type	Required	Description
HealthStatus	String	No	The health status of an ECS instance in the scaling group. Valid values: • Healthy: The ECS instances are in running status. • Unhealthy: The ECS instances are not in running status.
LifecycleState	String	No	The lifecycle status of an ECS instance in the scaling group. Valid values: • InService: the ECS instance has been added to the scaling group and runs properly. • Pending: the ECS instance is being added to the scaling group with relevant configurations not completed. • Removing: The ECS instance is being removed from the scaling group.
CreationType	String	No	The ECS instance type. Valid values: • AutoCreated: the ECS instance is automatically created by the Auto Scaling service in the scaling group. • Added: the ECS instance is created outside the Auto Scaling service and manually added to the scaling group.
PageNumber	Integer	No	The page number of the ECS instance list. The initial value and default value are both 1.
PageSize	Integer	No	When querying by page, this parameter indicates the number of lines per page. Maximum value: 50. Default value: 10.

Response parameters

Parameter	Type	Description
TotalCount	Integer	The total number of the ECS instances.
PageNumber	Integer	The number of current page.
PageSize	Integer	The number of lines per page.
ScalingInstances	ScalingInstanceSetType	A collection of details about the ECS instances that you are querying.

ScalingInstanceSetType is a collection of ScalingInstanceItemTypes.

Parameter	Type	Description
ScalingInstance	ScalingInstanceItemType	The details of an ECS instance.

The following table describes the attributes of ScalingInstanceItemType.

Parameter	Type	Description
InstanceId	String	The ID of an ECS instance.
ScalingGroupId	String	The ID of the scaling group to which an ECS instance belongs.
ScalingConfigurationId	String	The ID of an associated scaling configuration.
HealthStatus	String	The health status of an ECS instance in the scaling group.
LifecycleState	String	The lifecycle status of an ECS instance in the scaling group.
CreationTime	String	The time at which an ECS instance was added to the scaling group.
CreationType	String	The ECS instance type.

Error code

For more information about common error codes, see Client errors or Server errors.

Examples

Sample requests

```
http://ess.example.com/?Action=DescribeScalingInstances
&RegionId=cn-qingdao
& ScalingGroupId = dBCYxE26IHKcGq1xPcT ****
&<Common request parameter>
```

Response examples

XML format

```
<DescribeScalingInstancesResponse>
  <RequestId>DFF8797F-5B73-4BD7-A7D0-03479C458F7A</RequestId>
  <TotalCount>1</TotalCount>
  <PageNumber>1</PageNumber>
  <PageSize>10</PageSize>
  <ScalingInstances>
    <ScalingInstance>
      <CreationTime>2014-08-15T17:37Z</CreationTime>
      <CreationType>AutoCreated</CreationType>
      <HealthStatus>Healthy</HealthStatus>
      <InstanceId>i-283vvyytn</InstanceId>
      <LifecycleState>Active</LifecycleState>
      <ScalingConfigurationId>eOs27Kb0oXvQcUYjEGel****</ScalingConfigurationId>
      <ScalingGroupId>dBCYxE26IHKcGq1xPcTNBwV</ScalingGroupId>
    </ScalingInstance>
  </ScalingInstances>
</DescribeScalingInstancesResponse>
```

JSON format

```
{
 "RequestId": "13305F2D-A4C2-4E6B-B7C7-0F2150842EA3",
 "TotalCount": 1,
 "PageNumber": 1,
 "PageSize": 50,
 "ScalingInstances": {
  "ScalingInstance": [
   {
    "ScalingConfigurationId": "bU5uZHcAgtzwcL4IeDea****",
    "CreationType": "AutoCreated",
    "InstanceId": "i-28sov****",
    "CreationTime": "2014-08-14T10:59Z",
    "HealthStatus": "Healthy",
    "LifecycleState": "InService",
    "ScalingGroupId": "dE9YbOdCHqaFdFZHXVdD****"
   }
  ]
 }
}
```


2.3.1.7.8. DescribeScalingActivities

You can call this operation to query information about scaling activities.

- You can query all scaling activities in a scaling group by specifying the ScalingGroupId parameter.
- You can filter query results based on the status of scaling activities.
- Only scaling activities during the last 30 days can be returned.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeScalingActivities.
RegionId	String	Yes	The ID of the region where a scaling activity is located.
ScalingGroupId	String	No	The ID of the scaling group.

Parameter	Type	Required	Description
ScalingActivityId.N	String	No	The ID of scaling activity N. Valid values of N: 1 to 10. The IDs of inactive scaling activities do not appear in the query result without any error reported.
StatusCode	String	No	The status of the scaling activities. Valid values: • Successful: The scaling activities are successful. • Warning: The scaling activities are partially successful. • Failed: The scaling activity is failed. • InProgress: The scaling activity is in progress. • Rejected: The scaling activity request is rejected.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: 50. Default value: 10.

Response parameters

Parameter	Type	Description
TotalCount	Integer	The total number of scaling activities.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of entries returned per page.
ScalingActivities	ScalingActivitySetType	A collection of the scaling activity information.

ScalingActivitySetType is a collection of ScalingActivityItemTypes.

Parameter	Type	Description
ScalingActivity	ScalingActivityItemType	The details about the scaling activity.

The following table describes the attributes of ScalingActivityItemType.

Parameter	Type	Description
ScalingActivityId	String	The ID of a scaling activity.
ScalingGroupId	String	The ID of a scaling group.
Description	String	The description of the scaling activity.
Cause	String	The trigger for a scaling activity.
StartTime	String	The time when a scaling activity started.
EndTime	String	The time when a scaling activity ended.
Progress	Integer	The execution progress of a scaling activity.
StatusCode	String	The status of the scaling activities.
StatusMessage	String	Indicates whether the scaling activity is attaching or removing Elastic Compute Service (ECS) instances to or from the scaling group.

Error codes

For more information about errors common to all operations, see Client errors or Server errors.

Examples

Sample requests

```
http://ess.example.com/?Action=DescribeScalingActivities
&RegionId=cn-qingdao
&PageSize=50
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeScalingActivitiesResponse>
  <RequestId>8FAAE99E-EB43-4838-85AD-93F62454904C</RequestId>
  <TotalCount>1</TotalCount>
  <PageNumber>1</PageNumber>
  <PageSize>10</PageSize>
  <ScalingActivities>
    <ScalingActivity>
      <Cause>A scheduled task excuete scaling rule "srtest", changing the Total Capacity from "0" to "1
". </Cause>
      <Description>Add "1" ECS instance</Description>
      <EndTime>2014-08-17T12:39Z</EndTime>
      <Progress>100</Progress>
      <ScalingActivityId>ebta5WbUzC8gcwUWvfch****</ScalingActivityId>
      <ScalingGroupId>AG6CQdPU8OKdwLjgZcJ****</ScalingGroupId>
      <StartTime>2014-08-17T12:39Z</StartTime>
      <StatusCode>Successful</StatusCode>
      <StatusMessage>"1" ECS instances is added. </StatusMessage>
    </ScalingActivity>
  </ScalingActivities>
</DescribeScalingActivitiesResponse>
```

JSON format

```
{
 "RequestId":"0A016AD6-A91F-4210-9DEE-D5BBD4270F45",
 "TotalCount":2582,
 "PageNumber":1,
 "PageSize":1,
 "ScalingActivities":{
 "ScalingActivity":[
   {
    "ScalingActivityId":"bBxOR5dhKFoccGkbTrcy****",
    "StartTime":"2014-08-18T20:49Z",
    "EndTime":"2014-08-18T20:49Z",
    "Cause":" A scheduled task excuete scaling rule \"srtest\", changing the Total Capacity from \"0\" to
\"1\".",
    "Description":" Add \"1\" ECS instance ",
    "Progress":100,
    "ScalingGroupId":"c7acXJbAJmpPcGE7G3bw****",
    "StatusCode":"Successful",
    "StatusMessage":"\"1\" ECS instances is added. "
   }
  ]
 },
}
```


2.3.1.8. Scaling configurations

2.3.1.8.1. CreateScalingConfiguration

You can call this operation to create scaling configurations.

Description

You can call this operation to create scaling configurations based on input parameters.

- Scaling configurations cannot be modified. To use a different scaling configuration, you must create a new one and activate it in the scaling group. To activate the configuration, you must modify the ActiveScalingConfigurationId parameter.
- When creating a scaling configuration, you must select an image to determine the system disk configuration of the new instance. The image contains OS and application software configurations. The system disk of an instance created based on an image is the clone of the image.
- A security group must be specified for an instance when it is created, so a scaling configuration must also have a security group specified to create instances. You must create the security group in advance. Instances in the same security group can access each other. However, instances in different security groups are isolated by firewalls and cannot access each other by default. To allow instances in different security groups to access each other, you can configure

security group policies by using the security group authorization API. A security group can contain a maximum of 1,000 instances. If a security group contains 1,000 instances and is specified again, then the creation of the instance fails and a prompt appears.

- When you create an instance, the system allocates a system disk of the appropriate size for the specified instance image. The system disk type can be specified as a cloud disk, or as an ephemeral disk if you have the permission to activate an ephemeral disk. By default, a new user does not have this permission.
- The capacity of a cloud disk cannot exceed 2,000 GiB, and the capacity of an ephemeral disk cannot exceed 1 TiB (1,024 GiB).
- A cloud disk created with an instance has a Portable attribute of False, indicating that the cloud disk cannot be added or removed. The DeleteWithInstance attribute of each created disk is True.
- A maximum of four data disks can be added to an instance. The total capacity of ephemeral disks added to an instance cannot exceed 2 TiB (2,048 GiB). This value does not include the capacity of the system disk.
- When the system disk type is cloud disk, the added data disks cannot be ephemeral disks. When the system disk type is an ephemeral disk, the added data disks can be either ephemeral or cloud disks.
- When you create an instance, the ECS system allocates a system disk of the appropriate size for the specified instance image.
- Windows operating systems are not supported on instances with memory of 512 MiB or less. 32-bit operating systems are not supported on instances with a memory greater than or equal to 4 GiB.
- A security group with a specified VPCId cannot be specified for a scaling configuration unless the VSwitchId parameter has been specified for the scaling group.
- A maximum of 10 scaling configurations can be created in a scaling group.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateScalingConfiguration.
ScalingGroupId	String	Yes	The ID of the scaling group to which the scaling configuration belongs.
ImageId	String	Yes	The ID of the image file that you specified when you create the instance.
InstanceType	String	Yes	The ECS instance type.
SecurityGroupId	String	Yes	The ID of the security group to which the instance belongs. Instances that belong to the same security group can access each other.

Parameter	Type	Required	Description
ScalingConfigurationName	String	No	The display name of the scaling rule. The name must be 2 to 40 characters in length and can contain digits, letters, underscores (_), hyphens (-), and periods (.). It must start with a digit or letter. The name must be unique in the scaling group. If this parameter is not specified, the default value is ScalingConfigurationId.
InternetMaxBandwidthIn	Integer	No	The maximum inbound bandwidth from the Internet. Unit: Mbit/s. Valid values: 1 to 200. If this parameter is not specified, the default value is 200.

IoOptimized	String	No	Specifies whether the instance is I/O-optimized. Valid values:
			• optimized: I/O-optimized.
			• If this parameter is not specified:
			  ○ Instance types of Generation I are non I/O-optimized by default.
			  ○ Instance types other than Generation I are I/O-optimized by default.
			• For non I/O-optimized instance types, this parameter cannot be specified.

SystemDisk.Category	String	No	The system disk type. Valid values: • cloud: basic disk • cloud_efficiency: ultra disk • cloud_ssd: standard SSD • ephemeral_ssd: local SSD The default value is cloud for I/O-optimized instances of Generation I types. The default value is cloud_efficiency for other types of instances.
SystemDisk.Size	Integer	No	The size of the system disk. Unit: GiB. Valid values: • cloud: 40 to 500 • cloud_efficiency: 40 to 500 • cloud_ssd: 40 to 500 • ephemeral_ssd: 40 to 500 Default value: size=max{40, ImageSize}. After this parameter is specified, the size of the system disk must be greater than or equal to max{40, ImageSize}.
DataDisk.N.Category	String	No	The type of data disk N. Valid values: • cloud: basic disk • cloud_efficiency: ultra disk • cloud_ssd: standard SSD • ephemeral_ssd: local SSD Default value: cloud.

Parameter	Type	Required	Description
DataDisk.N.Size	Integer	No	The size of data disk N. Valid values of N: 1 to 4. Unit: GiB. Valid values: • cloud: 5 to 2000 • cloud_efficiency: 20 to 32768 • cloud_ssd: 20 to 32768 • ephemeral_ssd: 5 to 800 After this parameter is specified, the size of the data disk must be greater than or equal to the specified Snapshot.
DataDisk.N.SnapshotId	String	No	The snapshot used to create data disk N. Valid values of N: 1 to 4. Once this parameter is specified, the DataDisk.N.Size parameter is ignored. The size of the specified snapshot is equal to the size of the created data disk. If the snapshot was created on or before July 15, 2013, this operation cannot be performed.
DataDisk.N.Device	String	No	The mount point of data disk N. Valid values of N: 1 to 4. When this parameter is not specified, a mount point is assigned automatically when an ECS instance is created. Valid values: /dev/xvdb, /dev/xvdc... /dev/xvdz. The parameter value is empty by default. A maximum of four values can be entered.
DataDisk.n.DeleteWithInstance	String	No	Specifies whether the data disk is released with the instance. Valid values: • true: The disk is released with the instance. • false: The disk is not released with the instance. Default value: true. This parameter takes effect only when the DataDisk.N.Category parameter is set to cloud, cloud_efficiency, or cloud_ssd. Otherwise, an error will be returned.
LoadBalancerWeight	Integer	No	The weight of the backend server. Valid values: 0 to 100. Default value: 50.
UserData	String	No	The instance user data. Encoding: Base64. The raw data size cannot exceed 16 KiB.
KeyPairName	String	No	The name of the key pair. • When you specify Windows-based ECS instances, ignore this parameter. The parameter value is empty by default. The password is valid even if you have specified this parameter. • For Linux-based instances, the use of a password to logon is forbidden during initialization.

Parameter	Type	Required	Description
RamRoleName	String	No	The name of the RAM role assigned to instances. It is provided and maintained by RAM. You can use ListRoles to query the role name. For more information about the RamRoleName parameter, see API CreateRole and ListRoles.
Tags	String	No	The tags of the instance. Tags must be specified as key-value pairs, such as {"key1":"value1","key2":"value2", ... "key5":"value5"}. A maximum of five tags can be specified. The restrictions on a key are as follows: • It can be a maximum of 64 characters. • It cannot start with aliyun. • It cannot start with http:// or https://. • It cannot be a null string. The restrictions on a value are as follows: • It can be a maximum of 128 characters. • It cannot start with aliyun. • It cannot start with http:// or https://. • It can be a null string.
InstanceTypes.N	String	No	• If you use the InstanceTypes.N parameter, ignore the InstanceType parameter. • In the InstanceTypes.N parameter, N can be a value within the range [1, 10], allowing for up to 10 instance types to be added to a scaling configuration. • In the InstanceTypes.N parameter, N indicates the priority of instance types in the current scaling configuration. The instance type with N set to 1 has the highest priority. A higher value of N indicates a lower priority. • When an instance type with the highest priority cannot be used to create an instance, the instance type with the next highest priority is automatically used.
InstanceName	String	No	The name of an ECS instance that is created based on the current scaling configuration.

Response parameters

Parameter	Type	Description
ScalingConfigurationId	String	The globally unique scaling configuration ID generated by the system.

Error codes

For more information about errors common to all operations, see Client errors or Server errors.

Description	Error code	Error message	HTTP status code
The error message returned because the specified scaling group does not exist under this account.	InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404
The error message returned because the specified scaling configuration name already exists.	InvalidScalingConfigurationName.Duplicate	The specified value of parameter <parameter name> is duplicated.	400
The error message returned because the number of scaling configurations in the specified scaling group reaches the upper limit.	QuotaExceeded.ScalingConfiguration	Scaling configuration quota exceeded in the specified scaling group.	400
The error message returned because the specified image does not exist under this account.	InvalidImageId.NotFound	The specified image does not exist.	404
The error message returned because the specified security group does not exist under this account.	InvalidSecurityGroupId.NotFound	The specified security group does not exist.	404
The error message returned because the specified instance type does not support the specified image.	InvalidImageId.InstanceTypeMismatch	The specified image does not support the specified instance type.	400
The error message returned because the network type of the specified security group is different from that of the specified scaling group.	InvalidSecurityGroupId.IncorrectNetworkType	The network type of specified Security Group does not support this action.	400
The error message returned because the specified security group and the specified VSwitch are not in the same VPC.	InvalidSecurityGroupId.VPCMismatch	The specified security group and the specified virtual switch are not in the same VPC.	400

Description	Error code	Error message	HTTP status code
The error message returned because the number of ECS instances in the specified security group reaches the upper limit.	QuotaExceeded.SecurityGroupInstance	Instance quota exceeded in the specified security group.	400
The error message returned because the instance type of the specified scaling configuration is different from that of the current scaling configuration.	InstanceType.Mismatch	The specified scaling configuration and existing active scaling configuration have different instance type.	400
The error message returned because the total capacity of mounted ephemeral disks exceeds 2 TiB (2,048 GiB).	QuotaExceeded.EphemeralDiskSize	Ephemeral disk size quota exceeded.	403
The error message returned because the type of the specified system disk conflicts with the data disk type.	InvalidParameter.Conflict	The value of parameter `<parameter name>` and parameter `<parameter name>` are conflict.	400
The error message returned because you do not have the permission to create an ephemeral disk.	InvalidSystemDiskCategory.ValueUnauthorized	The system disk category is not authorized.	403
The error message returned because the specified snapshot does not exist.	InvalidDataDiskSnapshotId.NotFound	Snapshot "XXX" does not exist.	404
The error message returned because the size of the specified snapshot exceeds the upper limit of the disk size.	InvalidDataDiskSnapshotId.SizeNotSupported	The capacity of snapshot "XXX" exceeds the size limit of the specified disk category.	400

Description	Error code	Error message	HTTP status code
The error message returned because the specified snapshot was created on or before July 15, 2013.	InvalidSnapshot.TooOld	This operation is denied because the specified snapshot is created before 2013-07-15.	403
The error message returned because the mount point of the data disk is already occupied.	InvalidDevice.InUse	Device "XXX" has been occupied.	403
The error message returned because the name of the specified key pair does not exist.	InvalidKeyPairName.NotFound	The specified KeyPairName does not exist in our records.	400
The error message returned because you specify the KeyPairName in Windows OS.	InvalidParameter	The specified value of parameter `KeyPairName` is not valid.	400
The error message returned because you specify the RAM role name for a classic network instance.	InvalidNetworkType.ForRAMRole	RAMRole can't be used For classic instance.	400
The error message returned because the specified RAM role name does not exist.	InvalidRamRole.NotFound	The specified RamRoleName does not exist.	400
The error message returned because the specified user data is not encoded in Base64 format.	InvalidUserData.Base64FormatInvalid	The specified parameter UserData must be base64 encoded.	400
The error message returned because the size of the raw user data exceeds 16 KB.	InvalidUserData.SizeExceeded	The specified parameter UserData exceeds the size.	400

Examples

Sample requests

```
http://ess.example.com/?Action=CreateScalingConfiguration
&ScalingGroupId=AG6CQdPU8OKdwLjgZcJ****
&SecurityGroupId=sg-280ih****
&ImageId=centos6u5_64_20G_aliaegis_20140703.vhd
&InstanceType=ecs.t1.xsmall
&<Common request parameters>
```

Sample success responses

XML format

```
<CreateScalingConfigurationResponse>
   <ScalingConfigurationId>eOs27Kb0oXvQcUYjEGel****</ScalingConfigurationId>
   <RequestId>5CC0AD41-08ED-4559-A683-6F56355FE068</RequestId>
</CreateScalingConfigurationResponse>
```

JSON format

```
{
   "RequestId": "5CC0AD41-08ED-4559-A683-6F56355FE068",
   "ScalingConfigurationId": "eOs27Kb0oXvQcUYjEGel****",
}
```

2.3.1.8.2. DescribeScalingConfigurations

You can call this operation to query scaling configuration information.

Description

This operation queries scaling configuration information. You can query all scaling configurations in a scaling group by specifying the ScalingGroupId parameter.

Scaling configuration status (LifecycleState) can be set to either of the following:

- Active: Scaling groups use scaling configurations in the active status to automatically create ECS instances.
- Inactive: The scaling configuration is inactive in a scaling group. The scaling group does not use scaling configurations in inactive status to automatically create ECS instances.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeScalingConfigurations.

Parameter	Type	Required	Description
RegionId	String	Yes	The ID of the region where a scaling group to which a scaling configuration belongs is located.
ScalingGroupId	String	No	The ID of the scaling group.
ScalingConfigurationId.N	String	No	The ID of scaling configuration N. Valid values of N: 1 to 10. The IDs of inactive scaling configurations do not appear in the query result without any error reported.
ScalingConfigurationName.N	String	No	The name of scaling configuration N. Valid values of N: 1 to 10. The names of inactive scaling configurations do not appear in the query result without any error reported.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: 50. Default value: 10.

Response parameters

Parameter	Type	Description
TotalCount	Integer	The total number of scaling configurations.
PageNumber	Integer	The current page number.
PageSize	Integer	The number of entries returned per page.
ScalingConfigurations	ScalingConfigurationSetType	A collection of scaling configuration information.

ScalingConfigurationSetType is a collection of ScalingConfigurationItemTypes.

Parameter	Type	Description
ScalingConfiguration	ScalingConfigurationItemType	The scaling configuration information.

The following table describes the attributes of ScalingConfigurationItemType.

Parameter	Type	Description
ScalingConfigurationId	String	The ID of the scaling configuration.
ScalingConfigurationName	String	The display name of the scaling configuration.
ScalingGroupId	String	The ID of the scaling group to which the scaling configuration belongs.
ImageId	String	The ID of an image file.
InstanceType	String	The ECS instance type.
SecurityGroupId	String	The ID of a security group.
InternetMaxBandwidthIn	Integer	The maximum inbound bandwidth from the Internet. Unit: Mbit/s.
InternetMaxBandwidthOut	Integer	The maximum outbound bandwidth to the Internet. Unit: Mbit/s.
SystemDisk.Category	String	The category of the system disk.
DataDisks	DataDiskSetType	A collection of data disk details.
LifecycleState	String	The lifecycle status of the scaling configuration in the scaling group.
CreationTime	String	The time when a scaling configuration is created.

DataDiskSetType is a collection of DataDiskItemTypes.

Parameter	Type	Description
DataDisk	DataDiskItemType	The data disk information.

The following table describes the attributes of the DataDiskItemType.

Parameter	Type	Description
Size	Integer	The size of the disk.
Category	String	The category of the disk.
SnapshotId	String	The ID of the snapshot used to create data disks.
Device	String	The data disk mounting point.

Error codes

For more information about errors common to all operations, see Client errors or Server errors.

Examples

Sample requests

```
http://ess.example.com/?Action=CreateScalingConfiguration
&RegionId=cn-qingdao
&PageSize=50
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeScalingConfigurationsResponse>
  <RequestId>804F240A-8D3E-40A1-BD68-6B333DEA2CA8</RequestId>
  <TotalCount>1</TotalCount>
  <PageNumber>1</PageNumber>
  <PageSize>50</PageSize>
  <ScalingConfigurations>
    <ScalingConfiguration>
      <CreationTime>2014-08-14T10:58Z</CreationTime>
      <ImageId>centos6u5_64_20G_alia****.vhd</ImageId>
      <InstanceType>ecs.t1.xsmall</InstanceType>
      <InternetChargeType>PayByBandwidth</InternetChargeType>
      <InternetMaxBandwidthIn>200</InternetMaxBandwidthIn>
      <InternetMaxBandwidthOut>0</InternetMaxBandwidthOut>
      <LifecycleState>Active</LifecycleState>
      <ScalingConfigurationId>bU5uZHcAgtzwcL4IeDea****</ScalingConfigurationId>
      <ScalingConfigurationName>c1908dd1-690f-4c9b-ab73-350f1f06****</ScalingConfigurationName>
      <ScalingGroupId>dE9YbOdCHqaFdFZHXVdD****</ScalingGroupId>
      <SecurityGroupId>sg-280ih****</SecurityGroupId>
      <SystemDiskCategory>cloud</SystemDiskCategory>
      <DataDisks>
       <DataDisk>
         <Size>200</Size>
         <Category>cloud</Category>
         <SnapshotId>s-280s7****</SnapshotId>
         <Device>/dev/xvdb</Device>
       </DataDisk>
      </DataDisks>
    </ScalingConfiguration>
  </ScalingConfigurations>
</DescribeScalingConfigurationsResponse>
```

JSON format

```
{
  "RequestId": "67E4324F-CE14-4C2C-9D60-5422641DB76F",
  "TotalCount": 1,
  "PageNumber": 1,
  "PageSize": 1,
  "ScalingConfigurations": {
    "ScalingConfiguration": [
      {
        "ScalingConfigurationId": "eqkz17cfW3clcPExOtL****",
        "SecurityGroupId": "sg-28oew****",
        "CreationTime": "2014-08-18T21:07Z",
        "SystemDiskCategory": "cloud",
        "InternetMaxBandwidthIn": 200,
        "InternetMaxBandwidthOut": 0,
        "LifecycleState": "Inactive",
        "InternetChargeType": "PayByBandwidth",
        "ImageId": "rhel5u7_64_20G_alia****.vhd",
        "InstanceType": "ecs.s2.small",
        "ScalingConfigurationName": "LxVdcO****",
        "ScalingGroupId": "dRsEAGdvbjR5c4SVc2bq****",
        "DataDisks":{
            "DataDisk":[{
              "Size":200,
              "Category": cloud,
              "SnapshotId": s-280s7****,
              "Device":" /dev/xvdb"
             }]
        }
      }
    ]
  }
}
```

2.3.1.8.3. DeleteScalingConfiguration

You can call this operation to delete a specified scaling configuration.

Restrictions

- A scaling configuration that is currently active in a scaling group cannot be deleted.
- If any ECS instance created based on a scaling configuration is still in the scaling group, then the

scaling configuration cannot be deleted.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteScalingConfiguration.
ScalingConfigurationId	String	Yes	The ID of the scaling configuration.

Response parameters

For more information, see Common response parameters.

Error codes

For more information about errors common to all operations, see Client errors or Server errors.

Description	Error code	Error message	HTTP status code
The error message returned because the specified scaling configuration does not exist under this account.	InvalidScalingConfigurationId.NotFound	The specified scaling configuration does not exist.	404
The error message returned because the specified scaling configuration is in any state other than inactive.	IncorrectScalingConfigurationLifecycleState	The current lifecycle state of specified scaling configuration does not support this action.	400
The error message returned because the specified scaling configuration has associated ECS instances.	InstanceInUse	You cannot delete a scaling configuration or scaling group while there is an instance associated with it.	400

Examples

Sample requests

```
http://ess.example.com/?Action=DeleteScalingConfiguration
&ScalingConfigurationId=eOs27Kb0oXvQcUYjEGel****
&<Common request parameters>
```

Sample success responses

XML format

```
<DeleteScalingConfigurationResponse>
    <RequestId>61D30272-7111-44D9-BB45-FCB55E4A1410</RequestId>
</DeleteScalingConfigurationResponse>
```

JSON format

```
{
    "RequestId": "61D30272-7111-44D9-BB45-FCB55E4A1410"
}
```

2.3.1.9. Scaling rules

2.3.1.9.1. CreateScalingRule

You can call this operation to create a scaling rule.

A scaling rule defines specific scaling actions, such as attaching or removing Elastic Compute Service (ECS) instances and determining the number of instances to be scaled.

If the number of ECS instances in a scaling group is smaller than MinSize or greater than MaxSize after the execution of a rule, Auto Scaling automatically adjusts the number of ECS instances to be added or removed by executing the "Adjust scaling group instance number to MinSize" or "Adjust scaling group instance number to MaxSize" rule.

- Example 1: A scaling group has a MaxSize of 3, a TotalCapacity of 2, and a scaling rule of adding three ECS instances. When executing this scaling rule, Auto Scaling adds only one instance to the group to prevent TotalCapacity from exceeding MaxSize. (The values in the scaling rule are not changed.)
- Example 2: A scaling group has a MinSize of 2, a TotalCapacity of 3, and a scaling rule of removing five ECS instances. When executing this scaling rule, Auto Scaling removes only one instance from the group to prevent TotalCapacity from becoming smaller than MinSize. (The values in the scaling rule are not changed.)

Description

You can create scaling rules based on input parameters.

- When the AdjustmentType value is TotalCapacity, the number of ECS instances currently in the scaling group is adjusted to the specified value. The corresponding AdjustmentValue value cannot be less than 0.
- When the AdjustmentType value is QuantityChangeInCapacity or PercentChangeInCapacity, a positive number of the AdjustmentValue value indicates adding ECS instances, and a negative number of the AdjustmentValue value indicates removing ECS instances.
- When AdjustmentType is set to PercentChangeInCapacity, Auto Scaling rounds the number of ECS instances to be scaled to the nearest integer based on the formula: Number of ECS instances to be scaled = Current number of instances × Value of AdjustmentValue/100.
- When the cool-down time (Cooldown) is specified in a scaling rule, the specified time is applied to the scaling group after this rule is executed. Otherwise, the DefaultCooldown is applied to the scaling group.

- A scaling group can have a maximum of 10 scaling rules.
- The following APIs use the unique identifier of a scaling rule (ScalingRuleAri) returned by this operation:
  - ExecuteScalingRule: You can call this operation to manually run a specified scaling rule by setting ScalingRuleAri to the identifier.
  - CreateScheduledTask: You can call this operation to create a periodically executed task for a specified scaling rule by setting ScheduledAction to the identifier.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateScalingRule.
ScalingGroupId	String	Yes	The ID of the scaling group to which the scaling rule belongs.
AdjustmentType	String	Yes	The adjustment mode of the scaling rule. Valid values: • QuantityChangeInCapacity: adds or removes a specified number of ECS instances. • PercentChangeInCapacity: adds or removes a specified proportion of ECS instances. • TotalCapacity: adds or removes ECS instances to ensure that the current scaling group has a specified number of ECS instances.
AdjustmentValue	Integer	Yes	The number of ECS instances that are added or released when scaling occurs. • QuantityChangeInCapacity: (0, 100] U (-100, 0] • PercentChangeInCapacity: [0, 10000] U [-10000, 0] • TotalCapacity: [0, 100]

Parameter	Type	Required	Description
ScalingRuleName	String	No	The display name of the scaling rule. The name must be 2 to 40 characters in length. It must start with a letter or digit. It can contain digits, uppercase letters, lowercase letters, underscores (_), hyphens (-), and periods (.). The name of a scaling rule must be unique within the scaling group that it belongs to. If you do not specify this parameter, the default value (ScalingRuleId) is used.
Cooldown	Integer	No	The cool-down time of the scaling rule. Valid values: 0 to 86,400. Unit: seconds. Default value: empty.

Response parameters

Parameter	Type	Description
ScalingRuleId	String	The globally unique scaling rule ID generated by the system.
ScalingRuleAri	String	The unique identifier of the scaling rule.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified scaling group does not exist under this account.	InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404
The error message returned when the scaling rule name already exists.	InvalidScalingRuleName.Duplicate	The specified value of parameter `<parameter name>` is duplicated.	400
The error message returned when the number of scaling rules in the specified scaling group reaches the upper limit.	QuotaExceeded.ScalingRule	Scaling rule quota exceeded in the specified scaling group.	400

Examples

Sample requests

```
http://ess.example.com/?Action=CreateScalingRule
&ScalingGroupId=AG6CQdPU8OKdwLjgZcJ****
&AdjustmentType=QuantityChangeInCapacity
&AdjustmentValue=-10
&<Common request parameter>
```

Response examples

XML format

```
<CreateScalingRuleResponse>
   <RequestId>570C84F4-A434-488A-AFA1-1E3213682B33</RequestId>
   <ScalingRuleId>eMKWG8SRNb9dBLAjweN****</ScalingRuleId>
   <ScalingRuleAri>ari:acs:ess:cn-qingdao:1344371:scalingrule/eMKWG8SRNb9dBLAjweN****</ScalingRul
eAri>
</CreateScalingRuleResponse>
```

JSON format

```
{
   "RequestId": "04F0F334-1335-436C-A1D7-6C044FE73368",
   "ScalingRuleId": "eMKWG8SRNb9dBLAjweN****",
   "ScalingRuleAri":"ari:acs:ess:cn-qingdao:1344371:scalingrule/eMKWG8SRNb9dBLAjweN****"
}
```

2.3.1.9.2. ModifyScalingRule

You can modify a scaling rule.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyScalingRule.
ScalingRuleId	String	Yes	The ID of the scaling rule.

Parameter	Type	Required	Description
AdjustmentType	String	No	The adjustment type of the scaling rule. Valid values: • QuantityChangeInCapacity: adds or removes the specified number of ECS instances. • PercentChangeInCapacity: adds or removes the specified proportion of ECS instances. • TotalCapacity: adds or removes ECS instances to ensure that the current scaling group has the specified number of ECS instances.
AdjustmentValue	Integer	No	The number of ECS instances that are added or released when scaling occurs. Valid values: • QuantityChangeInCapacity: (0, 100] U [-100, 0) • PercentChangeInCapacity: [0, 10000] U [-10000, 0] • TotalCapacity: [0, 100]
ScalingRuleName	String	No	The display name of the scaling rule. The name must be 2 to 40 characters in length. It must start with a letter or number. It can contain numbers, uppercase letters, lowercase letters, underscores (_), hyphens (-), and periods (.). The name of a scaling rule must be unique within the scaling group that it belongs to. If you do not specify this parameter, the default value (ScalingRuleId) is used.
Cooldown	Integer	No	The cool-down time of the scaling rule. Valid values: 0 to 86,400. Unit: second. Default value: empty.

Response parameters

parameter	Type	Description
ScalingRuleId	String	The globally unique scaling rule ID generated by the system.
ScalingRuleAri	String	The unique identifier of the scaling rule.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified scaling group does not exist under this account.	InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404
The error message returned when the scaling rule name already exists.	InvalidScalingRuleName.Duplicate	The specified value of parameter `<parameter name>` is duplicated.	400
The error message returned when the number of scaling rules in the specified scaling group reach the upper limit.	QuotaExceeded.ScalingRule	Scaling rule quota exceeded in the specified scaling group.	400

Examples

Sample requests

```
http://ess.example.com/?Action=CreateScalingRule
&ScalingGroupId=AG6CQdPU8OKdwLjgZcJ****
&AdjustmentType=QuantityChangeInCapacity
&AdjustmentValue=-10
&<Common request parameter>
```

Response examples

XML format

```
<CreateScalingRuleResponse>
   <RequestId>570C84F4-A434-488A-AFA1-1E3213682B33</RequestId>
   <ScalingRuleId>eMKWG8SRNb9dBLAjweN****</ScalingRuleId>
   <ScalingRuleAri>ari:acs:ess:cn-qingdao:1344371:scalingrule/eMKWG8SRNb9dBLAjweN****</ScalingRul
eAri>
</CreateScalingRuleResponse>
```

JSON format

```
{
   "RequestId": "04F0F334-1335-436C-A1D7-6C044FE73368",
   "ScalingRuleId": "eMKWG8SRNb9dBLAjweN****",
   "ScalingRuleAri":"ari:acs:ess:cn-qingdao:1344371:scalingrule/eMKWG8SRNb9dBLAjweN****"
}
```

2.3.1.9.3. DescribeScalingRules

You can query information about scaling rules. You can query all scaling rules in a scaling group by specifying the scaling group ID.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeScalingRules.
RegionId	String	Yes	The ID of the region where the scaling group to which a scaling rule belongs is located.
ScalingGroupId	String	No	The ID of the scaling group to which a scaling rule belongs.
ScalingRuleId.N	String	No	The ID of scaling rule N. N ranges from 1 to 10. The IDs of inactive scaling rules are ignored in the query result and no error is reported.
ScalingRuleName.N	String	No	The name of scaling rule N. N ranges from 1 to 10. The names of inactive scaling rules are ignored in the query result and no error is reported.

Parameter	Type	Required	Description
ScalingRuleAri.N	String	No	The unique identifier of scaling rule N. N ranges from 1 to 10. The unique identifiers of inactive scaling rules are ignored in the query result and no error is reported.
PageNumber	Integer	No	The page number of the scaling rule list. The initial value and default value are both 1.
PageSize	Integer	No	The number of lines per page in paged query. Maximum value: 50. Default value: 10.

Response parameters

parameter	Type	Description
TotalCount	Integer	The total number of scaling rules.
PageNumber	Integer	The number of the current page.
PageSize	Integer	The number of lines per page.
ScalingRules	ScalingRuleSetType	A collection of details about the scaling rules you queried.

The ScalingRuleSetType is a collection of the ScalingRuleItemType.

Parameter	Type	Description
ScalingRule	ScalingRuleItemType	The details of a scaling rule.

The following table describes the attributes of ScalingRuleItemType.

Parameter	Type	Description
ScalingRuleId	String	The ID of the scaling rule.
ScalingGroupId	String	The ID of a scaling group.
ScalingRuleName	String	The name of a scaling rule.
Cooldown	Integer	The cool-down time of the scaling rule.

Parameter	Type	Description
AdjustmentType	String	The adjustment method of the scaling rule.
AdjustmentValue	Integer	The adjustment value of the scaling rule.
ScalingRuleAri	String	The unique identifier of the scaling rule.

Error code

For more information about common error codes, see Client errors or Server errors.

Examples

Sample requests

```
http://ess.example.com/?Action=DescribeScalingRules
&RegionId=cn-qingdao
&ScalingGroupId=AG6CQdPU8OKdwLjgZcJ****
&PageSize=50
&<Common request parameter>
```

Response examples

XML format

```
<DescribeScalingRulesResponse>
  <PageNumber>1</PageNumber>
  <PageSize>50</PageSize>
  <ScalingRules>
    <ScalingRule>
      <AdjustmentType>QuantityChangeInCapacity</AdjustmentType>
      <AdjustmentValue>1</AdjustmentValue>
      <Cooldown>20</Cooldown>
      <ScalingGroupId>AG6CQdPU8OKdwLjgZcJ****</ScalingGroupId>
      <ScalingRuleAri>ari:acs:ess:cn-qingdao:1344371:scalingRule/eMKWG8SRNb9dBLAjweN****</Scali
ngRuleAri>
      <ScalingRuleId>eMKWG8SRNb9dBLAjweN****</ScalingRuleId>
      <ScalingRuleName>eMKWG8SRNb9dBLAjweN****</ScalingRuleName>
    </ScalingRule>
  </ScalingRules>
  <TotalCount>1</TotalCount>
  <RequestId>3306A40D-3412-4101-9F19-5F81E3055DAD</RequestId>
</DescribeScalingRulesResponse>
```

JSON format


```
{
 "RequestId": "B583BFEF-A779-427A-9B74-262DDD249702",
 "TotalCount": 1,
 "PageNumber": 1,
 "PageSize": 10,
 "ScalingRules": {
 "ScalingRule": [
   {
    "ScalingRuleId": "efcqrZdjlookc0UkE3dA****",
    "ScalingRuleAri": "ari:acs:ess:cn-qingdao:1344371:scalingRule/efcqrZdjlookc0UkE3dA****",
    "Cooldown": 500,
    "ScalingGroupId": "ccMvs9dcZlE5c9CtrwbX****",
    "AdjustmentType": "TotalCapacity",
    "ScalingRuleName": "KFJoxG****",
    "AdjustmentValue": 5
   }
  ]
 }
}
```


2.3.1.9.4. DeleteScalingRule

You can delete the specified scaling rule.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteScalingRule.
ScalingRuleId	String	Yes	The ID of the scaling rule.

Response parameters

For more information about response parameters, see Common response parameters.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified scaling rule does not exist under this account.	InvalidScalingRuleId.NotFound	The specified scaling rule does not exist.	404

Examples

Sample requests

```
http://ess.example.com/?Action=DeleteScalingRule
&ScalingRuleId=eMKWG8SRNb9dBLAjweN****
&<Common request parameter>
```

Response examples

XML format

```
<DeleteScalingRuleResponse>
  <RequestId>F0595173-CA3A-4597-B0D3-97A07A042B9C</RequestId>
</DeleteScalingRuleResponse>
```

JSON format

```
{
  "RequestId": "F0595173-CA3A-4597-B0D3-97A07A042B9C"
}
```

2.3.1.10. Scaling tasks

2.3.1.10.1. ExecuteScalingRule

You can run a specified scaling rule.

Description

You can call this operation to run a scaling rule.

- You can only call this operation when the scaling group is active.
- You can only call this operation when the scaling group is not currently undergoing any scaling activities.
- If the scaling group does not have any scaling activities in progress, the operation can be immediately run without the need to wait for the cooldown period to expire.
- When you call this operation successfully, Auto Scaling receives the request and the scaling activity can be run. However, this operation may be unsuccessful. You can use the returned ScalingActivityId parameter to view the status of the scaling activity.

- If the number of ECS instances to be added would leave the number of instances in the scaling group greater than MaxSize, the rule Total Capacity = MaxSize is applied.
- If the number of ECS instances to be removed would leave the number of instances in the scaling group less than MinSize, the rule Total Capacity = MinSize is applied.
- A maximum of 100 ECS instances can be scaled automatically over all groups in all regions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ExecuteScalingRule.
ScalingRuleAri	String	Yes	The unique identifier of the scaling rule.
ClientToken	String	No	This parameter is used to ensure the idempotence of the request. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information about the ClientToken, see Ensure idempotence.

Response parameters

parameter	Type	Description
ScalingActivityId	String	The ID of the scaling activity.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified scaling rule does not exist under this account.	InvalidScalingRuleAri.NotFound	The specified scaling rule Ari does not exist.	404
The error message returned when Auto Scaling does not have full authorization to Open API.	Forbidden.Unauthorized	A required authorization for the specified action is not supplied.	403

Error message	Error code	Description	HTTP status code
The error message returned when the scaling group to which the specified scaling rule belongs is inactive.	IncorrectScalingGroupStatus	The current status of the specified scaling group does not support this action.	400
The error message returned when the scaling group to which the specified scaling rule belongs has a scaling activity.	ScalingActivityInProgress	You cannot delete a scaling group or launch a new scaling activity while there is a scaling activity in progress for the specified scaling group.	400
The error message returned when the number of ECS instances under this account reach the upper limit.	QuotaExceed.Instance	Living instance quota exceeded.	400
The error message returned when the Server Load Balancer instance in the scaling group to which the specified scaling rule belongs is not active.	IncorrectLoadBalancerStatus	The current status of the specified load balancer does not support this action.	400
The error message returned when the health check is not enabled for the SLB instance in the scaling group to which the specified scaling rule belongs.	IncorrectLoadBalancerHealthCheck	The current health check type of the specified load balancer does not support this action.	400
The error message returned when the network type of the ECS instance connected to the specified SLB instance is different from that of the scaling group.	InvalidLoadBalancerId.IncorrectInstanceNetworkType	The network type of the instance in the specified load balancer does not support this action.	400

Error message	Error code	Description	HTTP status code
The error message returned when the ECS instance connected to the SLB instance of the specified scaling group and the VSwitch are not in the same VPC.	InvalidLoadBalancerId.VPCMismatch	The specified virtual switch and the instance in the specified load balancer are not in the same VPC.	400
The error message returned when the RDS instance in the scaling group to which the specified scaling rule belongs is not running.	IncorrectDBInstanceStatus	The current status of DB instance "XXX" does not support this action.	400
The error message returned when the number of IP addresses in the RDS instance whitelist in the scaling group to which the scaling rule belongs reach the upper limit.	QuotaExceeded.DBInstanceSecurityIP	Security IP quota exceeded in DB instance "XXX".	400
The error message returned when the number of ECS instances already added to the specified security group reach the upper limit.	QuotaExceeded.SecurityGroupInstance	Instance quota exceeded in the specified security group.	400
The error message returned when there is no change in the number of instances in the scaling group after the scaling rule is executed.	IncorrectCapacity.NoChange	To execute the specified scaling rule, the total capacity will not change.	400
The error message returned when the number of ECS instances of Auto Scaling reach the upper limit.	QuotaExceeded.ScalingInstance	Scaling instance quota exceeded.	400
The error message returned when the ECS instance or disk of the specified type cannot be created in the specified region.	ResourceNotAvailable.ECS	The specified region or zone does not offer the specified disk or instance category.	400

Examples

Sample requests

```
http://ess.example.com/?Action=ExecuteScalingRule
&ScalingRuleAri=ari:acs:ess:cn-qingdao:1344371:scalingRule/cCBpdYdQuBe2cUxOdu6****
&<Common request parameter>
```

Response examples

XML format

```
<ExecuteScalingRuleResponse>
  <RequestId>262216B9-F9D4-4D16-BE9B-BD1C39A4F42B</RequestId>
  <ScalingActivityId>ebta5WbUzC8gcwUWvfch****</ScalingActivityId>
</ExecuteScalingRuleResponse>
```

JSON format

```
{
   "RequestId": "6469DCD0-13AC-487E-85A0-CE4922908FDE",
   "ScalingActivityId": "ebta5WbUzC8gcwUWvfch****"
}
```

2.3.1.10.2. AttachInstances

You can call this operation to add Elastic Compute Service (ECS) instances to a specified scaling group.

Description

- The restrictions on an added ECS instance are as follows:
  - The added ECS instance and the scaling group must be in the same region.
  - The added ECS instance must be running.
  - The added ECS instance cannot be added to another scaling group.
  - If the VSwitchId parameter is specified for a scaling group, Elastic Compute Service instances which reside in a classic network or in other VPCs cannot be added to the scaling group.
  - If the VSwitchId parameter is not specified for a scaling group, ECS instances of the VPC network type cannot be added to the scaling group.
- This operation can only be called when the scaling group is active.
- This operation can only be called when the scaling group is not currently undergoing any scaling activities.
- If the scaling group does not have any scaling activities in progress, the operation can be immediately run without the need to wait for the cooldown period to expire.
- When this operation is called, Auto Scaling receives the request. However, it is not guaranteed that the scaling activity can be run as intended. You can use the returned ScalingActivityId

parameter to view the status of the scaling activity.

- When the sum of the number of ECS instances currently in the scaling group (Total Capacity) and the number of instances to be added specified by this operation is greater than MaxSize, calling the operation fails.
- Manually added ECS instances are not associated with the active scaling configuration of the scaling group.

Request parameters

Request parameter description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AttachInstances.
ScalingGroupId	String	Yes	The ID of the scaling group.
InstanceId.N	String	Yes	The ID of the ECS instance. N ranges from 1 to 20.

Response parameters

parameter	Type	Description
ScalingActivityId	String	The ID of the scaling activity.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified scaling group does not exist under this account.	InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404
The error message returned when Auto Scaling does not have full authorization with Open API.	Forbidden.Unauthorized	A required authorization for the specified action is not supplied.	403

Error message	Error code	Description	HTTP status code
The error message returned when the specified scaling group is inactive.	IncorrectScalingGroupStatus	The current status of the specified scaling group does not support this action.	400
The error message returned when the specified ECS instance does not exist under this account.	InvalidInstanceId.NotFound	Instance "XXX" does not exist.	404
The error message returned when the specified Elastic Compute Service instance and the scaling group are not in the same region.	InvalidInstanceId. RegionMismatch	Instance "XXX" and the specified scaling group are not in the same Region.	400
The error message returned when the specified Elastic Compute Service instance type is different from that of the active scaling configuration.	InvalidInstanceId.InstanceTypeMismatch	Instance "XXX" and existing active scaling configurations have different instance types.	400
The error message returned when the specified Elastic Compute Service instance is not running.	IncorrectInstanceStatus	The current status of instance "XXX" does not support this action.	400
The error message returned when the network type of the specified ECS instance is different from that of the scaling group.	InvalidInstanceId. NetworkTypeMismatch	The network type of instance "XXX" does not support this action.	400

Error message	Error code	Description	HTTP status code
The error message returned when the added ECS instance and the specified scaling group are not in the same Virtual Private Cloud.	InvalidInstanceId.VPCMismatch	Instance "XXX" and the specified scaling group are not in the same Virtual Private Cloud.	400
The error message returned when the specified ECS instance is added to another scaling group.	InvalidInstanceId.InUse	Instance "XXX" is already added to another scaling group.	400
The error message returned when the specified scaling group has a scaling activity in progress.	ScalingActivityInProgress	You cannot delete a scaling group or launch a new scaling activity while there is a scaling activity in progress for the specified scaling group.	400
The error message returned when the SLB instance in the specified scaling group is inactive.	IncorrectLoadBalancerStatus	The current status of the specified load balancer does not support this action.	400
The error message returned when the health check is not enabled for the specified SLB instance.	IncorrectLoadBalancerHealthCheck	The current health check type of specified load balancer does not support this action.	400
The error message returned when the network type of the ECS instance connected to the specified SLB instance is different from that of the scaling group.	InvalidLoadBalancerId.IncorrectInstanceNetworkType	The network type of the instance in the specified load balancer does not support this action.	400

Error message	Error code	Description	HTTP status code
The error message returned when the Elastic Compute Service instance connected to the SLB instance of the specified scaling group and the VSwitch are not in the same VPC.	InvalidLoadBalancerId.VPCMismatch	The specified virtual switch and the instance in the specified load balancer are not in the same Virtual Private Cloud.	400
The error message returned when the RDS instance in the specified scaling group is not running.	IncorrectDBInstanceStatus	The current status of DB instance "XXX" does not support this action.	400
The error message returned when the number of IP addresses in the specified RDS instance whitelist reach the upper limit.	QuotaExceeded.DBInstanceSecurityIP	Security IP quota exceeded in DB instance "XXX".	400
The error message returned when the number of ECS instances in the specified security group reach the upper limit.	QuotaExceeded.SecurityGroupInstance	Instance quota exceeded in the specified security group.	400
The error message returned when the total number of ECS instances (Total Capacity) exceed MaxSize after an instance is added to the specified scaling group.	IncorrectCapacity.MaxSize	To add the instances, the total capacity will be greater than the MaxSize.	400

Examples

Sample requests

```
http://ess.example.com/?Action=AttachInstances
&ScalingGroupId=AG6CQdPU8OKdwLjgZcJ****
&InstanceId. 1=i-28wt4****
&<Common request parameter>
```

Response examples

XML format

```
<AttachInstancesResponse>
   <RequestId>DD0309B7-2613-4792-9B86-275906695253</RequestId>
   <ScalingActivityId>bybj9OcaOT4ucPMbFhcqHfA3</ScalingActivityId>
</AttachInstancesResponse>
```

JSON format

```
{
   "RequestId": "6469DCD0-13AC-487E-85A0-CE4922908FDE",
   "ScalingActivityId":"ebta5WbUzC8gcwUWvfch****"
}
```

2.3.1.10.3. RemoveInstances

You can remove ECS instances from a specified scaling group.

Description

- When an ECS instance automatically created by Auto Scaling is removed from a scaling group, the ECS instance is stopped and released.
- When a manually added ECS instance is removed from a scaling group, the ECS instance is neither stopped nor released.
- This operation can only be called when the scaling group is active.
- You can only call this operation when the scaling group does not currently have any scaling activities.
- If no scaling activity in the scaling group is in progress, the operation can be run immediately without waiting for cooldown to expire.
- When this operation is called, Auto Scaling receives the request. However, it is not guaranteed that the scaling activity can be run as intended. You can use the returned ScalingActivityId parameter to check the status of the scaling activity.
- When the difference between the number of ECS instances currently in the scaling group (Total Capacity) and the number of ECS instances to be removed is smaller than MinSize, calling the operation fails.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RemoveInstances.
ScalingGroupId	String	Yes	The ID of the scaling group.
InstanceId.N	String	Yes	The ID of the ECS instance. N ranges from 1 to 20.

Response parameters

Parameter	Type	Description
ScalingActivityId	String	The ID of the scaling activity.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified scaling group does not exist under this account.	InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404
The error message returned when the specified ECS instance does not exist in the scaling group.	InvalidInstanceId.NotFound	Instance "XXX" does not exist.	404
The error message returned when Auto Scaling does not have full authorization to Open API.	Forbidden.Unauthorized	The required authorization for the specified action is not supplied.	403
The error message returned when the specified scaling group is not active.	IncorrectScalingGroupStatus	The current status of the specified scaling group does not support this action.	400
The error message returned when the specified scaling group is currently undergoing a scaling activity.	ScalingActivityInProgress	You cannot delete a scaling group or launch a new scaling activity while there is a scaling activity in progress for the specified scaling group.	400

Error message	Error code	Description	HTTP status code
The error message returned when the SLB instance in the scaling group to which the specified scaling rule belongs is inactive.	IncorrectLoadBalancerStatus	The current status of the specified load balancer does not support this action.	400
The error message returned when the RDS instance in the scaling group to which the specified scaling rule belongs is not running.	IncorrectDBInstanceStatus	The current status of DB instance "XXX" does not support this action.	400
The error message returned when the number of ECS instances to be removed will leave fewer total ECS instances than MinSize.	IncorrectCapacity.MinSize	To remove the instances, the total capacity will be lesser than the MinSize.	400

Examples

Sample requests

```
http://ess.example.com/?Action=RemoveInstances
&ScalingGroupId=AG6CQdPU8OKdwLjgZcJ****
&InstanceId. 1=i-28wt4****
&<Common request parameter>
```

Response examples

XML format

```
<RemoveInstancesResponse>
   <RequestId>DD0309B7-2613-4792-9B86-275906695253</RequestId>
   <ScalingActivityId>bybj9OcaOT4ucPMbFhcq****</ScalingActivityId>
</RemoveInstancesResponse>
```

JSON format

```
{
   "RequestId": "6469DCD0-13AC-487E-85A0-CE4922908FDE",
   "ScalingActivityId": "ebta5WbUzC8gcwUWvfch****"
}
```

2.3.1.10.4. DetachInstances

You can call this operation to remove one or more Elastic Compute Service (ECS) instances from a scaling group.

Description

After an ECS instance is removed, it can either exist independent of any scaling group or be added to another scaling group. For more information about AttachInstances, see AttachInstances. Removing an ECS instance does not stop or release it. You can manually stop or release an ECS instance as needed. When calling this operation, you must take note of the following points:

- The specified scaling group must be enabled.
- The specified scaling group must not have any scaling activities in progress.
- If there is no scaling activity currently in progress in the scaling group, the operation can be immediately run without waiting for the cooldown period to expire.
- When this operation is called successfully, Auto Scaling receives the request. The scaling activity can be triggered, but it is not guaranteed that the scaling activity can be successfully run. You can use the ScalingActivityId parameter returned in the response to query the status of the scaling activity.
- The difference between the number of ECS instances currently in the specified scaling group and the number of ECS instances to be removed must not be smaller than MinSize.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DetachInstances.
ScalingGroupId	String	Yes	The ID of the scaling group.
InstanceId.N	String	Yes	The ID of the ECS instance. N can be an integer from 1 to 20.

Response parameters

Parameter	Type	Description
RequestId	String	The request ID.
ScalingActivityId	String	The ID of the scaling activity.

Examples

Sample requests

```
http://ess.example.com/?Action=DetachInstances
&ScalingGroupId=AG6CQdPU8OKdwLj****
&InstanceId. 1=i-28wt4****
& <Common request parameters>
```

Response examples

XML format

```
<DetachInstancesResponse>
   <RequestId>04F0F334-1335-436C-A1D7-6C044FE73368</RequestId>
   <ScalingActivityId>asa-xxxxxxxxx</ScalingActivityId>
</DetachInstancesResponse>
```

JSON format

```
{
   "RequestId": "04F0F334-1335-436C-A1D7-6C044FE73368",
   "ScalingActivityId":"asa-****"
}
```

Error code

Error code	Error message	HTTP status code	Description
IncorrectScalingGroupStatus	The current status of the specified scaling group does not support this action.	400	The error message returned when the specified scaling group is not enabled.
ScalingActivityInProgress	You cannot delete a scaling group or launch a new scaling activity while there is a scaling activity in progress for the specified scaling group.	400	The error message returned when the specified scaling group currently has a scaling activity.
IncorrectLoadBalancerStatus	The current status of the specified load balancer does not support this action.	400	The error message returned when the SLB instance is not active in the specified scaling group.
IncorrectDBInstanceStatus	The current status of DB instance "XXX" does not support this action.	400	The error message returned when the RDS instance in the specified scaling group is not running.

Error code	Error message	HTTP status code	Description
IncorrectCapacity.MinSize	To remove the instances, the total capacity will be lesser than the MinSize.	400	The error message returned when removing a number of ECS instances from a scaling group, which will cause the group to contain fewer ECS instances than the MinSize value.
Forbidden.Unauthorized	A required authorization for the specified action is not supplied.	403	The error message returned when you are not authorized to call this operation.
InvalidScalingGroupId.NotFound	The specified scaling group does not exist.	404	The error message returned when the specified scaling group does not exist.
InvalidInstanceId.NotFound	Instance "XXX" does not exist.	404	The error message returned when the specified ECS instance does not exist.

2.3.1.11. Scheduled tasks

2.3.1.11.1. CreateScheduledTask

You can create scheduled tasks based on input parameters.

Description

- You can create a maximum of 20 scheduled tasks.
- When a scheduled task fails to trigger due to an ongoing scaling activity in a scaling group or the scaling group is disabled, the scheduled task will be retried for the duration of the launch expiration time. After the duration of the launch expiration time, a scheduled task that has failed to be triggerred will be abandoned.
- If multiple tasks are scheduled at similar times to run scaling rules in the same group, the earliest task will run its scaling activity first. Other tasks will make attempts to execute their rules during their launch expiration time, but only one scaling activity can be run in a scaling group at a time. If the previous scaling activity is completed while another scheduled task is making triggering attempts during its launch expiration time, the scaling rule is executed and the corresponding scaling activity is triggered.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateScheduledTask.
RegionId	String	Yes	The ID of the region where the scheduled task is located.
ScheduledAction	String	Yes	The operations to be perform when the scheduled task is triggered. Enter the unique identifier of the scaling rule.
LaunchTime	String	Yes	The time at which the scheduled task was triggered. UTC time is used and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mm:ssZ. If the RecurrenceType parameter is specified, the task will be repeatedly run starting at the time specified by LaunchTime. If the RecurrenceType parameter is not specified, the task will be only executed once at the time specified by LaunchTime. You cannot enter a time point later than 90 days from the scheduled task creation or modification.
ScheduledTaskName	String	No	The display name of the scheduled task. The name must be 2 to 40 characters in length. It must start with a letter or number. It can contain numbers, uppercase letters, lowercase letters, underscores (_), hyphens (-), and periods (.). The name of the scheduled task must be unique within the same region for the same Alibaba Cloud account. If you do not specify this parameter, the default value (ScheduledScalingTaskId) is used.
Description	String	No	The description of the scheduled task. The description must be 2 to 200 characters in length.

Parameter	Type	Required	Description
LaunchExpirationTime	Integer	No	You can retry the task during this time period after the scheduled task fails. Unit: second. Default value: 600. Valid values: [0, 21600].
RecurrenceType	String	No	The recurrence type of the repeated task. Valid values: • Daily: The scheduled task is executed once after the specified number of days. • Weekly: The scheduled task is executed on each specified day of a week. • Monthly: The scheduled task is executed on each specified day of a month. • RecurrenceType, RecurrenceValue, and RecurrenceEndTime must be valid.
RecurrenceValue	String	No	The recurrence value of the scheduled task to be repeated. • Daily: A single value ranging from 1 to 31 can be entered. • Weekly: You can enter multiple values. You can specify numbers from 0 to 6 for days from Sunday to Saturday in sequence. Multiple values must be separated by commas (,). • Monthly: You can enter two values ranging from 1 to 31. The format is A-B. B must be greater than or equal to A. If you set the parameter to RecurrenceValue, you must also set both RecurrenceEndTime and RecurrenceType.

Parameter	Type	Required	Description
RecurrenceEndTime	String	No	The end time of the scheduled task to be repeated. UTC time is used and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ. You cannot enter a time point later than 90 days from the scheduled task creation or modification. If you set the parameter to RecurrenceValue, you must also set the both RecurrenceEndTime and RecurrenceType.
TaskEnabled	Bool	No	Indicates whether to start the scheduled task. • true: start the task. • false: stop the task.

Response parameters

Parameter	Type	Description
ScheduledTaskId	String	The globally unique scaling task ID generated by the system.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified region does not exist.	InvalidRegionId.NotFound	The specified region does not exist.	404
The error message returned when the name of the scheduled task already exists.	InvalidScheduledTaskName.Duplicate	The specified value of parameter `<parameter name>` is duplicated.	400
The error message returned when the specified ScheduledAction parameter and the scheduled task are not in the same region.	ScheduledAction.RegionMismatch	The specified scheduled task and the specified scheduled action are not in the same Region.	400

Error message	Error code	Description	HTTP status code
The error message returned when the number of scheduled tasks created by you reach the upper limit.	QuotaExceeded.ScheduledTask	Scheduled task quota exceeded.	400

Examples

Sample requests

```
http://ess.example.com/?Action=CreateScheduledTask
&RegionId=cn-qingdao
&LaunchTime=2014-08-17T16:52Z
&RecurrenceType=Daily
&RecurrenceValue=1
&RecurrenceEndTime=2014-08-17T16:55Z
&ScheduledAction=ari:acs:ess:cn-qingdao:1344371:scalingRule/cCBpdYdQuBe2cUxOdu6****
& <Common request parameters>
```

Response examples

XML format

```
<CreateScheduledTaskResponse>
   <RequestId>0F02D931-2B12-44D7-A0E9-39925C13D15E</RequestId>
   <ScheduledTaskId>edRtShc57WGXdt8TlPbr****</ScheduledTaskId>
</CreateScheduledTaskResponse>
```

JSON format

```
{
   "RequestId": "04F0F334-1335-436C-A1D7-6C044FE73368",
   "ScheduledTaskId": "edRtShc57WGXdt8TlPbr****"
}
```

2.3.1.11.2. ModifyScheduledTask

You can modify a scheduled task.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyScheduledTask.
ScheduledTaskId	String	Yes	The ID of the scheduled task.
ScheduledTaskName	String	No	The display name of the scaling rule. The name must be 2 to 40 characters in length. It must start with a letter or number. It can contain numbers, uppercase letters, lowercase letters, underscores (_), hyphens (-), and periods (.). The name of the scheduled task must be unique within the same region for the same Alibaba Cloud account. If you do not specify this parameter, the default value (ScheduledScalingTaskId) is used.
Description	String	No	The description of the scheduled task. It must be 2 to 200 characters in length.
ScheduledAction	String	No	The operation performed when the scheduled task is triggered. Enter the unique identifier of the scaling rule.
LaunchTime	String	No	The time at which the scheduled task is triggered. UTC time is used and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mm:ssZ. If the RecurrenceType parameter is specified, the task will be executed repeatedly at the time specified by LaunchTime. If the RecurrenceType parameter is not specified, the task is only executed once at the time specified by LaunchTime. You cannot enter a time point later than 90 days from the date of the scheduled task creation or modification.

Parameter	Type	Required	Description
LaunchExpirationTime	Integer	No	You can retry the task during this time period after the scheduled task fails. Unit: second. Default value: 600. Valid values: [0, 21600].
RecurrenceType	String	No	The type of the scheduled task to be repeated. Valid values: • Daily: The scheduled task is executed once after the specified number of days. • Weekly: The scheduled task is run on each specified day of the week. • Monthly: The scheduled task is run on each specified day of the month. After the scheduled task is modified, RecurrenceType, RecurrenceValue, and RecurrenceEndTime must be valid.

Parameter	Type	Required	Description
RecurrenceValue	String	No	The value determining how often a scheduled task recurs. • Daily: indicates the interval of days that a scheduled task is repeated on. You can enter a single value ranging from 1 to 31. • Weekly: indicates which days of the week that a scheduled task is repeated on. You can enter multiple values separated by commas (,). You can specify numbers from 0 to 6 for days from Sunday to Saturday in sequence. Multiple values must be separated by commas (,). • Monthly: You can enter two values ranging from 1 to 31. The format is A-B. B must be greater than or equal to A. After the scheduled task is modified, RecurrenceType, RecurrenceValue, and RecurrenceEndTime must be valid.
RecurrenceEndTime	String	No	The end time of the scheduled task to be repeated. UTC time is used and complies with the ISO 8601 standard. The format is YYYY-MM-DDThh:mmZ. You cannot enter a time point later than 90 days from the date of scheduled task creation or modification. After the scheduled task is modified, RecurrenceType, RecurrenceValue, and RecurrenceEndTime must be valid.

Parameter	Type	Required	Description
TaskEnabled	Bool	No	Indicates whether to start the scheduled task. • true: indicates the task is started. • false: indicates the task is stopped. Default value: true.

Response parameters

For more information about response parameters, see Common response parameters.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified scheduled task does not exist under this account.	InvalidScheduledTaskId.NotFound	The specified scheduled task does not exist.	404
The error message returned when the name of the scheduled task already exists.	InvalidScheduledTaskName.Duplicate	The specified value of parameter `<parameter name>` is duplicated.	400
The error message returned when the specified ScheduledAction parameter and the scheduled task are not in the same region.	ScheduledAction.RegionMismatch	The specified scheduled task and the specified scheduled action are not in the same Region.	400

Examples

Sample requests

```
http://ess.example.com/?Action=ModifyScheduledTask
&ScheduledTaskId=edRtShc57WGXdt8TlPbr****
&LaunchTime=2014-08-18T10:52Z
&RecurrenceEndTime=2014-08-20T16:55Z
&<Common request parameter>
```

Response examples

XML format

```
<ModifyScheduledTaskResponse>
    <RequestId>F9372E8D-C163-471F-BEB4-3A02B3CE176E</RequestId>
</ModifyScheduledTaskResponse>
```

JSON format

```
{
    "RequestId": "04F0F334-1335-436C-A1D7-6C044FE73368"
}
```

2.3.1.11.3. DescribeScheduledTasks

You can query information about a scheduled task. You can query information about relevant scheduled tasks by specifying the ScheduledAction parameter.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeScheduledTasks.
RegionId	String	Yes	The ID of the region where a scheduled task is located.
ScheduledTaskId.N	String	No	The ID of scheduled task N. N ranges from 1 to 20. The IDs of inactive scheduled tasks are ignored in the query result and no error is reported.
ScheduledTaskName.N	String	No	The display name of scheduled task N. N ranges from 1 to 20. The names of inactive scheduled tasks are ignored in the query result and no error is reported.
ScheduledAction.N	String	No	The operation performed when scheduled task N is triggered. N ranges from 1 to 20. Inactive operations are ignored in the query result and no error is reported.
PageNumber	Integer	No	The page number of the scheduled task list. The initial value and default value are both 1.

Parameter	Type	Required	Description
PageSize	Integer	No	The number of lines per page in paged query. Maximum value: 50. Default value: 10.

Response parameters

Parameter	Type	Description
TotalCount	Integer	The total number of scheduled tasks.
PageNumber	Integer	The number of the current page.
PageSize	Integer	The number of lines per page.
ScheduledTasks	ScheduledTaskSetType	A collection of details about the scheduled tasks you queried.

ScheduledTaskSetType is a collection of ScheduledTaskItemType.

Parameter	Type	Description
ScheduledTask	ScheduledTaskItemType	The details of the scheduled task.

The following table describes the attributes of ScheduledTaskItemType.

Parameter	Type	Description
ScheduledTaskId	String	The ID of the scheduled task.
ScheduledTaskName	String	The name of the scheduled task.
Description	String	The description of the scheduled task.
ScheduledAction	String	The operation performed when a scheduled task is triggered.
LaunchTime	String	The time at which the scheduled task is triggered.
LaunchExpirationTime	Integer	You can retry the task during this time period after the scheduled task fails.
RecurrenceType	String	The type of the scheduled task to be repeated.
RecurrenceValue	String	The recurring value of the scheduled task to be repeated.
RecurrenceEndTime	String	The end of the task recurrence period.

Parameter	Type	Description
TaskEnabled	Bool	Indicates whether to enable a scheduled task.

Error code

For more information about common error codes, see Client errors or Server errors.

Examples

Sample requests

```
http://ess.example.com/?Action=DescribeScheduledTasks
&RegionId=cn-qingdao
&ScheduledTaskId. 1=edRtShc57WGXdt8TlPbr****
&PageSize=50
&<Common request parameter>
```

Response examples

XML format

```
<DescribeScheduledTasksResponse>
  <RequestId>B9B498DA-E836-45FF-83C7-1930492FDD5A</RequestId>
  <TotalCount>1</TotalCount>
  <PageNumber>1</PageNumber>
  <PageSize>50</PageSize>
  <ScheduledTasks>
    <ScheduledTask>
      <Description/>
      <LaunchExpirationTime>600</LaunchExpirationTime>
      <LaunchTime>2014-08-18T10:52Z</LaunchTime>
      <RecurrenceEndTime>2014-08-20T16:55Z</RecurrenceEndTime>
      <RecurrenceType>Daily</RecurrenceType>
      <RecurrenceValue>1</RecurrenceValue>
      <ScheduledAction>ari:acs:ess:cn-qingdao:1344371:scalingrule/cCBpdYdQuBe2cUxOdu6****</Sch
eduledAction>
      <ScheduledTaskId>edRtShc57WGXdt8TlPbr****</ScheduledTaskId>
      <ScheduledTaskName>edRtShc57WGXdt8TlPbr****</ScheduledTaskName>
      <TaskEnabled>true</TaskEnabled>
    </ScheduledTask>
  </ScheduledTasks>
</DescribeScheduledTasksResponse>
```

JSON format

```
{
 "RequestId": "43434132-91C4-4264-8343-681130760A5C",
 "TotalCount": 1,
 "PageSize": 1,
 "PageNumber": 1,
 "ScheduledTasks": {
  "ScheduledTask": [
   {
    "TaskEnabled": true,
    "ScheduledTaskId": "b27CLSc8T478c2iqHr6****",
    "Description": "This is a scheduled task test.",
    "ScheduledTaskName": "9906a33f-14eb-42b8-8bdb-ee8cdf91****",
    "LaunchExpirationTime": 120,
    "RecurrenceType": "Daily",
    "RecurrenceEndTime": "2014-08-13T19:19Z",
    "LaunchTime": "2014-08-12T17:55Z",
    "RecurrenceValue": "1",
    "ScheduledAction": "ari:acs:ess:cn-qingdao:1344371:scalingrule/qGx9feK1giadmp3XKer****"
   }
  ]
 }
}
```


2.3.1.11.4. DeleteScheduledTask

You can call this operation to delete the specified scheduled task.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteScheduledTask.
ScheduledTaskId	String	Yes	The ID of the scheduled task.

Response parameters

For more information about response parameters, see Common response parameters.

Error code

For more information about common error codes, see Client errors or Server errors.

Error message	Error code	Description	HTTP status code
The error message returned when the specified scheduled task does not exist under this account.	InvalidScheduledTaskId.NotFound	The specified scheduled task does not exist.	404

Examples

Sample requests

```
http://ess.example.com/?Action=DeleteScheduledTask
&ScheduledTaskId=edRtShc57WGXdt8TlPbr****
&<Common request parameter>
```

Response examples

XML format

```
<DeleteScheduledTaskResponse>
    <RequestId>7683D637-CF8A-41DC-85A8-E128061E65FC</RequestId>
</DeleteScheduledTaskResponse>
```

JSON format

```
{
    "RequestId": "04F0F334-1335-436C-A1D7-6C044FE73368"
}
```

2.3.1.12. Error codes

2.3.1.12.1. Client errors

Client error description

Description	Error code	Error message	HTTP status code
The error message returned because a required parameter is not specified.	MissingParameter	The input parameter `<parameter name>` that is mandatory for processing this request is not supplied.	400

Description	Error code	Error message	HTTP status code
The error message returned because the specified parameter value is invalid.	InvalidParameter	The specified value of parameter `<parameter name>` is not valid.	400
The error message returned because the specified operation is invalid.	UnsupportedOperation	The specified action is not supported.	400
The error message returned because the specified version is invalid.	NoSuchVersion	The specified version does not exist.	400
The error message returned because the specified operation is denied by the throttling system.	Throttling	Request was denied due to request throttling.	400
The error message returned because the specified AccessKey pair is invalid.	InvalidAccessKeyId.NotFound	The Access Key ID provided does not exist in our records.	400
The error message returned because the specified operation is forbidden.	Forbidden	Users are not authorized to operate on the specified resource.	403
The error message returned because the specified operation is denied by the risk control system.	Forbidden.RiskControl	This operation is forbidden by Aliyun Risk Control system.	403
The error message returned because the specified signature is invalid.	SignatureDoesNotMatch	The signature we calculated does not match the one you provided.	403
The error message returned because you are not authorized to call ESS API operations.	Forbidden.Unsubscribed	Do not have permission to access this API.	403
The error message returned because the real-name verification is not completed.	Forbidden.UserVerification	Your user account is not verified by Aliyun.	403

Description	Error code	Error message	HTTP status code
The error message returned because the specified region does not support ESS.	ResourceNotAvailable	Resource you requested is not available in this region or zone.	400

2.3.1.12.2. Server errors

Server error description

Description	Error code	Error message	HTTPstatus code
The error message returned because the server fails to process this request.	InternalError	The request processing has failed due to some unknown error, exception or failure.	500
The error message returned because the server fails to process this request.	ServiceUnavailable	The request has failed due to a temporary failure of the server.	503

2.3.1.13. Ensure idempotence

If a request times out or an internal server error occurs when the ExecuteScalingRule operation is called to create or release ECS instances, the client may try to resend the request. In this case, the client provides the ClientToken parameter to prevent the server from creating or releasing more instances than intended. The ClientToken parameter also ensures that requests are idempotent. ClientToken is a unique and case-sensitive string that is generated by the client. The token can only contain ASCII characters and cannot exceed 64 characters in length.

If the same ClientToken value is used to call the CreateInstance operation, the server will return identical request results with the same ScalingActivityId values. Therefore, when the request is resent due to an error, the same ClientToken value can ensure that only one scaling activity is created and the corresponding ScalingActivityId value is obtained.

If the provided ClientToken has already been used but with different request parameters, ESS will return the `IdempotentParameterMismatch` error code. Note: You must specify the SignatureNonce, Timestamp, and Signature parameters again before the request is resent because ESS uses SignatureNonce to prevent replay attacks and Timestamp to mark the time of each request. Therefore, you must provide different SignatureNonce and Timestamp values. This also produces a different Signature value.

Typically, you only need to configure the client to resend a request in the case of Error 503 (ServiceUnAvailable) or no response. If Error 200 is returned, a retry can obtain the same result as that of the previous request, but the server status is not affected. If Error 4xx or 500 is returned, the request cannot be retried unless the error message states Try it later.

2.3.2. SDK reference

2.3.2.1. Java SDK

2.3.2.1.1. Quick start

This topic describes how to obtain and use the *ESS* Java SDK.

Preparation

- You must have an Apsara Stack tenant account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use Java SDK. For more information about how to obtain and view your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- For more information about how to obtain the service endpoint, see Obtain an endpoint.
- The Java SDK supports JDK V1.6 and later.

Installation

If you use Apache Maven to manage Java projects, you only need to import the JAR file to the *pom.xml* file of the project.

To use the SDK of a service, you must install the service SDK and the SDK core library.

The version of the core library is 4.1.0. The version of the *ESS* SDK is *2.1.1*.

```
<dependencies>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-sdk-core</artifactId>
      <version>4.1.0</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-core-4.1.0.jar</systemPath>
    </dependency>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-ess</artifactId>
      <version>2.1.1</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-ess-2.1.1.jar</systemPath>
    </dependency>
  </dependencies>
```

Usage

The following sample code shows how to use the Java SDK:

1. Create a DefaultAcsClient client and initialize it.
2. Create an API request and set request parameters.
3. Initiate the request and handle the response or exceptions.

```
package com.testprogram;
 import com.aliyuncs.profile.DefaultProfile;
 import com.aliyuncs.DefaultAcsClient;
 import com.aliyuncs.IAcsClient;
 import com.aliyuncs.exceptions.ClientException;
 import com.aliyuncs.exceptions.ServerException;
 import com.aliyuncs.ess.model.v20140828.*;
 public class Main {
    public static void main(String[] args) {
       // Create a DefaultAcsClient client and initialize it.
       DefaultProfile profile = DefaultProfile.getProfile(
          "<your-region-id>", // The region ID
          "<your-access-key-id>", // The AccessKey ID
          "<your-access-key-secret>"); // The AccessKey Secret
       // Set the endpoint of the service.
      profile.addEndpoint("your-region-id", "your-region-id", "product", "endpoint");
       IAcsClient client = new DefaultAcsClient(profile);
       // Create an API request and set request parameters.
       DescribeScalingGroupsRequest request = new DescribeScalingGroupsRequest();
       request.setPageSize(10);
       // Initiate the request and handle the response or exceptions.
       DescribeScalingGroupsResponse response;
       try {
          response = client.getAcsResponse(request);
          System.out.println(new Gson().toJson(response));
       } catch (ServerException e) {
          e.printStackTrace();
       } catch (ClientException e) {
          e.printStackTrace();
       }
    }
 }
```

2.3.2.1.2. Use the Java SDK

2.3.2.2. Python SDK

2.3.2.2.1. Quick start

This topic describes how to obtain and use the *ESS* Python SDK.

Preparation

- You must have an Apsara Stack account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use Python SDK. For more information about how to obtain and view your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- For more information about how to obtain an endpoint, see Obtain an endpoint.

Install the Python SDK

To install the Python SDK, follow these steps:

1. Install the SDK core library.
   - If you are using Python V2.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core
     ```

   - If you are using Python V3.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core-v3
     ```

2. Install the SDK.

   The following code shows how to install the ESS SDK:

   ```
   pip install aliyun-python-sdk-ess
   ```

Usage

The following example shows how to use the Python SDK:

1. Create a client. When you create the client, you must set the region ID, AccessKey ID, and AccessKey Secret.
2. Create an API request and set request parameters.
3. Initiate the request and process the response or exceptions.

```
#! /usr/bin/env python
#coding=utf-8

from aliyunsdkcore import client
from aliyunsdkcore.profile import region_provider
from aliyunsdkecs.request.v20140828 import DescribeScalingGroupsRequest

# global config
region_id = 'xxxxx'
secret_id = 'xxxxx'
secret_key = 'xxxxx'

# product config
product_name = 'ess'
endpoint = 'ess.example.com'

# create client
region_provider.modify_point(product_name, region_id, endpoint)
clt = client.AcsClient(secret_id, secret_key, region_id)

# setup request
request = DescribeScalingGroupsRequest()
request.set_accept_format('json')

# get response
response = clt.do_action_with_exception(request)

print response
```

2.3.2.2.2. Use the Python SDK

2.3.2.3. PHP SDK

2.3.2.3.1. Quick start

The PHP SDK allows you to access *ESS* without complex coding. This topic describes how to install and use the PHP SDK.

Preparation

- You must have an Apsara Stack tenant account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the PHP SDK. For more information about how to obtain and view your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.

- For more information about how to obtain the service endpoint, see Obtain an endpoint.
- The PHP SDK supports PHP V5.3, V5.4, V5.5, V5.6, V7.0, and V7.1. You can run the **php -v** command to obtain the current PHP version.

Installation

To install the PHP SDK, follow these steps:

1. Download the PHP SDK source code package from SDK template.
2. Add the PHP SDK reference to your code.

   In the following example, the PHP SDK is downloaded to `/path/to/aliyun-openapi-php-sdk`.

   ```
   require_once '/path/to/aliyun-openapi-php-sdk/aliyun-php-sdk-core/Config.php';
   ```

Usage

The following sample code shows how to use the PHP SDK:

1. Create a DefaultAcsClient client and initialize the client.

   When you create and initialize the DefaultAcsClient client, you must set the Region ID, AccessKey ID, and AccessKey Secret parameters.
2. Create an API request and set request parameters.
3. Initiate the request and handle the response or exceptions.

```
<? php
use Ess\Request\V20140828\DescribeScalingGroupsRequest;
// Create a DefaultAct.sClient client and initialize the client
$clientProfile = DefaultProfile::getProfile(
   "<your-region-id>", # The region ID
   "<your-access-key-id>", # The AccessKey ID
   "<your-access-key-secret>" #The AccessKey Secret
);
$client = new DefaultAcsClient($clientProfile);
# Specify the endpoint of the service.
$profile->endpoint ="your-region-id", "your-region-id", "product", "endpoint";
# Create an API request and set request parameters.
$request = new DescribeScalingGroupsRequest();
$request->setPageSize(10);
# Initiate the request and handle the response.
try {
   $response = $client->getAcsResponse($request);
   print_r($response);
} catch(ServerException $e) {
   print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
} catch(ClientException $e) {
   print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
}
? >
```

2.3.2.4. Go SDK

2.3.2.4.1. Quick start

The Go SDK allows you to access *ESS* without complex coding. This topic describes how to install and use the Go SDK.

Preparation

- You must have an Alibaba Cloud account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the Go SDK. For more information about how to obtain and view your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- For more information about how to obtain the service endpoint, see Obtain an endpoint.

Install the Go SDK

1. Download the Go SDK source code package from SDK template.
2. Decompress the package to the directory specified by *GO_PATH*.

Usage

The following code shows how to use the Go SDK:

1. Create a client.
2. Create an API request and configure request parameters.
3. Initiate the request and handle the response or exceptions.

```
package main

import (
    "github.com/aliyun/alibaba-cloud-sdk-go/services/ess"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "fmt"
)

func main() {
    // Create an essClient client.
    essClient, err := ess.NewClientWithAccessKey(
        "<your-region-id>", // The region ID
        "<your-access-key-id>", // The AccessKey ID
        "<your-access-key-secret>") // The AccessKey Secret
    if err ! = nil {
        // Handle exceptions.
        panic(err)
    }
   // Specify the endpoint of the service.
    request.Domain = "endpoint"
    // Create an API request and set request parameters.
    request := ess.CreateDescribeScalingGroupsRequest()
    // Set request.PageSize to 10.
    request.PageSize = requests.NewInteger(10)
    // Initiate the request and handle exceptions.
    response, err := essClient.DescribeScalingGroups(request)
    if err ! = nil {
        // Handle exceptions.
        panic(err)
    }
    fmt.Println(response)
}
```

4. Optional. Switch to HTTP or HTTPS.

```
request.Scheme = "HTTPS"
```

2.3.2.4.2. Use the Go SDK

2.3.2.5. .NET SDK

2.3.2.5.1. Quick start

.NET SDK allows you to access *ESS* without complex coding. This topic describes how to obtain and use the .NET Go SDK.

Preparation

- You must have an Apsara Stack tenant account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the .NET SDK. For more information about how to obtain and view your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- For more information about how to obtain the service endpoint, see Obtain an endpoint.
- The .Net SDK supports .NET Framework 4.0 and later.

Installation

To use the SDK of a service, you must install both the SDK and SDK core library. For example, to use the *ESS* SDK, you must obtain and install both the *ESS* SDK and its core library. Use the following methods to install the .NET SDK:

- Add the DLL reference
  i. Download the compressed package containing a DLL file from the.NET SDK list, and decompress it to obtain the DLL file.
  ii. Right-click your project in Solution Explorer of Visual Studio and choose **Reference** from the shortcut menu.
  iii. In the shortcut menu, select **Add Reference**.
  iv. In the dialog box that appears, click **Browse**, select the target DLL file, and click **Confirm**.
- Add the project reference
  i. Download the .NET SDK source code package from SDK template.
  ii. In the downloaded folder, find the *aliyun-net-openapi-XXX* subfolder, and then find the **.csproj* file, which is the .NET project file. In this example, the `aliyun-net-sdk-ess.csproj` file is in the `aliyun-net-openapi-ess` subfolder.
  iii. In Visual Studio, right-click your solution.
  iv. Choose **Add** > **Existing Project**.
  v. In the dialog box that appears, select the target .NET project file, for example, `aliyun-net-sdk-ess.csproj`, and click **Open**.
  vi. Right-click your project and choose **Reference** > **Add Reference**.

Usage

The following sample code shows how to use the .NET SDK:

1. Create a DefaultAcsClient client and initialize the client.
2. Create an API request and configure request parameters.

3. Initiate the request and handle the response or exceptions.

```
using Aliyun.Acs.Core;
using Aliyun.Acs.Core.Profile;
using Aliyun.Acs.Core.Exceptions;
using Aliyun.Acs.Ess.Model.V20140828;
class TestProgram
{
  static void Main(string[] args)
  {
    // Create a client for making requests.
    IClientProfile profile = DefaultProfile.GetProfile(
      "<your-region-id>",
      "<your-access-key-id>",
      "<your-access-key-secret>");
   // Specify the endpoint of the service.
   profile.setEndpoint("your-region-id", "your-region-id", "product", "endpoint");
   DefaultAcsClient client = new DefaultAcsClient(profile);
    try
    {
      // Create a request.
      DescribeScalingGroupsRequest request = new DescribeScalingGroupsRequest();
      request.PageSize = 10;
      // Initiate the request and receive the response.
      DescribeScalingGroupsResponse response = client.GetAcsResponse(request);
      System.Console.WriteLine(response.TotalCount);
    }
    catch (ServerException ex)
    {
      System.Console.WriteLine(ex.ToString());
    }
    catch (ClientException ex)
    {
      System.Console.WriteLine(ex.ToString());
    }
  }
}
```

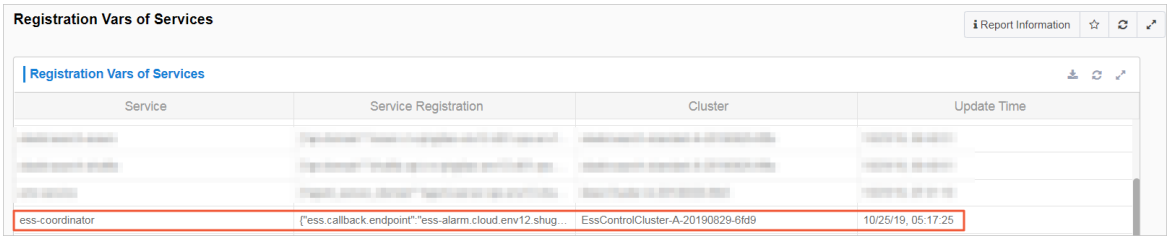
2.3.2.5.2. Use the .NET SDK

2.3.3. Obtain an endpoint

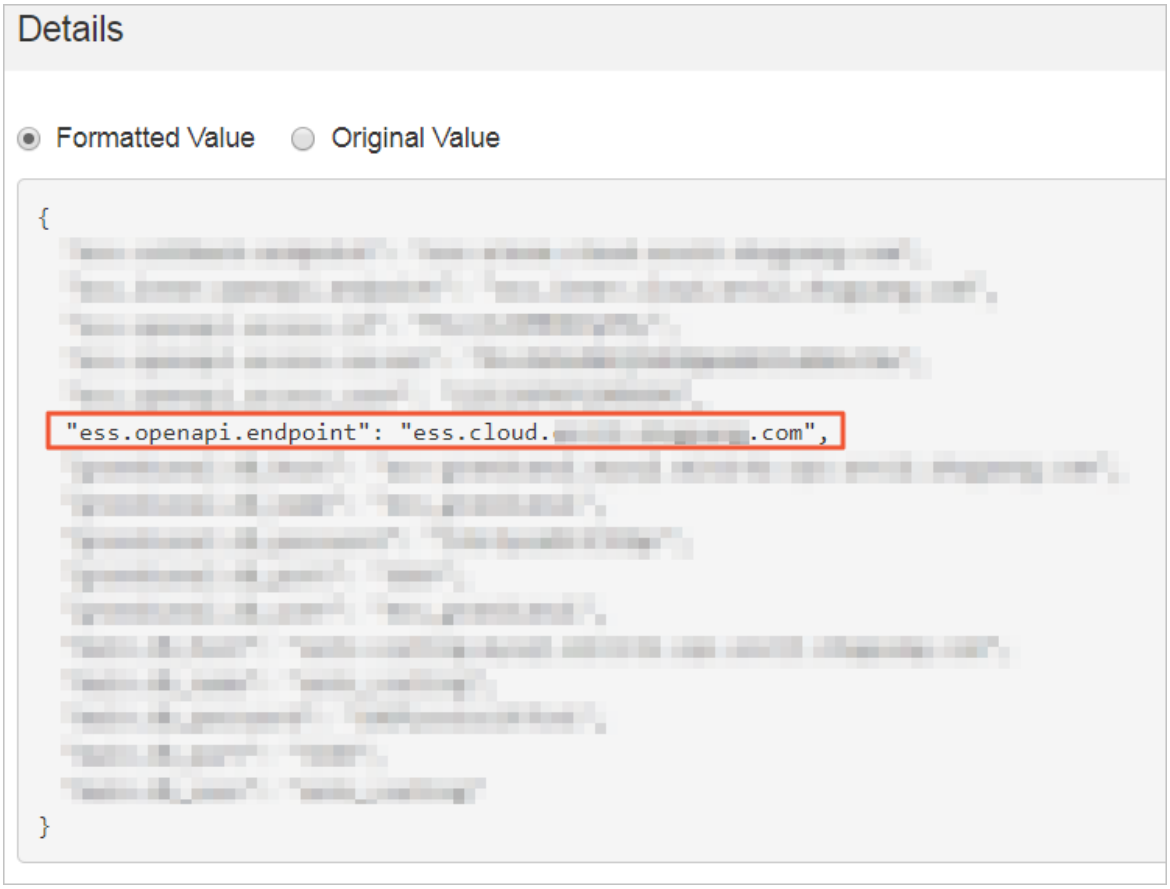
You can obtain the product endpoint in Apsara Stack Operations.

Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms > Apsara Stack Operations > Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. In the top navigation bar, choose **Reports > System Reports**.
5. On the **System Reports** page, click **Registration Vars of Services**.
6. On the **Registration Vars of Services** page, find the ess row, right-click the **Service Registration** column, and select **Show More**.



7. In the **Details** dialog box that appears, find the *ESS* endpoint based on the key value of *ESS*, which is *ess.openapi.endpoint*.



2.3.4. Obtain an AccessKey pair

You can obtain the AccessKey pair on the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**. The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.4. Object Storage Service (OSS)

2.4.1. API reference

2.4.1.1. OSS API reference overview

OSS provided by Apsara Stack is a secure, cost-friendly, and highly reliable cloud storage service that processes large amounts of data. You can upload data to and download data from OSS anytime, anywhere, and on any Internet device through the simple RESTful APIs described herein. OSS enables you to develop a variety of services that are capable of processing large amounts of data. These services include multimedia sharing websites, online storage, and personal and corporate data backups.

> **Note** Before using these APIs, make sure that you fully understand the OSS product instructions, use agreements, and billing methods.

2.4.1.2. API overview

Service operations

API parameters for service operations

API	Description
GetService	Obtains all the buckets of a specified account.

Bucket operations

API parameters for bucket operations

API	Description
PutBucket	Creates a bucket.
PutBucketACL	Sets the ACL for a bucket.
PutBucketLogging	Enables bucket access logging.
PutBucketWebsite	Enables static website hosting for a bucket.
PutBucketReferer	Sets hotlinking rules for a bucket.
PutBucketLifecycle	Sets lifecycle rules for objects in a bucket.
PutBucketTagging	Adds a group of tags to a bucket.
GetBucketAcl	Obtains the access permission of a bucket.
GetBucketLocation	Obtains the location information of the region to which a specified bucket belongs.
GetBucketLogging	Views the access log configuration of a bucket.
GetBucketWebsite	Views the static website hosting status of a bucket.
GetBucketReferer	Views hotlinking rules of a bucket.
GetBucketLifecycle	Views lifecycle rules of objects in a bucket.
GetBucketTagging	Obtains all tags associated with a bucket.
DeleteBucket	Deletes a bucket.
DeleteBucketLogging	Disables access logging for a bucket.
DeleteBucketWebsite	Disables static website hosting for a bucket.
DeleteBucketLifecycle	Deletes lifecycle rules of objects in a bucket.
DeleteBucketTagging	Deletes all tags associated with a bucket.
GetBucket(List Object)	Obtains information about all the objects in a bucket.
GetBucketInfo	Obtains bucket information.

API	Description
ListBucketByTagging	Lists matching buckets based on the specified tag key and tag value.

Object operations

API parameters for object operations

API	Description
PutObject	Uploads an object.
CopyObject	Copies an object to make it another object.
GetObject	Obtains an object.
AppendObject	Uploads an object by appending the object to an existing object.
DeleteObject	Deletes a single object.
DeleteMultipleObjects	Deletes multiple objects simultaneously.
HeadObject	Obtains Object Meta.
GetObjectMeta	Obtains basic Object Meta of an object in a bucket.
PostObject	Uploads an object in Post mode.
PutObjectACL	Sets the ACL for an object.
GetObjectACL	Obtains the ACL information of an object.
PutSymlink	Creates a symbolic link.
GetSymlink	Obtains a symbolic link.

Multipart upload operations

API parameters for multipart upload operations

API	Description
InitiateMultipartUploade	Initializes a MultipartUpload task.
UploadPart	Uploads an object in multiple parts.
UploadPartCopy	Copies and uploads an object in multiple parts.
CompleteMultipartUpload	Completes multipart upload of the entire object.
AbortMultipartUpload	Aborts a MultipartUpload task.
ListMultipartUploads	Lists all the ongoing MultipartUpload tasks.

API	Description
ListParts	Lists all the successfully uploaded parts mapped to a specific upload ID.

Cross-origin resource sharing (CORS)

API parameters for CORS

API	Description
PutBucketCORS	Sets CORS rules for a specified bucket.
GetBucketCORS	Obtains the CORS rules of a specified bucket.
DeleteBucketCORS	Disables the CORS function for a specified bucket and clears all the rules.
OptionObject	Preflights the request for cross-origin access.

2.4.1.3. Access control

2.4.1.3.1. Verify user signature

OSS uses an AccessKey pair (including an AccessKey ID and an AccessKey secret) to implement symmetric encryption and verify the identity of a requester. The AccessKey ID is used to identify the user. The AccessKey secret is used by the user to encrypt the signature string and used by OSS to verify the signature string. You must keep your AccessKey secret confidential. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

Based on the account types, AccessKey pairs can be categorized as follows:

- AccessKey pair of an Apsara Stack account: The AccessKey pair of an Apsara Stack account has full permissions on its resources.
- AccessKey pair of a RAM user: A RAM user is created and authorized by an Apsara Stack account. The AccessKey pair of a RAM user has limited permissions on specified resources.
- STS temporary access credential: A temporary access credential is generated by an Apsara Stack account or a RAM user. The AccessKey pair of a temporary credential has limited permissions on specified resources within the validity period of the credential. The permissions of the AccessKey pair are revoked after the temporary access credential expires.

Before you can use your identity to send a request to OSS, you must first generate a signature string for the request in the format specified by OSS. Then, you must use your AccessKey secret to generate a verification code and encrypt the signature string. After receiving the request, OSS finds the AccessKey secret based on your AccessKey ID, and uses the AccessKey secret to decrypt the signature string and verification code. Then, OSS calculates a verification code and compares it against the decrypted verification code. If the two verification codes are the same, OSS determines that the request is valid. Otherwise, OSS rejects the request and returns HTTP 403.

2.4.1.3.2. Add signatures to headers

You can include the Authorization header in the HTTP request to carry signature information and indicate that the requester has been authorized.

Calculation of the Authorization header

```
Authorization = "OSS " + AccessKeyId + ":" + Signature
Signature = base64(hmac-sha1(AccessKeySecret,
 VERB + "\n"
 + Content-MD5 + "\n"
 + Content-Type + "\n"
 + Date + "\n"
 + CanonicalizedOSSHeaders
 + CanonicalizedResource))
```

- `AccessKeySecret` specifies the key required for a signature.
- `VERB` specifies the HTTP request method, including PUT, GET, POST, HEAD, and DELETE.
- `\n` specifies a new line.
- `Content-MD5` specifies the MD5 hash of request content data. The message content excluding the header is obtained by calculating the MD5 hash to obtain a 128-bit number and then encoding the number in Base64. The request header can be used to check the message validity of whether the message content is consistent with the sent content. Example: eB5eJF1ptWaXm4bijSPyxw==. The request header can be empty. For more information, visit RFC2616 Content-MD5.
- `Content-Type` specifies the requested content type. Example: application/octet-stream. The content type can be empty.
- `Date` specifies the operation time. It must be in GMT. Example: Sun, 22 Nov 2015 08:16:38 GMT.
- `CanonicalizedOSSHeaders` specifies HTTP headers in alphabetical order. The prefix of the HTTP headers is **x-oss-**.
- `CanonicalizedResource` specifies the OSS resource you want to access.

Specifically, the values of Date and CanonicalizedResource cannot be empty. If the difference between the time on the client when the request is sent and the time on the server when the request is received is greater than 15 minutes, the OSS server denies the request and returns HTTP 403.

Construct CanonicalizedOSSHeaders

All HTTP headers whose prefixes are x-oss- are called CanonicalizedOSSHeaders. You can construct CanonicalizedOSSHeaders as follows:

1. The names of all HTTP request headers whose prefixes are x-oss- must be in lowercase letters. For example, `X-OSS-Meta-Name: TaoBao` is converted to `x-oss-meta-name: TaoBao`.
2. If the request is sent by using the AccessKey ID and AccessKey secret obtained by STS, you must add the obtained security-token value to the signature string in `x-oss-security-token:security-token` format.
3. Sort all obtained HTTP request headers in alphabetically ascending order.
4. Delete any space on either side of a delimiter between the request header and content. For example, `x-oss-meta-name: TaoBao` is converted to `x-oss-meta-name:TaoBao`.

5. Separate all content and headers with the (`\n`) delimiter to form the final CanonicalizedOSSHeaders.

> Note
>
> - CanonicalizedOSSHeaders can be empty. The (`\n`) delimiter at the end can be removed.
> - To construct only one canonicalized OSS header, add the (`\n`) delimiter to the end of the header. Example: `x-oss-meta-a\n` .
> - To construct multiple canonicalized OSS headers, add the (`\n`) delimiter to the end of each header. Example: `x-oss-meta-a:a\nx-oss-meta-b:b\nx-oss-meta-c:c\n` .

Construct CanonicalizedResource

The destination OSS resource specified in the request sent by the user is called CanonicalizedResource. You can construct CanonicalizedOSSHeaders as follows:

1. Set CanonicalizedResource to empty character string ("").
2. Specify the OSS resource you want to access in the following format: `/BucketName/ObjectName` . Set CanonicalizedResource to `/BucketName/` to access a bucket or to a forward slash (`/`) delimiter to access OSS.
3. If the requested resource contains subresources, sort all subresources in alphabetically ascending order and separate them with the ampersand (`&`) delimiter. The question mark (`?`) and subresource string are added to the end of the CanonicalizedResource string. In this case, CanonicalizedResource is in format of `/BucketName/ObjectName? acl&uploadId=UploadId.`
4. If query strings (also called HTTP request parameters) are specified in the request, sort these query strings and request values in alphabetically ascending order. Separate them with the ampersand (`&`) delimiter. Add them to CanonicalizedResource as parameters. In this case, CanonicalizedResource is in format of `/BucketName/ObjectName? acl&response-content-type=ContentType&uploadId=UploadId` .

> Note
>
> - OSS supports the following subresources: acl, uploads, location, cors, logging, website, referer, lifecycle, delete, append, tagging, objectMeta, uploadId, partNumber, security-token, position, img, style, styleName, replication, replicationProgress, replicationLocation, cname, bucketInfo, comp, qos, live, status, vod, startTime, endTime, symlink, x-oss-process, response-content-type, response-content-language, response-expires, response-cache-control, response-content-disposition, and response-content-encoding.
> - Three types of subresources are available:
>   - Resource identifiers such as acl, append, uploadId, and symlink subresources
>   - Subresources that specify the response header fields. Example: `response-***`
>   - Methods to process objects. Example: `x-oss-process`

Rules to calculate a signature header

1. A signature string must be in UTF-8 format. A signature string that contains Chinese characters must be encoded in UTF-8. The encoded signature string is used together with AccessKeySecret to calculate the final signature.
2. The HMAC-SHA1 method defined in RFC 2104 is used to calculate the final signature. In this method, the Key is `AccessKeySecret`.
3. Content-Type and Content-MD5 are not required in a request. If the request requires signature verification, the null value must be replaced with a new line (`\n`).
4. Among all non-standard HTTP headers, only headers starting with `x-oss-` require signature strings. Other non-standard HTTP headers are ignored by OSS. For example, The x-oss-magic header in the preceding example requires a signature string.
5. Headers starting with `x-oss-` must comply with the following conventions before signature verification:
   - The header name must be in lowercase.
   - The headers are sorted in alphabetically ascending order.
   - No spaces exist before or after the colon (:), which separates the header name and value.
   - Each header is followed by a new line (`\n`). If no headers are used, `CanonicalizedOSSHeaders` is set to null.

Examples

If the AccessKey ID is `4***7`, the AccessKey secret is `O***V`.

Signature examples

Request	Signature string calculation formula	Signature string
`PUT /nelson HTTP/1.0 Content-MD5: eB5eJF1ptWaXm4bijSPyxw== Content-Type: text/html Date: Thu, 17 Nov 2005 18:49:58 GMT Host: oss-example.regionid.example.com X-OSS-Meta-Author: ***@bar.com X-OSS-Magic: a***a`	`Signature = base64(hmac-sha1(AccessKeySecret,VERB + "\n" + Content-MD5 + "\n"+ Content-Type + "\n" + Date + "\n" + CanonicalizedOSSHeaders+ CanonicalizedResource))`	`"PUT\n ***w==\n text/html\n Thu, 17 Nov 2005 18:49:58 GMT\n x-oss-magic:a***a\nx-oss-meta-author:***@bar.com\n/oss-example/nelson"`

An example of the signature calculation method is as follows:

```
import base64
import hmac
import sha
h = hmac.new("O***V",
 "PUT\n***M=\ntext/html\nThu, 17 Nov 2005 18:49:58 GMT\nx-oss-magic:abracadabra\nx-oss-meta-auth
or:***@bar.com\n/oss-example/nelson", sha)
Signature = base64.b64encode(h.digest())
print("Signature: %s" % Signature)
```

The signature calculation result must be 2***A= based on Authorization = "OSS" + AccessKeyId + ":" + Signature. Authorization that consists of OSS 4***7:2***A= and the Authorization header is sent:

```
PUT /nelson HTTP/1.0
Authorization:OSS 4***7:2***A=
Content-Md5: e***w==
Content-Type: text/html
Date: Thu, 17 Nov 2005 18:49:58 GMT
Host: oss-example.regionid.example.com
X-OSS-Meta-Author: ***@bar.com
X-OSS-Magic: a***a
```

Detail analysis

1. If the imported AccessKey ID does not exist or is inactive, 403 Forbidden is returned. Error code: InvalidAccessKeyId.
2. If the Authorization value format in the request header is incorrect, 400 Bad Request is returned. Error code: InvalidArgument.
3. All OSS requests must use GMT provided in HTTP 1.1. The date format is `date1 = 2DIGIT SP mont h SP 4DIGIT; day month year (e.g., 02 Jun 1982)` . In this format, day is in 2-digit form. Therefore, Jun 2, 2 Jun 1982, and 2-Jun-1982 are all invalid formats.
4. If no date is entered or the date is in invalid format during signature verification, 403 Forbidden is returned. Error code: AccessDenied.
5. The difference between the time on the client when the request is sent and the time on the server when the request is received must be within 15 minutes. Otherwise, 403 Forbidden is returned. Error code: RequestTimeTooSkewed.
6. If the AccessKey ID is active but OSS determines that the signature of the request is invalid, 403 Forbidden is returned. The correct signature string for verification and encryption is returned to the user in the response. You can check whether the signature string is valid based on the response of OSS. Sample responses:

```
<? xml version="1.0" ? >
<Error>
 <Code>
 SignatureDoesNotMatch
 </Code>
 <Message>
 The request signature we calculated does not match the signature you provided. Check your key and si
gning method.
 </Message>
 <StringToSignBytes>
 47 45 54 0a 0a 0a 57 65 64 2c 20 31 31 20 4d 61 79 20 32 30 31 31 20 30 37 3a 35 39 3a 32 35 20 47 4d 54 0a 2f
75 73 72 65 61 6c 74 65 73 74 3f 61 63 6c
 </StringToSignBytes>
 <RequestId>
 1***2
 </RequestId>
 <HostId>
 regionid.example.com
 </HostId>
 <SignatureProvided>
 y***8=
 </SignatureProvided>
 <StringToSign>
 GET
Wed, 11 May 2011 07:59:25 GMT
/oss-example? acl
 </StringToSign>
 <OSSAccessKeyId>
 A***Q
 </OSSAccessKeyId>
</Error>
```

OSS SDKs automatically implements signatures in your requests. You do not need to manually calculate your signature when you use OSS SDKs. For more information about the signature implementation for specific programming languages, see the OSS SDK code. The following table describes the sample code used to implement signatures in various SDKs.

Sample code used to implement signatures in various SDKs

SDK	Signature implementation
Java SDK	OSSRequestSigner.java

SDK	Signature implementation
Python SDK	auth.py
.Net SDK	OssRequestSigner.cs
PHP SDK	OssClient.php
C SDK	oss_auth.c
JavaScript SDK	client.js
Go SDK	auth.go
Ruby SDK	util.rb
iOS SDK	OSSModel.m
Android SDK	OSSUtils.java

Calculate the Content-MD5 hash

Take message content "123456789" as an example. The following section provides a detailed description about the correct and incorrect methods to calculate the Content-MD5 hash of the string.

The algorithm defined in related standards can be simplified as follows:

1. Calculate the MD5-encrypted 128-bit binary array.

2. Encode the binary array (instead of the 32-bit string code) in Base64.

Python is used as an example.

The following code provides an example on how to calculate the Content-MD5 hash in Python:

```
>>> import base64,hashlib
>>> hash = hashlib.md5()
>>> hash.update("0123456789")
>>> base64.b64encode(hash.digest())
'eB5eJF1ptWaXm4bijSPyxw=='
```

Note:

Call the hash.digest() function to obtain a 128-bit binary array.

```
>>> hash.digest()
'x\x1e^$]i\xb5f\x97\x9b\x86\xe2\x8d#\xf2\xc7'
```

A common incorrect method is to directly encode the 32-bit string in Base64.

Example: Call the hash.hexdigest() function to obtain a visible 32-bit string.

```
>>> hash.hexdigest()
'781e5e245d69b566979b86e28d23f2c7'
```

Result of encoding the MD5 hash in Base64:

```
>>> base64.b64encode(hash.hexdigest())
'NzgxZTVlMjQ1ZDY5YjU2Njk3OWI4NmUyOGQyM2YyYzc='
```

2.4.1.3.3. Generate a signed URL

In addition to using an Authorization field in the header, you can also add signature information to a URL so that you can forward the URL to a third party for authorized access.

Implementation

- The following code provides an example of how to generate a signed URL:

  ```
  http://oss-example.regionid.example.com/oss-api.pdf?
  AccessKeyId=AccessKeyId&Expires=1141889120&Signature=vjb***%3D
  ```

- A signature must include at least the following three parameters: Signature, Expires, and AccessKeyId.
  - `Expires` indicates the timeout time of the URL. The value of this parameter is in the UNIX time format. The value is the number of seconds that elapsed since January 1, 1970 UTC. If the time OSS receives the URL request is later than the value of Expires that is included in the signature, an error code request timeout is returned. For example, the current time is 1141889060. To create a URL that is scheduled to expire in 60 seconds, you can set the value of Expires to 1141889120.
  - `AccessKeyId` indicates the AccessKey ID in the AccessKey pair.

- `Signature` indicates the signature information. For all requests and header fields that OSS supports, the algorithm of signing the string for a URL is basically the same as that of signing the string for a header.

  ```
  Signature = urlencode(base64(hmac-sha1(AccessKeySecret,
  VERB + "\n"
  + CONTENT-MD5 + "\n"
  + CONTENT-TYPE + "\n"
  + EXPIRES + "\n"
  + CanonicalizedOSSHeaders
  + CanonicalizedResource)))
  ```

  The difference is listed as follows:

  - When a signed URL is generated, the Expires parameter replaces the Date parameter.
  - Signatures cannot be included in a URL and the header field at the same time.
  - If more than one Signature, Expires, or AccessKeyId value is imported, the first input value is used.
  - Before verifying the signature of a request, OSS checks the request time to determine whether it is later than the time specified in Expires.
  - When you add a signature string to a URL, you need to encode the URL.

- When you add a signature to a temporary user URL, you need to include `security-token`. The format is as follows:

  ```
  http://oss-example.regionid.example.com/oss-api.pdf?
  AccessKeyId=AccessKeyId&Expires=1141889120&Signature=vjb***%3D&security-token=SecurityToke
  n
  ```

Examples

The following code provides an example of how to add a signature to a URL in Python:

```
import base64
import hmac
import sha
import urllib
h = hmac.new("O***V",
 "GET\n\n\n1141889120\n/oss-example/oss-api.pdf",
 sha)
urllib.quote (base64.encodestring(h.digest()).strip())
```

Note

- OSS SDKs provide methods for generating a signed URL. For more information, see "Authorized access" in SDK documents.
- For more information about how to generate a URL for OSS SDKs, see the following table.

URL signature implementation files for OSS SDKs

SDK	URL signature method	Implementation file
Java SDK	OSSClient.generatePresignedUrl	OSSClient.java
Python SDK	Bucket.sign_url	api.py
.Net SDK	OssClient.GeneratePresignedUri	OssClient.cs
PHP SDK	OssClient.signUrl	OssClient.php
JavaScript SDK	signatureUrl	object.js
C SDK	oss_gen_signed_url	oss_object.c

Detail analysis

- If you adopt the approach of generating a signed URL, the authorized data is exposed on the Internet before the authorization period expires. We recommend that you assess the use risks in advance.
- You can add a signature to a URL in PUT and GET requests.
- When a signature is added to a URL, the sequence of the Signature, Expires, and AccessKeyId parameters can be swapped. If one or more of the Signature, Expires, and AccessKeyId parameters are missing, error message 403 Forbidden is returned. Error code: AccessDenied.
- If the current access time is later than the Expires value set in the request or the time format is incorrect, error message 403 Forbidden is returned. Error code: AccessDenied.
- If a URL includes one or more of the Signature, Expires, and AccessKeyId parameters and the header includes signature information, error message 400 Bad Request is returned. Error code: InvalidArgument.
- When the signature string is generated, Date is replaced by Expires, but the headers such as content-type and content-md5 defined in the preceding section are still included. (Although Date still exists in the request header, you do not need to add it to the signature string.)

2.4.1.3.4. Authorized temporary access

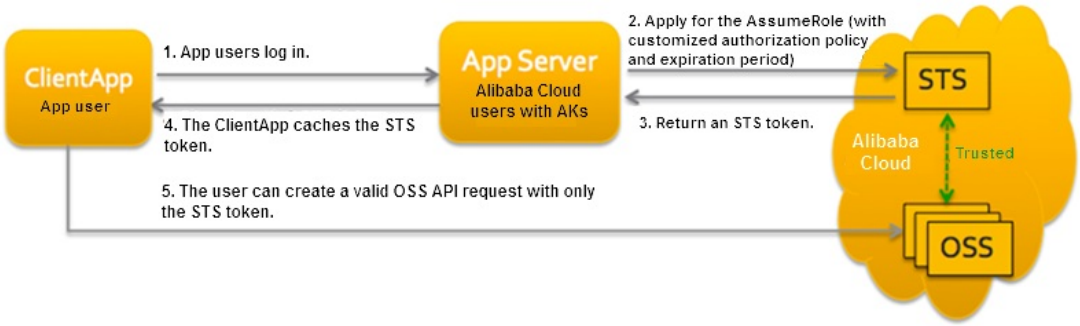
Introduction to STS

OSS allows you to use Alibaba Cloud STS for temporary access authorization. Alibaba Cloud STS is a Web service that provides a temporary access token for cloud computing users. Through STS, you can grant a third-party application or federated user (whose user ID is managed by yourself) an access credential with a custom validity period and permissions. The third-party application or federated user can use the access credential to directly call the Alibaba Cloud product APIs or use the Alibaba Cloud product SDKs to access the cloud product APIs.

- You do not need to expose your long-term key (AccessKey) to a third-party application. You need only to generate an access token and send the access token to the third-party application. You can customize the access permissions and validity period of this token.
- The access token automatically becomes invalid upon expiration.

An application is used as an example. The following figure shows the interaction process.

Interaction process



The solution is described in detail as follows:

1. Log on as an application user. You can manage your application user ID. You can customize the ID management system or use an external Web account or OpenID. For each valid application user, you can use the AppServer to precisely define the principle of least privilege (POLP).
2. The AppServer requests a security token from STS. Before calling STS, the AppServer needs to determine the POLP (described in policy syntax) of the application user and the expiration time of the authorization. Then, the AppServer calls the AssumeRole API of STS to obtain the security token.
3. STS returns a valid access credential to the AppServer. The access credential includes a security token, a temporary AccessKey (AccessKey ID and AccessKey Secret), and the expiration time.
4. The AppServer returns the access credential to the ClientApp. The ClientApp caches this credential. When the credential becomes invalid, the ClientApp must request a new valid access credential from the AppServer. For example, if the access credential is valid for one hour, the ClientApp can request the AppServer to update the access credential every 30 minutes.
5. The ClientApp uses the locally cached access credential to request Apsara Stack service APIs. Cloud services detect the STS access credential, verify the credential based on the STS service, and correctly respond to user requests.

The key is to call the AssumeRole API of STS to obtain a valid access credential. You can also directly use the STS SDK to call this API.

Use an STS credential to create a request with a signature

After obtaining an STS temporary credential, the client of the user uses the security token and temporary AccessKey (AccessKey ID and AccessKey Secret) in the credential to create a signature. The method for creating an authorized access signature is basically the same as using the AccessKey of a root account directly to add a signature to a header. Note that:

- The signature key used by the user is the temporary AccessKey (AccessKey ID and AccessKey Secret) that STS provides.
- The user needs to add the security token to the request header or in the URI as a request

parameter. Only either of these two methods can be used. If both methods are selected, OSS returns an InvalidArgument error.

- `x-oss-security-token:SecurityToken` is included in the request header. When CanonicalizedOSSHeaders of the signature is calculated, x-oss-security-token is taken into consideration.
- security-token=SecurityToken is included in the URL. When CanonicalizedResource of the signature is calculated, security-token is considered as a sub-resource.

2.4.1.3.5. Bucket permission control

OSS provides an Access Control List (ACL) for the bucket-level access control. Currently, three access permissions are available for a bucket: public-read-write, public-read, and private. They are described as follows:

- public-read-write: Anyone (including anonymous users) can perform Put Object, Get Object, and Delete Object operations on the objects in the bucket. The fees incurred by these operations are borne by the creator of the buckets. Therefore, exercise caution when using this permission.
- public-read: Only the creator of the bucket can perform write operations (including Put Object and Delete Object) on the objects in the bucket. Anyone (including anonymous users) can perform read operations (Get Object) on the objects in the bucket.
- private: Only the creator of the bucket can perform read and write operations (including Put Object, Delete Object, and Get Object) on the objects in the bucket. Others cannot access the objects in the bucket.

When you create a bucket without specifying its ACL, OSS automatically sets a private ACL for the bucket. For a bucket that already exists, only its creator can modify its ACL through the PutBucketACL API of OSS.

2.4.1.4. Definitions of common HTTP headers

Common request headers

Some common request headers are used for OSS RESTful APIs. These request headers can be used by all the OSS requests. The following table lists the specific definitions of the request headers.

Common request header parameters

Name	Description
Authorization	The verification information used to verify the validity of a request. Type: string. Default value: none. Scenario: non-anonymous requests.
Content-Length	The content length of an HTTP request that is defined in RFC2616. Type: string. Default value: none. Scenario: requests that need to submit data to OSS.

Name	Description
Content-Type	The content type of an HTTP request that is defined in RFC2616. Type: string. Default value: none. Scenario: requests that need to submit data to OSS.
Date	The GMT stipulated in the HTTP 1.1 protocol, for example, Wed, 05 Sep. 2012 23:00:00 GMT. Type: string. Default value: none.
Host	The value that is used to access the host. The format is `<bucketname>.regionid.example.com`. Type: string. Default value: none.

Common response headers

Some common request headers are used for OSS RESTful APIs. These request headers can be used by all the OSS requests. The following table lists the specific definitions of the request headers.

Common response header parameters

Name	Description
Content-Length	The content length of an HTTP request that is defined in RFC2616. Type: string. Default value: none. Scenario: requests that need to submit data to OSS.
Connection	The connection status between the client and the OSS server. Type: enumeration. Valid values: open and close Default value: none.
Date	The GMT stipulated in the HTTP 1.1 protocol, for example, Wed, 05 Sep. 2012 23:00:00 GMT. Type: string. Default value: none.

Name	Description
ETag	The entity tag that is created during the generation of an object and used to identify the content of the object. If an object is created by using the PutObject request, the ETag value of the object is the MD5 value of the object content. If an object is created by using another method, the ETag value of the content is the UUID of the object content. The ETag value of an object can be used to check whether the object content has changed. Type: string. Default value: none.
Server	The server that generates a response. Type: string. Default value: AliyunOSS
x-oss-request-id	The UUID of the response. It is created by Apsara Stack OSS. If you encounter any problems when using OSS, you can contact OSS support personnel and provide this field to help them quickly locate the problem. Type: string. Default value: none.

2.4.1.5. Service-relevant operations

2.4.1.5.1. GetService

Sending a Get request to the server can return all buckets owned by the requester, and the forward slash (/) represents the root directory.

Request syntax

```
GET / HTTP/1.1
Host: oss.example.com
Date: GMT Date
Authorization: SignatureValue
```

Request parameters

When using GetService(ListBuckets), you can prescribe a limit to the list with a prefix, marker, and max-uploads to return partial results.

Request parameters

Name	Description

Name	Description
prefix	Only the buckets whose names match a specified prefix are returned. If this parameter is not specified, prefix information is not used as a filter. Type: string. Default value: none.
marker	The starting position of the object list. Objects are sorted in the alphabetical order and those objects following this marker are listed. If this parameter is not specified, all entries are returned from the start. Type: string. Default value: none.
max-keys	The maximum number of buckets returned for one request. If this parameter is not specified, the default value is 100. The maximum value cannot exceed 1,000. Type: string. Default value: 100.

Response elements

Response elements

Name	Description
ListAllMyBucketsResult	The container used to store results of the GetService request. Type: container. Child elements: Owner and Buckets. Parent element: none.
Prefix	The prefix of the returned bucket names for one request. This element is available only when not all buckets are returned. Type: string. Parent element: ListAllMyBucketsResult.
Marker	The starting position of the current GetService(ListBucket) request. This element is available only when not all buckets are returned. Type: string. Parent element: ListAllMyBucketsResult.
MaxKeys	The maximum number of results returned for one request. This element is available only when not all buckets are returned. Type: string. Parent element: ListAllMyBucketsResult.

Name	Description
IsTruncated	Indicates whether all results have been returned. “true” means that not all results are returned this time; “false” means that all results are returned this time. This element is available only when not all buckets are returned. Type: enumeration. Valid values: true and false. Parent element: ListAllMyBucketsResult.
NextMarker	Indicates that this can be counted as a marker for the next GetService(ListBuckets) request to return the unreturned results. This element is available only when not all buckets are returned. Type: string. Parent element: ListAllMyBucketsResult.
Owner	The container that stores the information about the bucket owner. Type: container. Parent element: ListAllMyBucketsResult.
ID	The user ID of the bucket owner. Type: string. Parent element: ListAllMyBucketsResult.Owner.
DisplayName	The name of the bucket owner (which is currently the same as the user ID). Type: string. Parent element: ListAllMyBucketsResult.Owner.
Buckets	The container that stores the information about multiple buckets. Type: container. Child element: Bucket. Parent element: ListAllMyBucketsResult.
Bucket	The container that stores the bucket information. Type: container. Child elements: Name, CreationDate, and Location. Parent element: ListAllMyBucketsResult.Buckets.
Name	The bucket name. Type: string. Parent element: ListAllMyBucketsResult.Buckets.Bucket.

Name	Description
CreateDate	The time a bucket was created (format: yyyy-mm-ddThh:mm:ss.timezone, such as 2011-12-01T12:27:13.000Z) Parent element: ListAllMyBucketsResult.Buckets.Bucket.
Location	The region to which the bucket belongs. Type: string. Parent element: ListAllMyBucketsResult.Buckets.Bucket.
ExtranetEndpoint	The Internet domain name to access the bucket. Type: string. Parent element: ListAllMyBucketsResult.Buckets.Bucket.
IntranetEndpoint	The intranet domain name to access the bucket from ECS in the same region. Type: string. Parent element: ListAllMyBucketsResult.Buckets.Bucket.

Detail analysis

1. The API of GetService is valid only for users who have been authenticated.
2. If no information for user authentication is provided in a request (namely an anonymous access), 403 Forbidden is returned. Error code: AccessDenied.
3. When all buckets are returned, the returned XML does not contain the nodes Prefix, Marker, MaxKeys, IsTruncated, and NextMarker. If some results are not returned, the preceding nodes are added, in which NextMarker is used to assign the marker for the successive query.

Examples

- Sample request I:

```
GET / HTTP/1.1
Date: Thu, 15 May 2014 11:18:32 GMT
Host: regionid.example.com
Authorization: OSS n***i:C***I=
```

- Sample response I:

```
HTTP/1.1 200 OK
Date: Thu, 15 May 2014 11:18:32 GMT
Content-Type: application/xml
Content-Length: 556
Connection: keep-alive
Server: AliyunOSS
x-oss-request-id: 5***4
<? xml version="1.0" encoding="UTF-8"? >
<ListAllMyBucketsResult>
 <Owner>
 <ID>51264</ID>
 <DisplayName>51264</DisplayName>
 </Owner>
 <Buckets>
 <Bucket>
 <CreationDate>2015-12-17T18:12:43.000Z</CreationDate>
 <ExtranetEndpoint>regionid.example.com</ExtranetEndpoint>
 <IntranetEndpoint>regionid-internal.example.com</IntranetEndpoint>
 <Location>oss-cn-shanghai</Location>
 <Name>app-base-oss</Name>
 </Bucket>
 <Bucket>
 <CreationDate>2014-12-25T11:21:04.000Z</CreationDate>
 <ExtranetEndpoint>regionid.example.com</ExtranetEndpoint>
 <IntranetEndpoint>regionid-internal.example.com</IntranetEndpoint>
 <Location>regionid</Location>
 <Name>a***3</Name>
 </Bucket>
 </Buckets>
</ListAllMyBucketsResult>
```

- Sample request II:

```
GET /? prefix=xz02tphky6fjfiuc&max-keys=1 HTTP/1.1
Date: Thu, 15 May 2014 11:18:32 GMT
Host:  regionid.example.com
Authorization: OSS n***i:C***I=
```

- Sample response II:

```
HTTP/1.1 200 OK
Date: Thu, 15 May 2014 11:18:32 GMT
Content-Type: application/xml
Content-Length: 545
Connection: keep-alive
Server: AliyunOSS
x-oss-request-id: 5***5
<? xml version="1.0" encoding="UTF-8"? >
<ListAllMyBucketsResult>
 <Prefix>xz02tphky6fjfiuc</Prefix>
 <Marker></Marker>
 <MaxKeys>1</MaxKeys>
 <IsTruncated>true</IsTruncated>
 <NextMarker>xz02tphky6fjfiuc0</NextMarker>
 <Owner>
 <ID>ut_test_put_bucket</ID>
 <DisplayName>ut_test_put_bucket</DisplayName>
 </Owner>
 <Buckets>
 <Bucket>
 <CreationDate>2014-05-15T11:18:32.000Z</CreationDate>
 <ExtranetEndpoint>regionid.example.com</ExtranetEndpoint>
 <IntranetEndpoint>oss-cn-hangzhou-internal.example.com</IntranetEndpoint>
 <Location>oss-cn-hangzhou</Location>
 <Name>x***0</Name>
 </Bucket>
 </Buckets>
</ListAllMyBucketsResult>
```

2.4.1.6. Bucket-relevant operations

2.4.1.6.1. PutBucket

You can call PutBucket to create a bucket (anonymous access not allowed). The region where the new bucket is located is consistent with the region of the endpoint where a request is sent. Once the data center of the bucket is determined, all objects in this bucket will be stored in the corresponding region.

Request syntax

```
PUT / HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
x-oss-acl: Permission
Authorization: SignatureValue
```

Detail analysis

1. You can use the `x-oss-acl` header in a Put request to set access permissions for a bucket. Currently, three access permissions are available for a bucket: public-read-write, public-read, and private.
2. If the requested bucket already exists and is owned by the requester, OSS returns 200 OK.
3. If the requested bucket already exists but is not owned by the requester, the system returns 409 Conflict. Error code: BucketAlreadyExists.
4. If the bucket to be created does not conform to naming rules, the system returns 400 Bad Request. Error code: InvalidBucketName.
5. If the information for user authentication is not introduced when you initiate a Put Bucket request, the message of 403 Forbidden is returned. Error code: AccessDenied.
6. If the number of buckets exceeds the upper limit (10 by default) when you initiate a PutBucket request, OSS returns the 400 Bad Request error. Error code: TooManyBuckets.
7. If no access permission is specified for the created bucket, the Private permission applies by default.

Examples

Sample request:

```
PUT / HTTP/1.1
Host: BucketName.regionid.example.com
Date: Fri, 24 Feb 2012 03:15:40 GMT
x-oss-acl: private
Authorization: OSS q***c:7***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 24 Feb 2012 03:15:40 GMT
Location: /***
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.6.2. PutBucketACL

You can call PutBucketACL to change the access permission on a bucket. Currently, three access permissions are available for a bucket: public-read-write, public-read, and private. Put Bucket The x-oss-acl header field in a PutBucketACL request is used to set the ACL. Only the creator of the bucket has the permission to set the bucket ACL. If the operation succeeds, 200 is returned. Otherwise, the corresponding error code and message are returned.

Request syntax

```
PUT /? acl HTTP/1.1
x-oss-acl: Permission
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

1. When a bucket already exists and is owned by the request sender and the permission in the request is different from the existing permission, this request does not change bucket content but updates permission.
2. If the information for user authentication is not introduced when you initiate a Put Bucket request, the message of 403 Forbidden is returned. Error code: AccessDenied.
3. If the x-oss-acl header field is not specified in the request and the bucket already exists and belongs to the request sender, the original permission on the bucket remains unchanged.

Examples

Sample request:

```
PUT /? acl HTTP/1.1
x-oss-acl: public-read
Host: BucketName.regionid.example.com
Date: Fri, 24 Feb 2012 03:21:12 GMT
Authorization: OSS q***c:K***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 24 Feb 2012 03:21:12 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

If the permission specified does not exist, OSS returns the 400 Bad Request error.

Returned error example:

```
HTTP/1.1 400 Bad Request
x-oss-request-id: 5***9
Date: Fri, 24 Feb 2012 03:55:00 GMT
Content-Length: 309
Content-Type: text/xml; charset=UTF-8
Connection: keep-alive
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<Error>
 <Code>InvalidArgument</Code>
 <Message>no such bucket access control exists</Message>
 <RequestId>5***9</RequestId>
 <HostId>***-test.example.com</HostId>
 <ArgumentName>x-oss-acl</ArgumentName>
 <ArgumentValue>error-acl</ArgumentValue>
</Error>
```

2.4.1.6.3. PutBucketLogging

OSS provides bucket access logs for bucket owners to understand and analyze bucket access records easily. OSS does not guarantee that the bucket access logs contain all access records.

A bucket owner can enable the access logging function for his/her bucket. When this function is enabled, the OSS automatically records detailed information about the requests to this bucket, and follows the user-specified rules to write the access logs as an object into the user-specified bucket hourly. OSS provides bucket access logs for bucket owners to understand and analyze bucket access records easily. OSS does not guarantee that the bucket access logs contain all access records.

Request syntax

```
PUT /? logging HTTP/1.1
Date: GMT Date
Content-Length: ContentLength
Content-Type: application/xml
Authorization: SignatureValue
Host: BucketName.regionid.example.com
<? xml version="1.0" encoding="UTF-8"? >
<BucketLoggingStatus>
 <LoggingEnabled>
 <TargetBucket>TargetBucket</TargetBucket>
 <TargetPrefix>TargetPrefix</TargetPrefix>
 </LoggingEnabled>
</BucketLoggingStatus>
```

Request elements

Request elements

Name	Description	Required
BucketLoggingStatus	The container that stores access log status information. Type: container. Child element: LoggingEnabled. Parent element: none.	Yes
LoggingEnabled	The container that stores the access log information. This element is required only when server access logging is enabled. Type: container. Child elements: TargetBucket and TargetPrefix. Parent element: BucketLoggingStatus.	No
TargetBucket	The bucket that stores access logs. Type: string. Child element: none. Parent element: BucketLoggingStatus.LoggingEnabled.	This element is required when access logging is enabled.
TargetPrefix	The name prefix of the object that stores access logs. Type: string. Child element: none. Parent element: BucketLoggingStatus.LoggingEnabled.	No

The name format of the object that stores access logs.

```
<TargetPrefix><SourceBucket>-YYYY-mm-DD-HH-MM-SS-UniqueString
```

In the format, TargetPrefix is specified by the user. YYYY, mm, DD, HH, MM, and SS indicate the year, month, day, hour, minutes, and seconds of the creation time in Arabic numerals (note the digits); and UniqueString is the string generated by OSS system. The following is an example for the name of an object that stores OSS access logs:

```
MyLog-oss-example-2012-09-10-04-00-00-0000
```

In the preceding example, "MyLog-" is the object prefix specified by the user. “oss-example” is the name of the origin bucket; “2012-09-10-04-00-00” is the object creation time (Beijing time). “0000” is the string generated by OSS system.

Log object format

Log object format

Name	Example	Description
Remote IP	119.140.142.11	The IP address from which the request is initiated. (The proxy or user firewall may block this field.)
Reserved	-	Reserved field.
Reserved	-	Reserved field.
Time	[02/May/2012:00:00:04 +0800]	Time the OSS receives the request.
Request-URI	"GET /aliyun-logo.png HTTP/1.1"	User-Requested URI (including query-string).
HTTP Status	200	HTTP status code returned by the OSS.
SentBytes	5576	Traffic that the user downloads from OSS.
RequestTime (ms)	71	Time spent in completing this request (in ms).
Referer	http://www.aliyun.com/product/oss	Requested TTP Referer.
User-Agent	curl/7.15.5	The HTTP User-Agent header.
HostName	oss-example.regionid.example.com	The domain name for access request.
Request ID	505B01695037C2AF032593A4	The UUID used to uniquely identify this request.
LoggingFlag	true	Indicates whether the access logging function is enabled.
Requester Aliyun ID	1657136103983691	The Alibaba Cloud ID of the requester, "-" for anonymous access.
Operation	GetObject	Request type.
Bucket	oss-example	The name of the bucket requested for access.
Key	/aliyun-logo.png	User-Requested Key.
ObjectSize	5576	Object size.

Name	Example	Description
Server Cost Time (ms)	17	Time taken by the OSS server to process this request, in ms.
Error Code	NoSuchBucket	The error code returned by OSS.
Request Length	302	The length of user request, in bytes.
UserID	1657136103983691	The ID of the bucket owner.
Delta DataSize	280	The Bucket size variation. The hyphen (-) indicates no changes.
Sync Request	-	Indicates whether this is a origin retrieval request from CND. The hyphen (-) indicates that this is not an origin retrieval request.
Reserved	-	Reserved field.

Detail analysis

1. The source bucket to which an object belongs and the target bucket where the processed object is stored must belong to the same user.
2. In the preceding request syntax, BucketName indicates the bucket for which access logging is enabled. TargetBucket indicates the bucket into which access logs are saved. TargetPrefix indicates the name prefix of the object storing access logs and can be null.
3. The source bucket and target bucket can be the same or different buckets. You can save logs from multiple source buckets to the same target bucket. (In this case, we recommend that you assign different values to TargetPrefix.)
4. To disable the access logging function for a bucket, you only must send an empty BucketLoggingStatus request. For a detailed method, see the following sample request.
5. All PUT Bucket Logging requests must be provided with signatures, indicating that anonymous access is not supported.
6. If the initiator of a PUT Bucket Logging request is not the owner of the source bucket (BucketName in the sample request), the OSS returns error code 403.
7. If the source bucket does not exist, OSS returns the error code: NoSuchBucket.
8. If the initiator of a PUT Bucket Logging request is not the owner of the target bucket (indicated by TargetBucket in the sample request), OSS returns Error 403. If the target bucket does not exist, OSS returns the error code: InvalidTargetBucketForLogging.
9. The source bucket and target bucket must belong to the same region. Otherwise, Error 400 with the error code: InvalidTargetBucketForLogging is returned.
10. If a PUT Bucket Logging request has an invalid XML, the error code: MalformedXML is returned.
11. The source bucket and target bucket can be the same bucket. You can save the logs of different source buckets into the same target bucket. (Note that you must set TargetPrefix to different values.)
12. When the source bucket is deleted, the corresponding logging rules are also deleted.
13. OSS generates a bucket access log file every hour. However, all requests during the hour may

not be recorded in the log file, but may be recorded in the previous or next log file.

14. In the naming rules for log files generated by the OSS, "UniqueString" is just a UUID that the OSS generates for a file to uniquely identify the file.
15. Each time the OSS generates a bucket access log file, a PUT operation is counted and the occupied space is recorded, but the generated traffic is not recorded. After log files are generated, you can operate these log files as common objects.
16. OSS ignores all query-string parameters prefixed by "x-" but such query-string parameters are recorded in access logs. If you want to mark a special request from massive access logs, you can add a query-string parameter prefixed by "x-" to the URL. Example:

    ```
    http://oss-example.regionid.example.com/aliyun-logo.png
    ```

    ```
    http://oss-example.regionid.example.com/aliyun-logo.png?x-user=admin
    ```

    When OSS processes the preceding two requests, the results are the same. However, you can search access logs with x-user=admin to quickly locate the marked request.
17. You may see "-" in any field of OSS logs. It indicates that data is unknown or the field is invalid for the current request.
18. Certain fields are added to the end of OSS log files in future based on the requirements. We recommend that developers to consider compatibility issues when developing log processing tools.
19. If the Content-MD5 field value is specified in the request header, OSS calculates the Content-MD5 field value in the request body and checks whether the two values are the same. If they are different, OSS returns the InvalidDigest error.

Examples

Example of a request for enabling bucket access logging:

```
PUT /? logging HTTP/1.1
Host: ***.regionid.example.com
Content-Length: 186
Date: Fri, 04 May 2012 03:21:12 GMT
Authorization: OSS q***c:K***=
<? xml version="1.0" encoding="UTF-8"? >
<BucketLoggingStatus>
<LoggingEnabled>
<TargetBucket>doc-log</TargetBucket>
<TargetPrefix>MyLog-</TargetPrefix>
</LoggingEnabled>
</BucketLoggingStatus>
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 04 May 2012 03:21:12 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

Example of a request for disabling bucket access logging:

```
PUT /? logging HTTP/1.1
Host: ***.regionid.example.com
Content-Type: application/xml
Content-Length: 86
Date: Fri, 04 May 2012 04:21:12 GMT
Authorization: OSS q***c:K***=
<? xml version="1.0" encoding="UTF-8"? >
<BucketLoggingStatus>
</BucketLoggingStatus>
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 04 May 2012 04:21:12 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.6.4. PutBucketWebsite

You can call PutBucketWebsite to set a bucket to the static website hosting mode.

Request syntax

```
PUT /? website HTTP/1.1
Date: GMT Date
Content-Length: ContentLength
Content-Type: application/xml
Host: BucketName.regionid.example.com
Authorization: SignatureValue

<? xml version="1.0" encoding="UTF-8"? >
<WebsiteConfiguration>
  <IndexDocument>
    <Suffix>index.html</Suffix>
  </IndexDocument>
  <ErrorDocument>
    <Key>errorDocument.html</Key>
  </ErrorDocument>
</WebsiteConfiguration>
```

Request elements

Request elements

Name	Description	Required
ErrorDocument	The parent element of the child element Key. Type: container. Parent element: WebsiteConfiguration.	No
IndexDocument	The parent element of the child element Suffix. Type: container. Parent element: WebsiteConfiguration.	Yes
Key	The object name contained in the returned 404 Not Found message. Type: string. Parent element: WebsiteConfiguration.ErrorDocument. Conditional: This element is required only when ErrorDocument is set.	Conditional

Name	Description	Required
Suffix	The index file name added when a directory URL is returned. This element cannot be empty or contain a forward slash (/). For example, if the index file is set to index.html, regionid.example.com/mybucket/mydir/ contained in an access request is converted into regionid.example.com/mybucket/index.html by default. Type: string. Parent element: WebsiteConfiguration.IndexDocument.	Yes
WebsiteConfiguration	The container that holds the request. Type: container. Parent element: none.	Yes

Detail analysis

1. Static websites are the websites where all Webpages are composed of static content, including scripts such as JavaScript executed on the client. OSS does not support content that needs to be processed by the server, such as PHP, JSP, and APS.NET.
2. To use your own domain name to access bucket-based static websites, you can use CNAME. For more information about the configuration method, see section 3.4 "Bind a custom domain name."
3. When setting a bucket to the static website hosting mode, you must specify the index page, and the error page is optional.
4. When you set a bucket to the static website hosting mode, the specified index page and error page are an object in the bucket.
5. After a bucket is set to the static website hosting mode, the OSS returns the index page for anonymous access to the root domain name of the static website, and returns the result of Get Bucket for signed access to the root domain name of the static website.
6. If the Content-MD5 field value is specified in the request header, OSS calculates the Content-MD5 field value in the request body and checks whether the two values are the same. If they are different, OSS returns the InvalidDigest error.

Examples

Sample request:

```
PUT /? website HTTP/1.1
Host: oss-example.regionid.example.com
Content-Length: 209
Date: Fri, 04 May 2012 03:21:12 GMT
Authorization: OSS q***c:K***=

<? xml version="1.0" encoding="UTF-8"? >
<WebsiteConfiguration>
<IndexDocument>
<Suffix>index.html</Suffix>
</IndexDocument>
<ErrorDocument>
<Key>error.html</Key>
</ErrorDocument>
</WebsiteConfiguration>
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 04 May 2012 03:21:12 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.6.5. PutBucketReferer

You can call this operation to configure a Referer whitelist and specify whether to allow a request whose Refer field is empty.

Request syntax

```
PUT /? referer HTTP/1.1
Date: GMT Date
Content-Length: ContentLength
Content-Type: application/xml
Host: BucketName.oss.example.com
Authorization: SignatureValue

<? xml version="1.0" encoding="UTF-8"? >
<RefererConfiguration>
<AllowEmptyReferer>true</AllowEmptyReferer>
  <RefererList>
    <Referer> http://www.aliyun.com</Referer>
    <Referer> https://www.aliyun.com</Referer>
    <Referer> http://www. *.com</Referer>
    <Referer> https://www.?.aliyuncs.com</Referer>
  </RefererList>
</RefererConfiguration>
```

Request elements

Request elements

Element	Description	Required
RefererConfiguration	The container that contains the Referer configuration content. Type: container. Child node: AllowEmptyReferer and RefererList. Parent node: none.	Yes
AllowEmptyReferer	Specifies whether to allow the request whose Referer field is empty. Type: Boolean. Valid values: true and false. Default value: true. Parent node: RefererConfiguration.	Yes
RefererList	The container that contains the Referer whitelist. Type: container. Parent node: RefererConfiguration. Child node: Referer.	Yes
Referer	The specified Referer whitelist. Type: String. Parent node: RefererList.	No

Detail analysis

1. Only the bucket owner can initiate a PutBucketReferer request. Otherwise, OSS returns 403 Forbidden. Error code: AccessDenied.
2. The configuration specified in AllowEmptyReferer replaces the previous AllowEmptyReferer configuration. This field is required. By default, AllowEmptyReferer is set to true.
3. This operation replaces the existing configured whitelist with the whitelist specified by RefererList. When empty RefererList that contains no Referer request elements is uploaded, this operation overwrites the configured whitelist. The existing configured RefererList is

deleted.

4. If the Content-MD5 request header is specified, OSS calculates the Content-MD5 header value in the request body and checks whether the two values are the same. If they are different, InvalidDigest is returned.

Examples

Sample requests with no Referer fields included:

```
PUT /? referer HTTP/1.1
Host: BucketName.oss.example.com
Content-Length: 247
Date: Fri, 04 May 2012 03:21:12 GMT
Authorization: OSS q***c:K***=

<? xml version="1.0" encoding="UTF-8"? >
<RefererConfiguration>
<AllowEmptyReferer>true</AllowEmptyReferer>
< RefererList />
</RefererConfiguration>
```

Sample requests with Referer fields included:

```
PUT /? referer HTTP/1.1
Host: BucketName.oss.example.com
Content-Length: 247
Date: Fri, 04 May 2012 03:21:12 GMT
Authorization: OSS q***c:K***=

<? xml version="1.0" encoding="UTF-8"? >
<RefererConfiguration>
<AllowEmptyReferer>true</AllowEmptyReferer>
< RefererList>
<Referer> http://www.aliyun.com</Referer>
<Referer> https://www.aliyun.com</Referer>
<Referer> http://www. *.com</Referer>
<Referer> https://www.?.aliyuncs.com</Referer>
</ RefererList>
</RefererConfiguration>
```

Sample responses:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 04 May 2012 03:21:12 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.6.6. PutBucketLifecycle

The bucket owner can set the lifecycle of a bucket by using PutBucketLifecycle. After Lifecycle is enabled, OSS automatically deletes the objects or transitions the objects (to another storage class) corresponding the lifecycle rules on a regular basis.

Request syntax

```
PUT /? lifecycle HTTP/1.1
Date: GMT Date
Content-Length: ContentLength
Content-Type: application/xml
Authorization: SignatureValue
Host: BucketName.oss.example.com
<? xml version="1.0" encoding="UTF-8"? >
<LifecycleConfiguration>
 <Rule>
 <ID>RuleID</ID>
 <Prefix>Prefix</Prefix>
 <Status>Status</Status>
 <Expiration>
 <Days>Days</Days>
 </Expiration>
 <AbortMultipartUpload>
 <Days>Days</Days> </AbortMultipartUpload>
 </Rule>
</LifecycleConfiguration>
```

Request elements

Request elements

Name	Description	Required

Name	Description	Required
CreatedBeforeDate	Specifies the time before which the rules take effect. The date must conform to the ISO 8601 format and always be UTC 00:00. For example: 2002-10-11T00:00:00.000Z, which indicates that the objects with a last modification time before 2002-10-11T00:00:00.000Z are deleted or transitioned to another storage class, and the objects modified after this time are not deleted or transitioned. Type: string. Parent element: Expiration or AbortMultipartUpload.	Either Days or CreatedBeforeDate is specified.
Days	The number of days after which the rule takes effect following the last modification time of the object. Type: positive integer. Parent element: Expiration.	Either Days or CreatedBeforeDate is specified.
Expiration	The expiration time of the rule for the specified object. Type: container. Child element: Days or CreatedBeforeDate. Parent element: Rule.	No
AbortMultipartUpload	The expiration time of the rule for the specified uncompleted part. Type: container. Child element: Days or CreatedBeforeDate. Parent element: Rule.	No
ID	The unique ID of a rule. An ID is composed of 255 bytes at most. When you fail to specify this value or this value is null, the OSS generates a unique value for you. Type: string. Child element: none. Parent element: Rule.	No
LifecycleConfiguration	The container that stores lifecycle configurations, which can contain a maximum of 1,000 rules. Type: container. Chile element: Rule. Parent element: none.	Yes

Name	Description	Required
Prefix	Specifies the prefix applicable to a rule. Only those objects with a matching prefix can be affected by the rule. Overlapping prefixes are not allowed. Type: string. Child element: none. Parent element: Rule.	Yes
Rule	A matching rule. Type: container. Child elements: ID, Prefix, Status, and Expiration. Parent element: LifecycleConfiguration.	Yes
Status	If the value is Enabled, OSS executes this rule regularly. If the value is Disabled, OSS ignores this rule. Type: string. Parent element: Rule. Valid value: Enabled or Disabled.	Yes

Detail analysis

1. Only the bucket owner can initiate a PutBucketReferer request. Otherwise, OSS returns the 403 Forbidden message. Error code: AccessDenied.
2. This operation creates a new lifecycle rule. The original rule, if any, is overwritten.
3. You can also set an expiration time for an object, or for the Part. Here, the Part refers to the unsubmitted parts for multipart upload.

Examples

Sample request:

```
PUT /? lifecycle HTTP/1.1
Host: BucketName.oss.example.com
Content-Length: 443
Date: Mon, 14 Apr 2014 01:08:38 GMT
Authorization: OSS q***c:K***=
<? xml version="1.0" encoding="UTF-8"? >
</LifecycleConfiguration>
 <Rule>
 <ID>delete objects and parts after one day</ID>
 <Prefix>logs/</Prefix>
 <Status>Enabled</Status>
 <Expiration>
 <Days>1</Days>
 </Expiration>
 <AbortMultipartUpload>
 <Days>1</Days>
 </AbortMultipartUpload>
 </Rule>
 <Rule>
 <ID>delete created before date</ID>
 <Prefix>backup/</Prefix>
 <Status>Enabled</Status>
 <Expiration>
 <CreatedBeforeDate>2014-10-11T00:00:00.000Z</CreatedBeforeDate>
 </Expiration>
 <AbortMultipartUpload>
 <CreatedBeforeDate>2014-10-11T00:00:00.000Z</CreatedBeforeDate>
 </AbortMultipartUpload>
 </Rule>
</LifecycleConfiguration>
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Mon, 14 Apr 2014 01:17:10 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.6.7. PutBucketTagging

You can call PutBucketTagging to add a group of tags to a bucket. By using tags, you can manage buckets by category, such as checking bills by tag and displaying only the buckets with the specified tags during the ListBucket operation.

Request syntax

```
PUT /? tagging HTTP/1.1
Date: GMT Date
Content-Length: ContentLength
Content-Type: application/xml
Authorization: SignatureValue
Host: BucketName.regionid.example.com
<? xml version="1.0" encoding="UTF-8"? >
<Tagging>
 <TagSet>
 <Tag>
 <Key>Tag Name</Key>
 <Value>Tag Value</Value>
 </Tag>
 </TagSet>
</Tagging>
```

Request elements

Request elements

Name	Description	Required
Tagging	The container for the bucket tag. Type: container. Child element: TagSet. Parent element: none.	Yes
TagSet	The container that holds a group of tags. Each bucket can have a maximum of 10 tags. Type: container. Child element: Tag. Parent element: Tagging.	Yes

Name	Description	Required
Tag	The container that holds a single tag. Type: container. Child element: Key or Value. Parent element: TagSet.	Yes
Key	The name of the tag. For the same bucket, the tag name is unique and required. The tag name is case-sensitive. Type: string. Child element: none. Parent element: Tag.	Yes
Value	The value of the tag. A tag can have multiple values or an empty value. The value is case-sensitive. Type: string. Child element: none. Parent element: Tag.	Yes

Detail analysis

1. A maximum of 10 tags can be created for a bucket. If the number of tags that you have created exceeds the threshold, OSS returns the HTTP 400 Bad Request message. Error code: TooManyTags.
2. The key and value of a bucket tag can be all UTF-8 characters except those whose decimal values in ASCII code are smaller than 32 or equal to 127. The key and value are case-sensitive. The tag key can have a maximum of 64 characters. The tag value can have a maximum of 128 characters. If the key or value of a bucket tag does not comply with these rules, OSS returns the HTTP 400 Bad Request message. Error code: InvalidArgument.
3. Two tags with duplicate keys cannot be created for a bucket. Otherwise, OSS returns the HTTP 400 Bad Request message. Error code: RepeatedTags.
4. The prefix aliyun is the tag prefix reserved by OSS. A tag key cannot start with the prefix aliyun (neither uppercase nor lowercase). Otherwise, OSS returns the HTTP 400 Bad Request message. Error code: InvalidArgument.
5. PutBucketTagging uses the overwriting semantics. A newly added tag completely overwrites the existing one.

Examples

Sample request

```
PUT /? tagging HTTP/1.1
Host: ***.regionid.example.com
Content-Type: application/xml
Content-Length: 86
Date: Thu, 23 Jun 2015 15:39:12 GMT
Authorization: OSS q***c:K***=
<Tagging>
 <TagSet>
 <Tag>
 <Key>Project</Key>
<Value>Project One</Value>
 </Tag>
 <Tag>
 <Key>User</Key>
 <Value>jsmith</Value>
 </Tag>
 </TagSet>
</Tagging>
```

Sample response

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Thu, 23 Jun 2015 15:39:12 GMT
Content-Length: 0
Connection: close
Server: AliyunOSS
```

2.4.1.6.8. GetBucket

You can call GetBucket to list the information about all objects in a bucket.

Request syntax

```
GET / HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Request parameters

When you initiate a GetBucket (ListObject) request, you can use prefix, marker, delimiter, and max-keys to prescribe a limit to the list to return partial results. In addition, you can use the encoding-type parameter to encode the following elements in the response: Delimiter, Marker, Prefix, NextMarker, and Key.

Request parameters

Name	Description
delimiter	The delimiter used to group objects by name. CommonPrefixes specify a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter. Type: string. Default value: none.
marker	The starting position of the object list. Objects are sorted in the alphabetical order and those objects following this marker are listed. Type: string. Default value: none.
max-keys	The maximum number of objects returned for one request. If this parameter is not specified, the default value 100 is used. The maximum number cannot exceed 1,000. Type: string. Default value: 100.
prefix	The prefix that must be contained in the keys of the returned objects. Note that if you use a prefix to make a query, the returned key values still contain the prefix. Type: string. Default value: none.
encoding-type	The encoding type of the key in the response. Parameters delimiter, marker, prefix, NextMarker, and key use UTF-8 characters, but the XML 1.0 Standard does not support parsing certain control characters, such as the characters with ASCII values from 0 to 10. If some elements in the response contain control characters that are not supported by the XML 1.0 Standard, encoding-type can be specified to encode these elements, such as delimiter, marker, prefix, NextMarker, and key. Type: string. Default value: none. Valid value: url.

Response elements

Response elements

Name	Description

Name	Description
Contents	The container that stores the returned Object Meta. Type: container. Parent element: ListBucketResult.
CommonPrefixes	If the Delimiter parameter is specified in the request, the response contains the CommonPrefixes element. This element specifies a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter. Type: string. Parent element: ListBucketResult.
Delimiter	The delimiter used to group objects by name. CommonPrefixes specify a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter. Type: string. Parent element: ListBucketResult.
EncodingType	The encoding type of the key in the response. In addition, you can use the encoding-type parameter to encode the following elements in the response: Delimiter, Marker, Prefix, NextMarker, and Key. Type: string. Parent element: ListBucketResult.
DisplayName	The name of the object owner. Type: string. Parent element: ListBucketResult.Contents.Owner.
ETag	The entity tag that is created during the generation of an object and used to identify the content of the object. If an object is created upon a PutObject request, the ETag value of the object is the MD5 value of the object content. If an object is created with another method, the ETag value of the content is the UUID of the object content. The ETag value of an object can be used to check whether the object content has changed. However, we recommend that you not use the ETag of an object as the MD5 value of the object to verify data integrity. Type: string. Parent element: ListBucketResult.Contents.
ID	The user ID of the bucket owner. Type: string. Parent element: ListBucketResult.Contents.Owner.

Name	Description
IsTruncated	Indicates whether all results have been returned. True indicates that this response does not contain all the parts discovered by OSS. False indicates that this response contains all the parts discovered by OSS. Type: enumeration. Valid values: true and false. Parent element: ListBucketResult.
Key	The key of the object. Type: string. Parent element: ListBucketResult.Contents.
LastModified	The last modification time of the object. Type: time. Parent element: ListBucketResult.Contents.
ListBucketResult	The container that stores the response of the GetBucket request. Type: container. Child element: Name, Prefix, Marker, MaxKeys, Delimiter, IsTruncated, Nextmarker, and Contents. Parent element: none.
Marker	The starting position for returning objects upon the GetBucket (ListObject) request. Type: string. Parent element: ListBucketResult.
MaxKeys	The maximum number of objects returned for this request. Type: string. Parent element: ListBucketResult.
Name	The name of the bucket. Type: string. Parent element: ListBucketResult.
Owner	The container that stores the information about the bucket owner. Type: container. Child nodes: DisplayName and ID. Parent element: ListBucketResult.

Name	Description
Prefix	The prefix contained in the names of returned objects. Type: string. Parent element: ListBucketResult.
Size	The size of the returned object content, in bytes. Type: string. Parent element: ListBucketResult.Contents.
StorageClass	The storage type of the returned objects. Currently, only the Standard type is available. Type: string. Parent element: ListBucketResult.Contents.

Detail analysis

1. The user-defined Object Meta is not returned for the GetBucket request.
2. If the bucket to be accessed does not exist, or if you attempt to access a bucket which cannot be created because of standard naming rules are not followed when naming a bucket, Error 404 Not Found with the error code NoSuchBucket is returned.
3. If you have no permission to access the bucket, the system returns Error 403 Forbidden with the error code AccessDenied.
4. If listing cannot be completed at one time because of the max-keys setting, `<NextMarker>` is appended to the returned result, indicating that this can be taken as a marker for continued listing. The value in NextMarker is still in the list result.
5. During a condition query, even if the marker does not exist in the list actually, what is returned is printed starting from the next to what conforms to the marker letter sorting. If the value of max-keys is less than 0 or exceeds 1000, OSS returns the 400 Bad Request message. Error code: InvalidArgument.
6. If the prefix, marker, or delimiter parameters do not meet the length requirement, 400 Bad Request is returned. Error code: InvalidArgument.
7. The prefix and marker parameters are used to achieve display by pages, and the parameter length must be less than 1,024 bytes.
8. If Prefix is set to a folder name in the request, the object names starting with this prefix are listed, including all recursive objects and subfolders in this folder. Additionally, if we set the Delimiter as “/ “, the returned values lists the files in the folder and the subfolders are returned in the CommonPrefixes section. Recursive files and folders in the subfolders are not displayed. For example, a bucket has the following three objects: fun/test.jpg, fun/movie/001.avi, and fun/movie/007.avi. If the prefix is set to fun/, three objects are returned. If the delimiter is set to a forward slash (/) additionally, the fun/test.jpg object and the fun/movie/ prefix are returned. In other words, the folder logic is achieved.

Scenario example

Four objects are available in the my_oss bucket and are named as:

- oss.jpg
- fun/test.jpg
- fun/movie/001.avi
- fun/movie/007.avi

Examples

Sample request:

```
GET / HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 08:43:27 GMT
Authorization: OSS q***c:B***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 24 Feb 2012 08:43:27 GMT
Content-Type: application/xml
Content-Length: 1866
Connection: keep-alive
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<ListBucketResult xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
<Name>oss-example</Name>
<Prefix></Prefix>
<Marker></Marker>
<MaxKeys>100</MaxKeys>
<Delimiter></Delimiter>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>fun/movie/001.avi</Key>
    <LastModified>2012-02-24T08:43:07.000Z</LastModified>
    <ETag>&amp;quot;5***E&amp;quot;</ETag>
    <Type>Normal</Type>
    <Size>344606</Size>
    <StorageClass>Standard</StorageClass>
    <Owner>
      <ID>00220120222</ID>
      <DisplayName>user-example</DisplayName>
    </Owner>
  </Contents>
```

```
  <Contents>
    <Key>fun/movie/007.avi</Key>
    <LastModified>2012-02-24T08:43:27.000Z</LastModified>
    <ETag>&amp;quot;5***E&amp;quot;</ETag>
    <Type>Normal</Type>
    <Size>344606</Size>
    <StorageClass>Standard</StorageClass>
    <Owner>
      <ID>00220120222</ID>
      <DisplayName>user-example</DisplayName>
    </Owner>
  </Contents>
<Contents>
    <Key>fun/test.jpg</Key>
    <LastModified>2012-02-24T08:42:32.000Z</LastModified>
    <ETag>&amp;quot;5***E&amp;quot;</ETag>
    <Type>Normal</Type>
    <Size>344606</Size>
    <StorageClass>Standard</StorageClass>
    <Owner>
      <ID>0***2</ID>
      <DisplayName>***</DisplayName>
    </Owner>
  </Contents>
  <Contents>
    <Key>oss.jpg</Key>
    <LastModified>2012-02-24T06:07:48.000Z</LastModified>
    <ETag>&amp;quot;5***E&amp;quot;</ETag>
    <Type>Normal</Type>
    <Size>344606</Size>
    <StorageClass>Standard</StorageClass>
    <Owner>
      <ID>0***2</ID>
      <DisplayName>***</DisplayName>
    </Owner>
  </Contents>
</ListBucketResult>
```

Example of a request that contains the prefix parameter:

```
GET /? prefix=fun HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 08:43:27 GMT
Authorization: OSS q***c:B***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 24 Feb 2012 08:43:27 GMT
Content-Type: application/xml
Content-Length: 1464
Connection: keep-alive
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<ListBucketResult xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
<Name>***</Name>
<Prefix>fun</Prefix>
<Marker></Marker>
<MaxKeys>100</MaxKeys>
<Delimiter></Delimiter>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>fun/movie/001.avi</Key>
    <LastModified>2012-02-24T08:43:07.000Z</LastModified>
    <ETag>&amp;quot;5***E&amp;quot;</ETag>
    <Type>Normal</Type>
    <Size>344606</Size>
    <StorageClass>Standard</StorageClass>
    <Owner>
      <ID>0***2</ID>
      <DisplayName>***</DisplayName>
    </Owner>
  </Contents>
  <Contents>
    <Key>fun/movie/007.avi</Key>
    <LastModified>2012-02-24T08:43:27.000Z</LastModified>
    <ETag>&amp;quot;5***E&amp;quot;</ETag>
    <Type>Normal</Type>
    <Size>344606</Size>
    <StorageClass>Standard</StorageClass>
```

```
    <StorageClass>Standard</StorageClass>
    <Owner>
      <ID>0***2</ID>
      <DisplayName>***</DisplayName>
    </Owner>
  </Contents>
  <Contents>
    <Key>fun/test.jpg</Key>
    <LastModified>2012-02-24T08:42:32.000Z</LastModified>
    <ETag>&amp;quot;5***E&amp;quot;</ETag>
    <Type>Normal</Type>
    <Size>344606</Size>
    <StorageClass>Standard</StorageClass>
    <Owner>
      <ID>0***2</ID>
      <DisplayName>***</DisplayName>
    </Owner>
  </Contents>
</ListBucketResult>
```

Example of a request that contains prefix and delimiter parameters:

```
GET /? prefix=fun/&delimiter=/ HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 08:43:27 GMT
Authorization: OSS q***c:D***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 24 Feb 2012 08:43:27 GMT
Content-Type: application/xml
Content-Length: 712
Connection: keep-alive
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<ListBucketResult xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
<Name>oss-example</Name>
<Prefix>fun/</Prefix>
<Marker></Marker>
<MaxKeys>100</MaxKeys>
<Delimiter>/</Delimiter>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>fun/test.jpg</Key>
    <LastModified>2012-02-24T08:42:32.000Z</LastModified>
    <ETag>&amp;quot;5***E&amp;quot;</ETag>
    <Type>Normal</Type>
    <Size>344606</Size>
    <StorageClass>Standard</StorageClass>
    <Owner>
      <ID>0***2</ID>
      <DisplayName>***</DisplayName>
    </Owner>
  </Contents>
 <CommonPrefixes>
    <Prefix>fun/movie/</Prefix>
 </CommonPrefixes>
</ListBucketResult>
```

2.4.1.6.9. GetBucketAcl

You can call GetBucketACL to obtain the access permission for a bucket.

Request syntax

```
GET /? acl HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Response elements

Response elements

Name	Description
AccessControlList	The container that stores the ACL information. Type: container. Parent element: AccessControlPolicy.
AccessControlPolicy	The container that stores the results of the GetBucketAcl request. Type: container. Parent element: none.
DisplayName	The name of the bucket owner (which is currently the same as the user ID). Type: string. Parent element: AccessControlPolicy.Owner.
Grant	The ACL permission of the bucket. Type: enumeration. Valid values: private, public-read, and public-read-write. Parent element: AccessControlPolicy.AccessControlList.
ID	The user ID of the bucket owner. Type: string. Parent element: AccessControlPolicy.Owner.
Owner	The container that stores the information about the bucket owner. Type: container. Parent element: AccessControlPolicy.

Detail analysis

Only the bucket owner can call the GetBucketAcl API.

Examples

Sample request:

```
GET /? acl HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 04:11:23 GMT
Authorization: OSS q***c:C***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***B
Date: Fri, 24 Feb 2012 04:11:23 GMT
Content-Length: 253
Content-Type: application/xml
Connection: keep-alive
Server: AliyunOSS

<? xml version="1.0" ? >
<AccessControlPolicy>
  <Owner>
    <ID>0***2</ID>
    <DisplayName>***</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>public-read</Grant>
  </AccessControlList>
</AccessControlPolicy>
```

2.4.1.6.10. GetBucketLocation

You can call GetBucketLocation to view the location information about the region to which a bucket belongs.

Request syntax

```
GET /? location HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Response elements

Response elements

Name	Description
LocationConstraint	The region to which the bucket belongs. Type: string. Values: oss-cn-hangzhou, oss-cn-qingdao, oss-cn-beijing, oss-cn-hongkong, oss-cn-shenzhen, and oss-cn-shanghai.

Detail analysis

1. Only the owner of a bucket can view the location information of the bucket. If other users attempt to access the location information, the error 403 Forbidden with the error code: AccessDenied is returned.
2. The LocationConstraint parameter has the following valid values: oss-cn-hangzhou, oss-cn-qingdao, oss-cn-beijing, oss-cn-hongkong, oss-cn-shenzhen, oss-cn-shanghai, oss-us-west-1, oss-us-east-1, and oss-ap-southeast-1, which respectively correspond to China (Hangzhou), China (Qingdao), China (Beijing), Hong Kong, China (Shenzhen), China (Shanghai), US (Silicon Valley), US (Virginia), and Singapore.

Examples

Sample request:

```
Get /? location HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 04 May 2012 05:31:04 GMT
Authorization: OSS q***c:c***=
```

Sample response with logging rules configured:

```
HTTP/1.1 200
x-oss-request-id: 5***B
Date: Fri, 15 Mar 2013 05:31:04 GMT
Connection: keep-alive
Content-Length: 90
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<LocationConstraint xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >oss-cn-hangzhou</LocationC
onstraint >
```

2.4.1.6.11. GetBucketInfo

You can call GetBucketInfo to view the bucket information. The information includes:

- The time the domain name was created.
- Internet access endpoint
- Intranet access endpoint
- Bucket owner information
- Bucket ACL (AccessControlList)

Request syntax

```
GET /? bucketInfo HTTP/1.1
Host: BucketName.oss.example.com
Date: GMT Date
Authorization: SignatureValue
```

Response elements

Response elements

Name	Description
BucketInfo	The container that stores the bucket information content. Type: container. Child element: Bucket. Parent element: none.
Bucket	The container that stores the specific information about the bucket. Type: container. Parent element: BucketInfo node.
CreationDate	The creation time of the bucket. Time format: 2013-07-31T10:56:21.000Z. Type: time. Parent element: BucketInfo.Bucket.
ExtranetEndpoint	The Internet domain name to access the bucket. Type: string. Parent element: BucketInfo.Bucket.
IntranetEndpoint	The intranet domain name to access the bucket from ECS in the same region. Type: string. Parent element: BucketInfo.Bucket.
Location	The region of the data center where the bucket is located. Type: string. Parent element: BucketInfo.Bucket.
Name	The name of the bucket. Type: string. Parent element: BucketInfo.Bucket.

Name	Description
Owner	The container that stores the information about the bucket owner. Type: container. Parent element: BucketInfo.Bucket.
ID	The user ID of the bucket owner. Type: string. Parent element: BucketInfo.Bucket.Owner.
DisplayName	The name of the bucket owner (which is currently the same as the user ID). Type: string. Parent element: BucketInfo.Bucket.Owner.
AccessControlList	The container that stores the ACL information. Type: container. Parent element: BucketInfo.Bucket.
Grant	The ACL permission of the bucket. Type: enumeration. Valid values: private, public-read, and public-read-write. Parent element: BucketInfo.Bucket.AccessControlList.

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. Only the bucket owner can obtain CORS rules. Otherwise, OSS returns the 403 Forbidden message. Error code: AccessDenied.
3. The request can be initiated from any OSS endpoint.

Examples

Sample request:

```
Get /? bucketInfo HTTP/1.1
Host: BucketName.oss.example.com
Date: Sat, 12 Sep 2015 07:51:28 GMT
Authorization: OSS q***c: B***=
```

Sample response after the bucket information is obtained successfully:

```
HTTP/1.1 200
x-oss-request-id: 5***B
Date: Sat, 12 Sep 2015 07:51:28 GMT
Connection: keep-alive
Content-Length: 531
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<BucketInfo>
 <Bucket>
  <CreationDate>2013-07-31T10:56:21.000Z</CreationDate>
  <ExtranetEndpoint>regionid.example.com</ExtranetEndpoint>
  <IntranetEndpoint>regionid-internal.example.com</IntranetEndpoint>
  <Location>regionid</Location>
  <Name>oss-example</Name>
  <Owner>
   <DisplayName>***</DisplayName>
   <ID>2***3</ID>
  </Owner>
  <AccessControlList>
   <Grant>private</Grant>
  </AccessControlList>
 </Bucket>
</BucketInfo>
```

Sample response if the requested bucket information does not exist:

```
HTTP/1.1 404
x-oss-request-id: 5***B
Date: Sat, 12 Sep 2015 07:51:28 GMT
Connection: keep-alive
Content-Length: 308
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<Error>
 <Code>NoSuchBucket</Code>
 <Message>The specified bucket does not exist. </Message>
 <RequestId>5***4</RequestId>
 <HostId>nosuchbucket.oss.example.com</HostId>
 <BucketName>nosuchbucket</BucketName>
</Error>
```

Sample response if the requester has no access permission to the bucket information:

```
HTTP/1.1 403
x-oss-request-id: 5***C
Date: Sat, 12 Sep 2015 07:51:28 GMT
Connection: keep-alive
Content-Length: 209
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<Error>
 <Code>AccessDenied</Code>
 <Message>AccessDenied</Message>
 <RequestId>5***E</RequestId>
 <HostId>BucketName.oss.example.com</HostId>
</Error>
```

2.4.1.6.12. GetBucketLogging

You can call GetBucketLogging to view the access log configuration of a bucket.

Request syntax

```
GET /? logging HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Response elements

Response elements

Name	Description
BucketLoggingStatus	The container that stores the access log status information. Type: container. Child element: LoggingEnabled. Parent element: none.
LoggingEnabled	The container that stores the access log information. This element is required only when server access logging is enabled. Type: container. Child elements: TargetBucket and TargetPrefix. Parent element: BucketLoggingStatus.
TargetBucket	The bucket that stores access logs. Type: character. Child element: none. Parent element: BucketLoggingStatus.LoggingEnabled.
TargetPrefix	The name prefix of the object that stores access logs. Type: character. Child element: none. Parent element: BucketLoggingStatus.LoggingEnabled.

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. Only the owner of a bucket can view the access logging configuration of the bucket. If other users attempt to access the configuration, the error 403 Forbidden with the error code: AccessDenied is returned.
3. If no logging rules are set for the source bucket, OSS returns an XML message body with the element BucketLoggingStatus being null.

Examples

Sample request:

```
Get /? logging HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 04 May 2012 05:31:04 GMT
Authorization: OSS q***c:c***=
```

Sample response with logging rules configured:

```
HTTP/1.1 200
x-oss-request-id: 5***B
Date: Fri, 04 May 2012 05:31:04 GMT
Connection: keep-alive
Content-Length: 210
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<BucketLoggingStatus xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
  <LoggingEnabled>
    <TargetBucket>mybucketlogs</TargetBucket>
    <TargetPrefix>mybucket-access_log/</TargetPrefix>
  </LoggingEnabled>
</BucketLoggingStatus>
```

Sample response without logging rules configured:

```
HTTP/1.1 200
x-oss-request-id: 5***B
Date: Fri, 04 May 2012 05:31:04 GMT
Connection: keep-alive
Content-Length: 110
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<BucketLoggingStatus xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
</BucketLoggingStatus>
```

2.4.1.6.13. GetBucketWebsite

You can call GetBucketWebsite to view the static website hosting status of a bucket.

Request syntax

```
GET /? website HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Response elements

Response elements

Name	Description
ErrorDocument	The parent element of the child element Key. Type: container. Parent element: WebsiteConfiguration.
IndexDocument	The parent element of the child element Suffix. Type: container. Parent element: WebsiteConfiguration.
Key	The object name contained in the returned 404 Not Found message. Type: string. Parent element: WebsiteConfiguration.ErrorDocument. Conditional: This element is required only when ErrorDocument is set.
Suffix	The index file name added when a directory URL is returned. This element cannot be empty or contain a forward slash (/). For example, if the index file is set to index.html, regionid.example.com/mybucket/mydir/ contained in an access request is converted into regionid.example.com/mybucket/index.html by default. Type: string. Parent element: WebsiteConfiguration.IndexDocument.
WebsiteConfiguration	The container that holds the request. Type: container. Parent element: none.

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. Only the owner of a bucket can view the static website hosting status of the bucket. If other users attempt to access the status information, the 403 Forbidden error with the error code: AccessDenied is returned.
3. If the source bucket is not configured with static website hosting, OSS returns a 404 error with

the error code: NoSuchWebsiteConfiguration.

Examples

Sample request:

```
Get /? website HTTP/1.1
Host: BucketName.regionid.example.com
Date: Thu, 13 Sep 2012 07:51:28 GMT
Authorization: OSS q***c:B***=
```

Sample response with logging rules configured:

```
HTTP/1.1 200
x-oss-request-id: 5***B
Date: Thu, 13 Sep 2012 07:51:28 GMT
Connection: keep-alive
Content-Length: 218
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<WebsiteConfiguration xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
<IndexDocument>
<Suffix>index.html</Suffix>
  </IndexDocument>
  <ErrorDocument>
    <Key>error.html</Key>
  </ErrorDocument>
</WebsiteConfiguration>
```

Sample response without logging rules configured:

```
HTTP/1.1 404
x-oss-request-id: 5***B
Date: Thu, 13 Sep 2012 07:56:46 GMT
Connection: keep-alive
Content-Length: 308
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<Error xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
  <Code>NoSuchWebsiteConfiguration</Code>
  <Message>The specified bucket does not have a website configuration. </Message>
  <BucketName>oss-example</BucketName>
  <RequestId>5***F</RequestId>
  <HostId>BucketName.regionid.example.com</HostId>
</Error>
```

2.4.1.6.14. GetBucketReferer

You can call GetBucketReferer to view the referer configuration of a bucket.

Request syntax

```
GET /? referer HTTP/1.1
Host: BucketName.oss.example.com
Date: GMT Date
Authorization: SignatureValue
```

Response elements

Response elements

Name	Description
RefererConfiguration	The container that stores the referer configuration content. Type: container. Child elements: AllowEmptyReferer node and RefererList node. Parent element: none.

Name	Description
AllowEmptyReferer	Specifies whether the Referer field can be left unspecified in an access request. Type: enumeration. Valid values: true and false. Default value: true. Parent element: RefererConfiguration.
RefererList	The container that stores the referer access whitelist. Type: container. Parent element: RefererConfiguration. Child element: Referer.
Referer	The specified referer access whitelist. Type: string. Parent element: RefererList.

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. Only the owner of a bucket can view the referer configuration of the bucket. If other users attempt to access the configuration, the error 403 Forbidden with the error code: AccessDenied is returned.
3. If no referer configuration has been conducted for the bucket, OSS returns the default AllowEmptyReferer value and an empty RefererList.

Examples

Sample request:

```
Get /? referer HTTP/1.1
Host: BucketName.oss.example.com
Date: Thu, 13 Sep 2012 07:51:28 GMT
Authorization: OSS q***: B***=
```

Sample response with a referer rule configured for the bucket:

```
HTTP/1.1 200
x-oss-request-id: 5***B
Date: Thu, 13 Sep 2012 07:51:28 GMT
Connection: keep-alive
Content-Length: 218
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<RefererConfiguration>
<AllowEmptyReferer>true</AllowEmptyReferer >
  <RefererList>
    <Referer> http://www.aliyun.com</Referer>
    <Referer> https://www.aliyun.com</Referer>
    <Referer> http://www. *.com</Referer>
    <Referer> https://www.?.aliyuncs.com</Referer>
  </RefererList>
</RefererConfiguration>
```

Sample response without referer rules configured for the bucket:

```
HTTP/1.1 200
x-oss-request-id: 5***B
Date: Thu, 13 Sep 2012 07:56:46 GMT
Connection: keep-alive
Content-Length: 308
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<RefererConfiguration>
<AllowEmptyReferer>true</AllowEmptyReferer>
< RefererList />
</RefererConfiguration>
```

2.4.1.6.15. GetBucketLifecycle

You can call Get Bucket Lifecycle to view the lifecycle configuration of a bucket.

```
GET /? lifecycle HTTP/1.1
Host: BucketName.oss.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

1. Only the owner of a bucket can view the lifecycle configuration of the bucket. If other users attempt to access the configuration, the error 403 Forbidden with the error code: AccessDenied is returned.
2. If the bucket or lifecycle configuration does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket or NoSuchLifecycle.

Examples

Sample request:

```
Get /? lifecycle HTTP/1.1
Host: BucketName.oss.example.com
Date: Mon, 14 Apr 2014 01:17:29 GMT
Authorization: OSS q***:c***=
```

Sample response with bucket lifecycle configured:

```
HTTP/1.1 200
x-oss-request-id: 5***B
Date: Mon, 14 Apr 2014 01:17:29 GMT
Connection: keep-alive
Content-Length: 255
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<LifecycleConfiguration>
 <Rule>
  <ID>delete after one day</ID>
  <Prefix>logs/</Prefix>
  <Status>Enabled</Status>
  <Expiration>
   <Days>1</Days>
  </Expiration>
 </Rule>
</LifecycleConfiguration>
```

Sample response without bucket lifecycle configured:

```
HTTP/1.1 404
x-oss-request-id: 5***B
Date: Mon, 14 Apr 2014 01:17:29 GMT
Connection: keep-alive
Content-Length: 278
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<Error>
 <BucketName>oss-example</BucketName>
 <Code>NoSuchLifecycle</Code>
 <Message>No Row found in Lifecycle Table. </Message>
 <RequestId>5***9</RequestId>
 <HostId> BucketName.oss.example.com</HostId>
</Error>
```

2.4.1.6.16. GetBucketTagging

You can use GetBucketTagging to obtain all buckets that are associated with a specified bucket.

Request syntax

```
GET /? tagging HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Request elements

Request elements

Name	Description	Required
Tagging	The container for the bucket tag. Type: container. Child element: TagSet. Parent element: none.	Yes
TagSet	The container that stores a group of tags. Type: container. Child element: Tag. Parent element: Tagging.	Yes

Name	Description	Required
Tag	The container that stores a single tag. Type: container. Child element: Key or Value. Parent element: TagSet.	Yes
Key	The name of the tag. Type: string. Child element: none. Parent element: Tag.	Yes
Value	The value of the tag. Type: string. Child element: none. Parent element: Tag.	Yes

Detail analysis

1. If the requested bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. If the bucket is not associated with any tags, OSS returns an empty TagSet.

Examples

Sample request:

```
GET /? tagging HTTP/1.1
Host: ***.regionid.example.com
Date: Thu, 23 Jun 2015 15:39:15 GMT
Authorization: OSS q***:C***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 534B371674E88A4D8906008B
Date: Thu, 23 Jun 2015 15:39:15 GMT
Content-Length: 86
Content-Type: application/xml
Connection: close
Server: AliyunOSS
<? xml version="1.0" ? >
<Tagging>
 <TagSet>
 <Tag>
 <Key>Project</Key>
 <Value>Project One</Value>
 </Tag>
 <Tag>
 <Key>User</Key>
 <Value>jsmith</Value>
 </Tag>
 </TagSet>
</Tagging>
```

2.4.1.6.17. DeleteBucket

You can call DeleteBucket to delete a bucket.

Request syntax

```
DELETE / HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. To prevent unexpected deletion, OSS does not allow the bucket owner to delete a non-empty bucket.
3. If you try to delete a non-empty bucket, the error 409 Conflict with the error code: BucketNotEmpty is returned.
4. Only the bucket owner has the permission to delete the bucket. If you try to delete a bucket you have no permission on, the error 403 Forbidden is returned. Error code: AccessDenied.

Examples

Sample request:

```
DELETE / HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 05:31:04 GMT
Authorization: OSS q***:c***=
```

Sample response:

```
HTTP/1.1 204 No Content
x-oss-request-id: 534B371674E88A4D8906008B
Date: Fri, 24 Feb 2012 05:31:04 GMT
Connection: keep-alive
Content-Length: 0
Server: AliyunOSS
```

2.4.1.6.18. DeleteBucketLogging

You can call DeleteBucketLogging to disable access logging of a bucket.

Request syntax

```
DELETE /? logging HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. Only the bucket owner can disable access logging for the bucket. If you try to operate a bucket that does not belong to you, OSS returns the 403 Forbidden message. Error code: AccessDenied.
3. If access logging is not enabled for the target bucket, HTTP status code 204 is returned.

Examples

Sample request:

```
DELETE /? logging HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 05:35:24 GMT
Authorization: OSS q***c:6***=
```

Sample response:

```
HTTP/1.1 204 No Content
x-oss-request-id: 5***B
Date: Fri, 24 Feb 2012 05:35:24 GMT
Connection: keep-alive
Content-Length: 0
Server: AliyunOSS
```

2.4.1.6.19. DeleteBucketWebsite

You can call DeleteBucketWebsite to disable static website hosting of a bucket.

Request syntax

```
DELETE /? website HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. Only the bucket owner can disable the static website hosting mode for a bucket. If you try to operate a bucket that does not belong to you, OSS returns the 403 Forbidden message. Error code: AccessDenied.

Examples

Sample request:

```
DELETE /? website HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 05:45:34 GMT
Authorization: OSS q***:L***=
```

Sample response:

```
HTTP/1.1 204 No Content
x-oss-request-id: 5***B
Date: Fri, 24 Feb 2012 05:45:34 GMT
Connection: keep-alive
Content-Length: 0
Server: AliyunOSS
```

2.4.1.6.20. DeleteBucketLifecycle

You can call DeleteBucketLifecycle to delete the lifecycle configuration of a specified bucket.

Request syntax

```
DELETE /? lifecycle HTTP/1.1
Host: BucketName.oss.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

1. This operation is used to delete all lifecycle rules of a specified bucket. After that, no objects are automatically deleted in this bucket.
2. If the bucket or lifecycle configuration does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket or NoSuchLifecycle.
3. Only the bucket owner can delete the lifecycle configuration of a bucket. If you try to operate a bucket that does not belong to you, OSS returns the 403 Forbidden message. Error code: AccessDenied.

Examples

Sample request:

```
DELETE /? lifecycle HTTP/1.1
Host: BucketName.oss.example.com
Date: Mon, 14 Apr 2014 01:17:35 GMT
Authorization: OSS q***:6***=
```

Sample response:

```
HTTP/1.1 204 No Content
x-oss-request-id: 5***B
Date: Mon, 14 Apr 2014 01:17:35 GMT
Connection: keep-alive
Content-Length: 0
Server: AliyunOSS
```

2.4.1.6.21. DeleteBucketTagging

You can call DeleteBucketTagging to delete all tags associated with a bucket.

Request syntax

```
DELETE /? tagging HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. If the bucket is not associated with any tags, OSS returns the 204 No Content message.

Examples

Sample request:

```
DELETE /? tagging HTTP/1.1
Host: ***.regionid.example.com
Date: Thu, 23 Jun 2015 15:39:18 GMT
Authorization: OSS q***c:C***=
```

Sample response:

```
HTTP/1.1 204 No Content
x-oss-request-id: 5***B
Date: Thu, 23 Jun 2015 15:39:18 GMT
Connection: close
Content-Length: 0
Server: AliyunOSS
```

2.4.1.6.22. ListBucketByTagging

ListBucketByTagging is not opened as an independent API. Instead, it is implemented by adding two parameters tag-key and tag-value to the GetService API. Based on the specified tag-key and tag-value, OSS lists the matching buckets. The following table describes the parameters that are added.

Query parameters

Name	Description
tag-key	The tag that the returned buckets must contain. This parameter can be left unspecified, which indicates that buckets will not be filtered based on the tag. Type: string. Default value: none.

Name	Description
tag-value	The tag that the returned buckets must contain. This parameter must be used alongside tag-key. This parameter can be left unspecified, which indicates that buckets will not be filtered based on the tag. Type: string. Default value: none.

Examples

Suppose that test_user has three buckets: bucket 1, bucket 2, and bucket 3. Bucket 1 and bucket 2 have the tag key1:value1 and bucket 3 has the tag key3:value3. The following example lists the buckets with tag-key=key1 and tag-value=value1 as required:

Sample request:

```
GET /tag-key=key1&tag-value=value1 HTTP/1.1
Date: Fri, 15 May 2015 11:18:32 GMT
Host: 10.97.188.37
Authorization: OSS n***:C***=
```

Sample response:

```
HTTP/1.1 200 OK
Date: Fri, 15 May 2015 11:18:32 GMT
Content-Type: application/xml
Content-Length: 156
Connection: close
Server: AliyunOSS
x-oss-request-id: 5***4
<? xml version="1.0" encoding="UTF-8"? >
<ListAllMyBucketsResult>
 <Owner>
 <ID>***</ID>
 <DisplayName>***</DisplayName>
 </Owner>
 <Buckets>
 <Bucket>
 <Location>oss-cn-hangzhou</Location>
 <Name>bucket1</Name>
 <CreationDate>2015-05-15T11:18:32.000Z</CreationDate>
 </Bucket>
 <Bucket>
 <Location>oss-cn-hangzhou</Location>
 <Name>bucket2</Name>
 <CreationDate>2015-05-15T11:18:32.000Z</CreationDate>
 </Bucket>
 </Buckets>
</ListAllMyBucketsResult>
```

2.4.1.7. Object-relevant operations

2.4.1.7.1. PutObject

You can call PutObject to upload objects.

Request syntax

```
PUT /ObjectName HTTP/1.1
Content-Length: ContentLength
Content-Type: ContentType
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Request header

Request header

Name	Description
Cache-Control	Specifies the Web page caching behavior when the object is downloaded. For more information, see RFC2616. Type: string. Default value: none.
Content-Disposition	Specifies the name of the object when the object is downloaded. For more information, see RFC2616. Type: string. Default value: none.
Content-Encoding	Specifies the content encoding format when the object is downloaded. For more information, see RFC2616. Type: string. Default value: none.
Content-MD5	As defined in RFC 1864, the message content (excluding the header) is calculated to obtain an MD5 value, which is a 128-bit number. Then, this number is Base64-encoded into a Content-MD5 value. This request header field can be used to check the validity of a message, that is, whether the message content is consistent with the sent content. Although this request header field is optional, we recommend that you use it for end-to-end checks. Type: string. Default value: none. Restriction: none.
Expires	Specifies the expiration time. For more information, see RFC2616. Type: string. Default value: none. Note OSS does not limit or verify this value.

Name	Description
x-oss-server-side-encryption	The encryption algorithm that OSS uses to encrypt an object when the object is created. Type: string. Valid values: AES256 and KMS. Note You must purchase and enable Key Management Service (KMS) to use the KMS encryption algorithm. Otherwise, OSS returns the KmsServiceNotEnabled error code.
x-oss-object-acl	The access permission granted by OSS for an object when the object is created. Type: string. Valid values: public-read, private, and public-read-write.

Detail analysis

1. If the Content-MD5 field value is specified in the request header, OSS calculates the Content-MD5 field value in the request body and checks whether the two values are the same. If they are different, OSS returns the InvalidDigest error.
2. If the Content-Length value in the request header is smaller than the length of data transmitted in the actual request body, OSS still creates a file, but the object size is equal to the size defined by Content-Length, and the remaining data is dropped.
3. If a file of the same name with the object to be added already exists, and you are authorized to access this object, the new object overwrites the existing object, and OSS returns the 200 OK message.
4. If the PutObject request carries a parameter prefixed with x-oss-meta-, the parameter is treated as user meta, such as x-oss-meta-location. An object may have multiple similar parameters, but the total size of the user-defined Object Meta cannot exceed 8 KB.
5. If the Content length parameter is not added to the header, the system returns the 411 Length Required error. Error code: MissingContentLength.
6. If the length is set, but the message body is not sent, or the size of the sent body is smaller than the specified size, the server waits until the timeout occurs, and then returns the 400 Bad Request message. Error code: RequestTimeout.
7. If the bucket of the object to be added does not exist, the system returns the 404 Not Found error. Error code: NoSuchBucket.
8. If you have no permission to access the bucket of the object to be added, the system returns the 403 Forbidden error. Error code: AccessDenied.
9. If the length of the added object exceeds 5 GB, OSS returns the 400 Bad Request message. Error code: InvalidArgument.
10. If the length of the input object key exceeds 1,023 bytes, the system returns the 400 Bad Request message. Error code: InvalidObjectName

11. When you put an object, OSS supports the following five header fields defined in RFC2616: Cache-Control, Expires, Content-Encoding, Content-Disposition, and Content-Type. If these headers are set when you upload an object, the corresponding header values are automatically set to the uploaded values next time this object is downloaded.
12. If the x-oss-server-side-encryption header is specified when you upload an object, the value of this header must be set to AES256. Otherwise, the system returns the 400 error and the error code: InvalidEncryptionAlgorithmError. If this parameter is specified in the request header, the response header also contains this parameter, and OSS stores the uploaded object after encryption. When this object is downloaded, the response header contains x-oss-server-side-encryption, the value of which is set to the encryption algorithm of this object.

FAQs

Content-MD5 calculation method error

For example, if the content to be uploaded is "123456789", the Content-MD5 value of the string is calculated based on the algorithm defined in relevant standards as follows: 1. Calculate the MD5-encrypted 128-bit binary array. 2. Encode the binary array (but not the 32-bit string code) with Base64. Python is used as an example. The correct code for the calculation is as follows:

```
>>> import base64,hashlib
>>> hash = hashlib.md5()
>>> hash.update("0123456789")
>>> base64.b64encode(hash.digest())
'eB5eJF1ptWaXm4bijSPyxw=='
```

A correct example is to use the `hash.digest()` method to calculate a 128-bit binary array: `>>> hash.digest() 'x\x1e^$]i\xb5f\x97\x9b\x86\xe2\x8d#\xf2\xc7'`. A common incorrect operation is to encode the calculated 32-bit string code with Base64. An incorrect example is to use the `hash.hexdigest()` method to calculate a visible 32-bit string code: `>>> hash.hexdigest() '781e5e245d69b566979b86e28d23f2c7'`. If an incorrect MD5 value is Base64-encoded, the result is: `>>> base64.b64encode(hash.hexdigest()) 'NzgxZTVlMjQ1ZDY5YjU2Njk3OWI4NmUyOGQyM2YyYzc='`.

Examples

Sample request:

```
PUT /oss.jpg HTTP/1.1
Host: ***.regionid.example.com
Cache-control: no-cache
Expires: Fri, 28 Feb 2012 05:38:42 GMT
Content-Encoding: utf-8
Content-Disposition: attachment;filename=oss_download.jpg
Date: Fri, 24 Feb 2012 06:03:28 GMT
Content-Type: image/jpg
Content-Length: 344606
Authorization: OSS q***:k***=

[344606 bytes of object data]
```

Sample response:

```
HTTP/1.1 200 OK
Server: AliyunOSS
Date: Sat, 21 Nov 2015 18:52:34 GMT
Content-Length: 0
Connection: keep-alive
x-oss-request-id: 5***A
x-oss-bucket-version: 1***9
ETag: "A***2"
```

2.4.1.7.2. GetObject

You can call GetObject to obtain an object. You must have read permissions before you use Get Object.

Request syntax

```
GET /ObjectName HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
Range: bytes=ByteRange (Optional)
```

Request parameters

OSS allows you to customize some headers in the OSS response request when you send a GET request, on the premise that the GET request you send must carry a signature. These headers include:

Request parameters

Name	Description
response-content-type	The content-type header in the response returned by OSS. Type: string. Default value: none.
response-content-language	The content-language header in the response returned by OSS. Type: string. Default value: none.
response-expires	The expires header in the response returned by OSS. Type: string. Default value: none.
response-cache-control	The cache-control header in the response returned by OSS. Type: string. Default value: none.
Response-content-Disposition	The content-disposition header in the response returned by OSS. Type: string. Default value: none.
response-content-encoding	The content-encoding header in the response returned by OSS. Type: string. Default value: none.

Request header

Request header

Name	Description
Range	The transmission range of an object. For example, if this parameter is set to bytes=0-9, OSS transfers byte 0 to byte 9. Type: string. Default value: none.

Name	Description
If-Modified-Since	The object transfer condition. If the specified time is earlier than the actual object modification time, OSS transfers the object and returns the 200 OK message. Otherwise, OSS returns the 304 Not Modified message. Type: string. Default value: none. Time format: GMT, for example: Fri, 13 Nov 2015 14:47:53 GMT.
If-Unmodified-Since	The object transfer condition. If the specified time is equal to or later than the actual object modification time, OSS transfers the object and returns the 200 OK message. Otherwise, OSS returns the 412 Precondition Failed message. Type: string. Default value: none. Time format: GMT, for example: Fri, 13 Nov 2015 14:47:53 GMT.
If-Match	The object transfer condition. If the ETag value of the source object is equal to the ETag value specified in the request, OSS transfers the object and returns the 200 OK message. Otherwise, OSS returns the 412 Precondition Failed message. Type: string. Default value: none.
If-None-Match	The object transfer condition. If the ETag value of the source object is not equal to the ETag value specified in the request, OSS transfers the object and returns the 200 OK message. Otherwise, OSS returns the 304 Not Modified message. Type: string. Default value: none.

Detail analysis

1. The Range parameter in the GetObject request can be set to support resumable data transmission. We recommend that you use this function if the object size is large.
2. If the Range parameter is used in the request header, the returned message includes the length of the entire file and the range returned for the request. For example, if the returned message is Content-Range: bytes 0-9/44, the length of the entire object is 44, and the range returned is 0 to 9. If the range requirement is not met, the system transfers the entire file and does not include Content-Range in the result.
3. If the time specified by If-Modified-Since does not conform to the time format, OSS returns the object and the 200 OK message.
4. If-Modified-Since and If-Unmodified-Since can coexist. If-Match and If-None-Match can also coexist.
5. If a request does not meet the condition specified by If-Unmodified-Since or If-Match, OSS returns the 412 Precondition.
6. If a request does not meet the condition specified by If-Modified-Since or If-None-Match, OSS returns the 304 Not Modified message.

7. If the object does not exist, OSS returns the 404 Not Found message. Error code: NoSuchKey.
8. OSS does not allow you to customize the headers in OSS returned request by using request parameters in the GET request during anonymous access.
9. When you customize some headers in OSS returned request, OSS sets these headers to the values specified by parameters in the GET Object Request only when the request is successfully processed (when the system returns the 200 OK message).
10. If this object is encrypted with entropy on the server side, the system automatically returns the decrypted object on receiving the GetObject request, and returns x-oss-server-side-encryption in the response header. The value of x-oss-server-side-encryption indicates the server-side encryption algorithm of the object.
11. If you want to compress and transfer the returned content using GZIP, add Accept-Encoding:gzip to the display mode in the request header. OSS determines whether to return the data compressed by GZIP to you based on the Content-Type and size of the file. If the content is compressed using GZIP, the content does not contain the ETag. Currently, OSS supports GZIP compression for the following Content-Types: HTML, Javascript, CSS, XML, RSS, and JSON. The object size must be at least 1 KB.
12. If the object type is symbolic link, the content of the target object is returned. In the response header, `Content-Length` , `ETag` , and `Content-Md5` are Object Meta of the target object. `La st-Modified` is the maximum value of the target object and symbolic link. Others are Object Meta of symbolic links.
13. If the object type is symbolic link, and the target object does not exist, the system returns Error 404 Not Found. Error code: SymlinkTargetNotExist.
14. If the object type is symbolic link, and the target object type is symbolic link, the system returns Error 400 Bad request. Error code: InvalidTargetType.

Examples

Sample request:

```
GET /oss.jpg HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 06:38:30 GMT
Authorization: OSS q***:U***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 3***1
x-oss-object-type: Normal
Date: Fri, 24 Feb 2012 06:38:30 GMT
Last-Modified: Fri, 24 Feb 2012 06:07:48 GMT
ETag: "5***E "
Content-Type: image/jpg
Content-Length: 344606
Server: AliyunOSS
[344606 bytes of object data]
```

Sample request with range specified:

```
GET /oss.jpg HTTP/1.1
Host:***. regionid.example.com
Date: Fri, 28 Feb 2012 05:38:42 GMT
Range: bytes=100-900
Authorization: OSS q***:q***=
```

Sample response:

```
HTTP/1.1 206 Partial Content
x-oss-request-id: 2***9
x-oss-object-type: Normal
Date: Fri, 28 Feb 2012 05:38:42 GMT
Last-Modified: Fri, 24 Feb 2012 06:07:48 GMT
ETag: "5***E "
Accept-Ranges: bytes
Content-Range: bytes 100-900/344606
Content-Type: image/jpg
Content-Length: 801
Server: AliyunOSS
[801 bytes of object data]
```

Sample request with the returned message header customized:

```
GET /oss.jpg? response-expires=Thu%2C%2001%20Feb%202012%2017%3A00%3A00%20GMT& response-co
ntent-type=text&response-cache-control=No-cache&response-content-disposition=attachment%253B%
2520filename%253Dtesting.txt&response-content-encoding=utf-8&response-content-language=%E4%B8
%AD%E6%96%87 HTTP/1.1
Host: ***.regionid.example.com:
Date: Fri, 24 Feb 2012 06:09:48 GMT
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***1
x-oss-object-type: Normal
Date: Fri, 24 Feb 2012 06:09:48 GMT
Last-Modified: Fri, 24 Feb 2012 06:07:48 GMT
ETag: "5***E "
Content-Length: 344606
Connection: keep-alive
Content-disposition: attachment; filename:testing.txt
Content-language: Chinese
Content-encoding: utf-8
Content-type: text
Cache-control: no-cache
Expires: Fri, 24 Feb 2012 17:00:00 GMT
Server: AliyunOSS
[344606 bytes of object data]
```

Sample request of symbolic link:

```
GET /link-to-oss.jpg HTTP/1.1
Accept-Encoding: identity
Date: Tue, 08 Nov 2016 03:17:58 GMT
Host: ***.regionid.example.com
Authorization: OSS q***:q***=
```

Sample response:

```
HTTP/1.1 200 OK
Server: AliyunOSS
Date: Tue, 08 Nov 2016 03:17:58 GMT
Content-Type: application/octet-stream
Content-Length: 20
Connection: keep-alive
x-oss-request-id: 5***D
Accept-Ranges: bytes
ETag: "8***7"
Last-Modified: Tue, 08 Nov 2016 03:17:58 GMT
x-oss-object-type: Symlink
Content-MD5: g***w==
```

2.4.1.7.3. CopyObject

To copy an existing object in the OSS into another object, you can send a PUT request into the OSS, and add the element x-oss-copy-source to the PUT request header to specify the copy source. The OSS automatically determines that this is a copy operation, and directly performs this operation on the server side. If the copy operation is successful, the system returns the information of the new object to you. You can call CopyObject to copy objects smaller than 1 GB. To copy an object larger than 1 GB, you must use MultipartUpload. For more information, see UploadPartCopy.

Request syntax

```
PUT /DestObjectName HTTP/1.1
Host: DestBucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
x-oss-copy-source: /SourceBucketName/SourceObjectName
```

Request header

Request header

Name	Description
x-oss-copy-source	The source IP address for object copy. The requester must have the permission to read the source object. Type: string. Default value: none.

Name	Description
x-oss-copy-source-if-match	The object copy condition. If the ETag value of the source object is equal to the ETag value specified in the request, OSS copies the object and returns the 200 OK message. Otherwise, OSS returns the 412 Precondition Failed message. Type: string. Default value: none.
x-oss-copy-source-if-none-match	The object copy condition. If the ETag value of the source object is not equal to the ETag value specified in the request, OSS copies the object and returns the 200 OK message. Otherwise, OSS returns the 304 Not Modified message. Type: string. Default value: none.
x-oss-copy-source-if-unmodified-since	The object copy condition. If the specified time is equal to or later than the actual object modification time, OSS transfers the object and returns the 200 OK message. Otherwise, OSS returns the 412 Precondition Failed message. Type: string. Default value: none.
x-oss-copy-source-if-modified-since	The object copy condition. If the source object has been modified since the time specified in the request, OSS copies the object. Otherwise, OSS returns the 304 Not Modified error. Type: string. Default value: none.
x-oss-metadata-directive	Valid values include COPY and REPLACE. If this parameter is set to COPY, the system copies meta for the new object from the source object. If this parameter is set to REPLACE, the system ignores all meta values of the source object, and uses the meta value specified in this request. If this parameter is set to a value other than COPY and REPLACE, the system returns the 400 Bad Request message. Note that when the value is COPY, the source object's x-oss-server-side-encryption meta value cannot be copied. Type: string. Default value: COPY. Valid values: COPY and REPLACE.
x-oss-server-side-encryption	The entropy coding-based encryption algorithm that OSS uses to encrypt a new object when creating it. Type: string. Valid values: AES256 and KMS. Note You must purchase and enable Key Management Service (KMS) to use the KMS encryption algorithm. Otherwise, OSS returns the KmsServiceNotEnabled error code.

Name	Description
x-oss-object-acl	The access permission granted by OSS for an object when the object is created. Type: string. Valid values: public-read, private, and public-read-write.

Response elements

Response elements

Name	Description
CopyObjectResult	The result of CopyObject. Type: string. Default value: none.
ETag	The ETag value of the new object. Type: string. Parent element: CopyObjectResult.
LastModified	The last update time of the new object. Type: string. Parent element: CopyObjectResult.

Detail analysis

1. You can use the Copy Object operation to modify the meta information of an existing object.
2. If the source object URL is the same as the target object URL in the Copy Object operation, the system directly replaces the meta information in the source object regardless of the value of x-oss-metadata-directive.
3. The OSS allows the Copy Object request to contain any number of the four pre-judgment headers. For more information about the related logic, see Detail Analysis of Get Object.
4. To complete a Copy Object operation, the requester must have the permission to read the source object.
5. The source object and the target object must belong to the same region. Otherwise, the system returns the error code 403 AccessDenied. The error message is Target object does not reside in the same data center as source object.
6. In the billing statistics of the Copy Object operation, the number of Get requests increases by 1 in the bucket of the source object, the number of Put requests increases by 1 in the bucket of the target object, and a storage space is added accordingly.
7. In the Copy Object operation, all relevant request headers start from x-oss-, and therefore must be added to the signature string.
8. If the x-oss-server-side-encryption header is specified in the Copy Object request, and its value (AES256) is valid, the target object is encrypted on the server side after the Copy Object operation is performed no matter whether the source object has been encrypted on the server side. In addition, the Copy Object response header contains x-oss-server-side-encryption, the value of which is set to the encryption algorithm of the target object. When this target object is downloaded, the response header also contains x-oss-server-side-encryption, the value of which is set to the encryption algorithm of this target object. If the x-oss-server-side-encryption request header is not specified in the Copy Object operation, the target object is the data that is not encrypted on the server side even if the source object has been encrypted on the server side.

9. When receiving a CopyObject request in which the x-oss-metadata-directive header field is set to COPY (default value), OSS does not copy the x-oss-server-side-encryption value of the source object. Instead, OSS checks whether the x-oss-server-side-encryption header field is specified in the request and determines whether to encrypt the new object accordingly.
10. When the x-oss-server-side-encryption request header is specified in the COPY operation, and the request value is not AES256, the system returns Error 400 with the error code InvalidEncryptionAlgorithmError.
11. If the size of the file to be copied is larger than 1 GB, the system returns Error 400 with the error code EntityTooLarge.
12. CopyObject cannot be used to copy the objects created by using AppendObject.
13. If the object type is symbolic link, copy the symbolic link only.

Examples

Sample request:

```
PUT /copy_oss.jpg HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 07:18:48 GMT
x-oss-copy-source: /oss-example/oss.jpg
Authorization: OSS q***:g***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***1
Content-Type: application/xml
Content-Length: 193
Connection: keep-alive
Date: Fri, 24 Feb 2012 07:18:48 GMT
Server: AliyunOSS
<? xml version="1.0" encoding="UTF-8"? >
<CopyObjectResult xmlns="http://doc.oss-cn-hangzhou.aliyuncs.com">
 <LastModified>Fri, 24 Feb 2012 07:18:48 GMT</LastModified>
 <ETag>"5***E"</ETag>
</CopyObjectResult>
```

2.4.1.7.4. AppendObject

You can call AppendObject to upload an object by appending the object to an existing object. An object created through AppendObject is an appendable object. An object uploaded through PutObject is a normal object.

Request syntax

```
POST /ObjectName? append&position=Position HTTP/1.1
Content-Length: ContentLength
Content-Type: ContentType
Host: BucketName.oss.example.com
Date: GMT Date
Authorization: SignatureValue
```

Request header

Request header

Name	Description
Cache-Control	The Webpage caching behavior when the object is downloaded. For more information, see RFC2616. Type: string. Default value: none.
Content-Disposition	The name of the object when the object is downloaded. For more information, see RFC2616. Type: string. Default value: none.
Content-Encoding	The content encoding format when the object is downloaded. For more information, see RFC2616. Type: string. Default value: none.
Content-MD5	As defined in RFC 1864, the message content (excluding the header) is calculated to obtain an MD5 value, which is a 128-bit number. Then, this number is Base64-encoded into a Content-MD5 value. This request header field can be used to check the validity of a message, that is, whether the message content is consistent with the sent content. Although this request header field is optional, we recommend that you use it for end-to-end checks. Type: string. Default value: none. Restriction: none.
Expires	The expiration time. For more information, see RFC2616. Type: integer. Default value: none.

Name	Description
x-oss-server-side-encryption	The encryption algorithm that OSS uses to encrypt an object when the object is created. Type: string. Valid values: AES256 and KMS. Note You must purchase and enable Key Management Service (KMS) to use the KMS encryption algorithm. Otherwise, OSS returns the KmsServiceNotEnabled error code.
x-oss-object-acl	The access permission granted by OSS for an object when the object is created. Type: string. Valid values: public-read, private, and public-read-write.

Response header

Response header

Name	Description
x-oss-next-append-position	The position that must be provided in the next request. It indicates the current object length. This header is contained when a successful message is returned for Append Object, or when a 409 error occurs because of the mismatch between the position and the object length. Type: 64-bit integer.
x-oss-hash-crc64ecma	The 64-bit CRC value of the object. This value is calculated based on the ECMA-182 standard. Type: 64-bit integer.

Association with other operations

1. The Append Object method is not applicable to a non-appendable object. For example, if a normal object with the same name already exists and the Append Object method is still called, OSS returns a 409 error with an error code of ObjectNotAppendable.
2. If you perform the Put Object operation on an existing appendable object, this appendable object is overwritten by the new object and the object type is changed to normal object.
3. After the Head Object operation is performed, OSS returns x-oss-object-type. If the object is an appendable object, the object type is Appendable. For an appendable object, after the Head Object operation is performed, the system also returns x-oss-next-append-position and x-oss-hash-crc64ecma.
4. In the response XML of the Get Bucket (List Objects) request, the type of an appendable object is set to Appendable.
5. You can neither use Copy Object to copy an appendable object nor change the server-side encryption attribute of this object. You can use Copy Object to modify the user-defined Object

Meta of this object.

Detail analysis

1. The two URL parameters, append and position, are CanonicalizedResource, and must be included in the signature.
2. URL parameters must also include append, which specifies that the operation is AppendObject.
3. URL query parameters must include position, which specifies the position from which the append of the object starts. The value of position in the first AppendObject operation must be 0. The value of position in the subsequent operation is the current object length. For example, if the value of position specified in the first Append Object request is 0, and the value of content-length is 65536, the value of position specified in the second Append Object request must be set to 65536. After each operation succeeds, x-oss-next-append-position in the response header also specifies the position of the next Appendix Object request.
4. If the position value is different from the current object length, the OSS returns the 409 message and the error code PositionNotEqualToLength. If the preceding error occurs, you can obtain the position for the next AppendObject request from x-oss-next-append-position in the response header, and send an AppendObject request again.
5. If the position value is 0 and an appendable object with the same name does not exist, or if the length of an appendable object with the same name is 0, the Append Object operation succeeds. Otherwise, the system regards that the position and object length mismatch.
6. If the position value is 0 and an object with the same name does not exist, headers (such as x-oss-server-side-encryption) can be set in the Append Object request like the Put Object request. This is the same as the case of Initiate Multipart Upload. If the position value is 0, and the correct x-oss-server-side-encryption header is added to the request, the header of the response to the subsequent Append Object request also contains x-oss-server-side-encryption, which indicates the encryption algorithm. Later, if meta must be modified, you can use the Copy Object request.
7. Taking the concurrency into consideration, even if you set the value of position to x-oss-next-append-position, you may fail to append the object owing to PositionNotEqualToLength.
8. The length limit of an object generated by AppendObject is the same as that of an object generated by PutObject.
9. Each time after an AppendObject operation is performed, the last modification time of this object is updated.
10. If the position value is correct and the content with a length of 0 is appended to an existing appendable object, the status of the object does not change.

CRC64-based calculation method

The CRC value of an appendable object is calculated based on the ECMA-182 standard. The calculation method is the same as that of XZ. CRC64 can be calculated using the boost CRC module as follows:

```
typedef boost::crc_optimal<64, 0x42F0E1EBA9EA3693ULL, 0xffffffffffffffffULL, 0xffffffffffffffffULL, true, t
rue> boost_ecma;

uint64_t do_boost_crc(const char* buffer, int length)
{
   boost_ecma crc;
   crc.process_bytes(buffer, length);
   return crc.checksum();
}
```

Alternatively, CRC64 can be calculated using the Python crcmod based on the following formula:

```
do_crc64 = crcmod.mkCrcFun(0x142F0E1EBA9EA3693L, initCrc=0L, xorOut=0xffffffffffffffffL, rev=True)

print do_crc64( “123456789” )
```

Examples

Sample request:

```
POST /oss.jpg? append&position=0 HTTP/1.1
Host: BucketName.oss.example.com
Cache-control: no-cache
Expires: Wed, 08 Jul 2015 16:57:01 GMT
Content-Encoding: utf-8
Content-Disposition: attachment;filename=oss_download.jpg
Date: Wed, 08 Jul 2015 06:57:01 GMT
Content-Type: image/jpg
Content-Length: 1717
Authorization: OSS q***:k***=

[1717 bytes of object data]
```

Sample response:

```
HTTP/1.1 200 OK
Date: Wed, 08 Jul 2015 06:57:01 GMT
ETag: "0***0"
Connection: keep-alive
Content-Length: 0
Server: AliyunOSS
x-oss-hash-crc64ecma: 14741617095266562575
x-oss-next-append-position: 1717
x-oss-request-id: 5***1
```

2.4.1.7.5. DeleteObject

You can call DeleteObject to delete an object.

Request syntax

```
DELETE /ObjectName HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

1. To delete an object with Delete Object, you must have the write permission to this object.
2. If the object to be deleted does not exist, OSS returns the 204 No Content status code.
3. If the bucket of the object does not exist, the system returns the 404 Not Found message.
4. If the object type is symbolic link, only the symbolic link is deleted.

Examples

Sample request:

```
DELETE /copy_oss.jpg HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 07:45:28 GMT
Authorization: OSS q***:z***=
```

Sample response:

```
HTTP/1.1 204 NoContent
x-oss-request-id: 5***1
Date: Fri, 24 Feb 2012 07:45:28 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.7.6. DeleteMultipleObjects

You can call DeleteMultipleObjects to delete multiple objects in the same bucket with one HTTP request. You can use the DeleteMultipleObjects operation to delete up to 1,000 objects with one request. Two response modes are available: Verbose and Quiet.

- Verbose mode: The message body returned by OSS contains the result of each deleted object.
- Quiet mode: The message body returned by OSS only contains the results for objects which encountered an error in the DELETE process. If all objects are successfully deleted, no message body is returned.

Request syntax

```
POST /? delete HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Content-Length: ContentLength
Content-MD5: MD5Value
Authorization: SignatureValue

<? xml version="1.0" encoding="UTF-8"? >
<Delete>
 <Quiet>true</Quiet>
 <Object>
  <Key>key</Key>
 </Object>
...
</Delete>
```

Request parameters

During the DeleteMultipleObjects operation, you can use the encoding-type parameter to encode the key in the response.

Request parameters

Name	Description

Name	Description
encoding-type	The encoding type of the key in the response. Currently, URL encoding is supported. The Key is UTF-8-encoded, but the XML 1.0 Standard does not support parsing certain control characters, such as the characters with ASCII values from 0 to 10. If the key contains control characters not supported by the XML 1.0 Standard, you can set the encoding-type parameter to encode the returned Key. Type: string. Default value: none. Valid value: url.

Request elements

Request elements

Name	Description
Delete	The container that stores the DeleteMultipleObjects request. Type: container. Child element: one or more object elements and the optional quiet element. Parent element: none.
Key	The name of the object you want to delete. Type: string. Parent element: Object.
Object	The container that stores the information about the object. Type: container. Child element: key Parent element: Delete.
Quiet	The switch that enables the Quiet response mode. Type: enumeration. Valid values: true and false. Default value: false. Parent element: Delete.

Response elements

Response elements

Name	Description

Name	Description
Deleted	The container that stores the successfully deleted object. Type: container. Child element: key. Parent element: DeleteResult.
DeleteResult	The container that stores the response of the DeleteMultipleObjects request. Type: container. Child element: Deleted. Parent element: none.
Key	The name of the object on which OSS performs the Delete operation. Type: string. Parent element: Delete.
EncodingType	The encoding type of the key in the response. If the encoding-type parameter is specified in the request, the key is encoded in the response. Type: string. Parent element: container.

Detail analysis

1. The Content-Length and Content-MD5 fields must be specified in the Delete Multiple Objects request. OSS verifies that the received message body is correct based on the two fields before the Delete operation is performed.
2. Method to generate the Content-MD5 field: Encrypt the MD5 value of the Delete Multiple Objects request to obtain a 128-byte array, and encode the array using Base64. The final string obtained is the content of the Content-MD5 field.
3. The return mode of the Delete Multiple Objects request is Verbose by default.
4. If the Delete Multiple Objects request is used to delete a non-existing object, the operation is still regarded as successful.
5. The Delete Multiple Objects request can contain a message body of up to 2 MB. If the size of the message body exceeds 2 MB, the system returns the MalformedXML error code.
6. The Delete Multiple Objects request can be used to delete up to 1,000 objects at a time. If the number of objects to be deleted at a time exceeds 1,000, the system returns the MalformedXML error code.
7. If the Content-MD5 field value is specified in the request header, OSS calculates the Content-MD5 field value in the request body and checks whether the two values are the same. If they are different, OSS returns the InvalidDigest error.

Examples

Sample request I:

```
POST /? delete HTTP/1.1
Host: ***.regionid.example.com
Date: Wed, 29 Feb 2012 12:26:16 GMT
Content-Length:151
Content-MD5: o***==
Authorization: OSS q***:+z***=

<? xml version="1.0" encoding="UTF-8"? >

<Delete>
 <Quiet>false</Quiet>
 <Object>
  <Key>multipart.data</Key>
 </Object>
 <Object>
  <Key>test.jpg</Key>
 </Object>
 <Object>
  <Key>demo.jpg</Key>
 </Object>
</Delete>
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 7***7
Date: Wed, 29 Feb 2012 12:26:16 GMT
Content-Length: 244
Content-Type: application/xml
Connection: keep-alive
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<DeleteResult xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
  <Deleted>
    <Key>multipart.data</Key>
  </Deleted>
  <Deleted>
    <Key>test.jpg</Key>
  </Deleted>
  <Deleted>
    <Key>demo.jpg</Key>
  </Deleted>
</DeleteResult>
```

Sample request II:

```
POST /? delete HTTP/1.1
Host: ***.regionid.example.com
Date: Wed, 29 Feb 2012 12:33:45 GMT
Content-Length:151
Content-MD5: o***A==
Authorization: OSS q***c:W***=

<? xml version="1.0" encoding="UTF-8"? >

<Delete>
 <Quiet>true</Quiet>
 <Object>
  <Key>multipart.data</Key>
 </Object>
 <Object>
  <Key>test.jpg</Key>
 </Object>
 <Object>
  <Key>demo.jpg</Key>
 </Object>
</Delete>
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***1
Date: Wed, 29 Feb 2012 12:33:45 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.7.7. HeadObject

You can call HeadObject to return the specified Object Meta, without the object content returned.

Request syntax

```
HEAD /ObjectName HTTP/1.1
Host: BucketName/regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Request header

Request header

Name	Description
If-Modified-Since	The information return condition. If the specified time is earlier than the actual object modification time, OSS returns Object Meta and the 200 OK message. Otherwise, OSS returns the 304 Not Modified message. Type: string. Default value: none.
If-Unmodified-Since	The information return condition. If the specified time is equal to or later than the actual object modification time, OSS returns Object Meta and the 200 OK message; otherwise, OSS returns the 412 Precondition Failed message. Type: string. Default value: none.
If-Match	The information return condition. If the ETag value of the source object is equal to the ETag value specified in the request, OSS returns Object Meta and the 200 OK message. Otherwise, OSS returns the 412 Precondition Failed message. Type: string. Default value: none.
If-None-Match	The information return condition. If the ETag value of the source object is not equal to the ETag value specified in the request, OSS returns Object Meta and the 200 OK message. Otherwise, OSS returns the 304 Not Modified message. Type: string. Default value: none.

Detail analysis

1. After the Head Object request is sent, no message body is returned even if the system returns the 200 OK message or an error message.
2. The If-Modified-Since, If-Unmodified-Since, If-Match, and If-None-Match query conditions can be set in the header of the Head Object request. For the detailed setting rules, see the related fields in the Get Object request. If the object is not modified, OSS returns the 304 Not Modified message.
3. If you specify the user-defined Object Meta prefixed with x-oss-meta- when sending a PutObject request, for example, x-oss-meta-location, the user-defined Object Meta is returned.
4. If the object does not exist, OSS returns the 404 Not Found message.
5. If this object is entropy encrypted on the server side, the system automatically returns the decrypted object on receiving the GetObject request, and returns x-oss-server-side-encryption in the response header. The value of x-oss-server-side-encryption indicates the server-side encryption algorithm of the object.
6. If the object type is symbolic link, in the response header, `Content-Length`, `ETag`, and `Content-Md5` are Object Meta of the target object. `Last-Modified` is the maximum value of the target object and symbolic link. Others are Object Meta of symbolic links.
7. If the object type is symbolic link, and the target object does not exist, the system returns Error 404 Not Found. Error code: SymlinkTargetNotExist.
8. If the object type is symbolic link, and the target object type is symbolic link, the system returns Error 400 Bad request. Error code: InvalidTargetType.

Examples

Sample request:

```
HEAD /oss.jpg HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 07:32:52 GMT
Authorization: OSS q***:J***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***1
x-oss-object-type: Normal
Date: Fri, 24 Feb 2012 07:32:52 GMT
Last-Modified: Fri, 24 Feb 2012 06:07:48 GMT
ETag: "f***8"
Content-Length: 344606
Content-Type: image/jpg
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.7.8. GetObjectMeta

You can call Get Object to obtain the basic meta information of an object in a bucket (but the meta information does not return the content). The Object Meta includes the Etag, Size (the object size), and LastModified.

Request syntax

```
GET /ObjectName? objectMeta HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

Detail analysis:

1. After the Get Object Meta request is sent, no message body is returned no matter whether the system returns the OK message or an error message.
2. Get Object Meta must contain the parameters of the ObjectMeta request. Otherwise, it indicates a Get Object request.
3. If the object does not exist, OSS returns the 404 Not Found message.
4. Get Object Meta is more lightweight than Header Object. Only some basic meta information of an object in a bucket is returned. The Object Meta includes the ETag, Size (the object size), and LastModified. The Size is measured with the value of the Content-Length header.

5. If the file type is symbolic link, only the information of the symbolic link itself is returned.

Examples

Sample request:

```
GET /oss.jpg? objectMeta HTTP/1.1
Host: ***.regionid.example.com
Date: Wed, 29 Apr 2015 05:21:12 GMT
Authorization: OSS q***c:C***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***1
Date: Wed, 29 Apr 2015 05:21:12 GMT
ETag: "5***E"
Last-Modified: Fri, 24 Feb 2012 06:07:48 GMT
Content-Length: 344606
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.7.9. PutObjectACL

The Put Object ACL API is used to modify the access permission of an object. Currently, an object may have three types of access permissions: private, public-read, and public-read-write. You can use the x-oss-object-acl field in the PutObjectACL request header to set the ACL of an object. Only the bucket owner has the permission to perform this operation. If the operation succeeds, 200 is returned. Otherwise, the corresponding error code and message are returned.

Request syntax

```
PUT /ObjectName? acl HTTP/1.1
x-oss-object-acl: Permission
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Definition of object ACLs

Definition of object ACLs

Name	Description

Name	Description
private	The object is a private resource. Only the owner or authorized user has the read and write permissions on the object. A signature is required for anonymous access requests.
public-read	Only the owner or authorized user of an object has the read and write permissions on the object. Other users (including anonymous users) have only read permissions on the object.
public-read-write	All users of an object have the read and write permissions on the object.
default	The object inherits the read-write permissions of the bucket.

Detail analysis

1. The read operations of an object include: GetObject, HeadObject, CopyObject, and UploadPartCopy. The write operations of an object include:
   - PutObject
   - PostObject
   - AppendObject
   - DeleteObject
   - DeleteMultipleObjects
   - CompleteMultipartUpload
   - Copy to a new object by using CopyObject
2. The x-oss-object-acl field must be set to one of the preceding three ACLs. Otherwise, OSS returns the 400 Bad Request message. Error code: InvalidArgument.
3. Use the PutObjectACL API to set the ACL of an object. In addition, when writing an object, you can include the x-oss-object-acl field in the request header to set the ACL of the object. The effect is equivalent to PutObject ACL. For example, if the PutObject request header carries x-oss-object-acl, you can set the ACL of an object while uploading the object.
4. When a user who has no permission to read an object attempts to read the object, OSS returns the 403 Forbidden message with the error code AccessDenied. The following message appears: You do not have read permission on this object.
5. When a user who has no permission to write an object attempts to write the object, OSS returns the 403 Forbidden message with the error code AccessDenied. The following message appears: You do not have write permission on this object.
6. Only the owner of a bucket has permissions to call PutObjectACL to modify the ACL of an object in this bucket. When another user calls PutObjectACL, OSS returns the 403 Forbidden message with the error code AccessDenied. The following message appears: You do not have write acl permission on this object.
7. The ACL privileges of objects take precedence over those of buckets. For example, OSS allows users to access a public-read-write object in a bucket is public-read-write, the system first checks the ACL of the object when a user accesses the object. As a result, all users can access

this object even if the bucket is a private bucket. If no ACL has been set for an object, its ACL is the same as that of the bucket.

Examples

Sample request:

```
Put/test-object? acl HTTP/1.1
x-oss-object-acl: public-read
Host: ***.regionid.example.com
Date: Wed, 29 Apr 2015 05:21:12 GMT
Authorization: OSS q***c:K***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***1
Date: Wed, 29 Apr 2015 05:21:12 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.7.10. GetObjectACL

You can call GetObjectACL to obtain permissions to access an object in a bucket.

Request syntax

```
GET /ObjectName? acl HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Response elements

Response elements

Name	Description
AccessControlList	The container that stores the ACL information. Type: container. Parent element: AccessControlPolicy.

Name	Description
AccessControlPolicy	The container that stores results of the GetObjectACL request. Type: container. Parent element: none.
DisplayName	The name of the bucket owner (which is currently the same as the user ID). Type: string. Parent element: AccessControlPolicy.Owner.
Grant	The ACL permission of the object. Type: enumeration. Valid values: private, public-read, and public-read-write. Parent element: AccessControlPolicy.AccessControlList.
ID	The user ID of the bucket owner. Type: string. Parent element: AccessControlPolicy.Owner.
Owner	The container that stores the information about the bucket owner. Type: container. Parent element: AccessControlPolicy.

Detail analysis

1. Only the bucket owner can call the GetObjectACL API to obtain the ACL of an object in the bucket. If you are not the bucket owner and send a GetObjectACL request, OSS returns the 403 Forbidden message. Error code: AccessDenied. The following message is displayed: You do not have read acl permission on this object.
2. If a GetObjectACL request is sent but no ACL has been set for the object, OSS returns the default ACL for this object, indicating that the bucket ACL applies. In other words, if the access permission of the bucket is private, the access permission of this object is also private. If the access permission of the bucket is public-read-write, the access permission of this object is also public-read-write.

Examples

Sample request:

```
GET /test-object? acl HTTP/1.1
Host: ***.regionid.example.com
Date: Wed, 29 Apr 2015 05:21:12 GMT
Authorization: OSS q***c:C***=
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***1
Date: Wed, 29 Apr 2015 05:21:12 GMT
Content-Length: 253
Content-Type: application/xml
Connection: keep-alive
Server: AliyunOSS

<? xml version="1.0" ? >
<AccessControlPolicy>
  <Owner>
    <ID>0***2</ID>
    <DisplayName>0***2</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>public-read </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

2.4.1.7.11. PostObject

You can use PostObject to upload an object to a specified bucket using the HTML form. As a substitute of Put Object, Post Object makes it possible to upload objects to a bucket based on the browser. The message body of Post Object is encoded using multipart/form-data. In the Put Object operation, parameters are transferred through the HTTP request header.

Request syntax

```
POST / HTTP/1.1
Host: BucketName.regionid.example.com
User-Agent: browser_data
Content-Length: ContentLength
Content-Type: multipart/form-data; boundary=9431149156168
--9431149156168
Content-Disposition: form-data; name="key"
key
--9431149156168
Content-Disposition: form-data; name="success_action_redirect"
success_redirect
--9431149156168
Content-Disposition: form-data; name="Content-Disposition"
attachment;filename=oss_download.jpg
--9431149156168
Content-Disposition: form-data; name="x-oss-meta-uuid"
myuuid
--9431149156168
Content-Disposition: form-data; name="x-oss-meta-tag"
mytag
--9431149156168
Content-Disposition: form-data; name="OSSAccessKeyId"
access-key-id
--9431149156168
Content-Disposition: form-data; name="policy"
encoded_policy
--9431149156168
Content-Disposition: form-data; name="Signature"
signature
--9431149156168
Content-Disposition: form-data; name="file"; filename="MyFilename.jpg"
Content-Type: image/jpg
file_content
--9431149156168
Content-Disposition: form-data; name="submit"
Upload to OSS
--9431149156168--
```

Form fields

Form fields

Name	Description	Required
OSSAccessKeyId	The AccessKey ID of the bucket owner. Type: string. Default value: none. Restriction: This form field is required when the bucket does not allow public-read-write or when the policy (or Signature) form field is provided.	Conditional
policy	Specify validity of the form fields in the request. A request that does not contain the policy form field is treated as an anonymous request, which can be used only to access buckets that allow public-read-write. For more information, see 5.7.4.1 Post policy. Type: string. Default value: none. Restriction: This form field is required when the bucket does not allow public-read-write or when the OSS Access Key ID (or Signature) form field is provided.	Conditional
Signature	The signature information that is computed based on the Access Key Secret and Policy. The OSS checks the signature information to verify validity of the Post Object request. Type: string. Default value: none. Restriction: This form field is required when the bucket does not allow public-read-write, or when the OSSAccessKeyId (or Policy) form field is provided.	Conditional
Cache-Control, Content-Type, Content-Disposition, Content-Encoding, and Expires	REST request header fields. For more information, see PutObject. Type: string. Default value: none.	Optional
file	The file or text content. It must be the last field in the form. The browser automatically sets Content-Type based on the object type and overwrites the user setting. The OSS can only upload one object at a time. Type: string. Default value: none.	Required

Name	Description	Required
key	The name of the object you want to upload. If the name of the uploaded file needs to be used as the object name, use the ${filename} variable. For example, if the user uploads the b.jpg object and the key field is set to /user/a/${filename}, the object name is /user/a/b.jpg. If the object name contains the path, remove the path from the file name. For example, if the user uploads the a/b/c/b.jpg file, use the object name b.jpg. If the Key field is set to /user/a/${filename}, the final object name is /user/a/b.jpg. Type: string. Default value: none.	Required
success_action_redirect	The URL to which the client is redirected after successful uploads. If this form field is not specified, the returned result is specified by success_action_status. If upload fails, the OSS returns an error code, and the client is not redirected to any URL. Type: string. Default value: none.	Optional
success_action_status	The status code returned to the client after a successful upload if success_action_redirect is not specified. Valid values: 200, 201, and 204 (default). If this field is set to 200 or 204, the OSS returns an empty object and a corresponding status code. If this field is set to 201, the OSS returns an XML file and the 201 status code. If this field is not specified or set to an invalid value, the OSS returns an empty file and the 204 status code. Type: string. Default value: none.	Optional
x-oss-meta-*	The user meta value set by the user. OSS does not check or use this value. Type: string. Default value: none.	Optional
x-oss-server-side-encryption	The encryption algorithm that OSS uses to encrypt an object when the object is created. Type: string. Valid value: AES256.	Optional
x-oss-object-acl	The access permission granted by OSS for an object when the object is created. Type: string. Valid values: public-read, private, and public-read-write.	Optional

Name	Description	Required
x-oss-security-token	If an STS temporary security credential is used for this access, you must set this field to the SecurityToken value and set OSSAccessKeyId to the value of the paired temporary AccessKeyId. The method of calculating a signature based on a temporary AccessKey ID is the same as that based on a typical AccessKey ID. Type: string. Default value: none.	Optional

Response header

Response header

Name	Description
x-oss-server-side-encryption	If x-oss-server-side-encryption is specified in the request, the response header contains this field, which indicates the encryption algorithm used. Type: string.

Response elements

Response elements

Name	Description
PostResponse	The container that stores the response of the PostObject request. Type: container. Child elements: Bucket, ETag, Key, and Location
Bucket	The bucket name. Type: string. Parent element: PostResponse.
ETag	The entity tag (ETag) created when an object is generated. For an object created with PostObject, the ETag value is the object UUID, which can be used to check whether the object content has changed. Type: string. Parent element: PostResponse.
Location	The URL of the created object. Type: string. Parent element: PostResponse.

Detail analysis

1. To perform the PostObject operation, you must have the permission to write the bucket. If the

bucket allows public-read-write, signature information is optional. If the bucket does not allow public-read-write, signature verification must be performed. Unlike PutObject, PostObject uses an AccessKey Secret to calculate the signature for policy. The computed signature string is used as the value of the signature form field. OSS checks this value to verify the validity of the signature.

2. No matter whether the bucket allows public-read-write, once any one of the OSSAccessKeyId, Policy, and Signature form fields is uploaded, the remaining two form fields are required. If the remaining two form fields are missing, the OSS returns the error code: InvalidArgument.
3. The form submitted by using PostObject must be encoded with multipart/form-data. In other words, Content-Type in the header must be set to:

   ```
   multipart/form-data; boundary=xxxxxx
   ```

   where boundary is the boundary string.
4. The URL of the submitted form can be the domain of the bucket. You do not need to specify the object in the URL. In other words, the request line is:

   ```
   POST / HTTP/1.1
   ```

   Do not write it as:

   ```
   POST /ObjectName HTTP/1.1
   ```
5. The policy specifies the valid values of form fields in the Post Object request. The OSS checks validity of the request based on the policy. If the request is invalid, the OSS returns the error code: AccessDenied. When checking validity of the policy, the OSS does not check irrelevant form fields in the policy.
6. The form and policy must be encoded with UTF-8. The policy is a JSON text encoded with UTF-8 and Base64.
7. The Post Object request can contain extra form fields. The OSS checks validity of these form fields based on the policy.
8. If the Content-MD5 field value is specified in the request header, OSS calculates the Content-MD5 field value in the request body and checks whether the two values are the same. If they are different, OSS returns the InvalidDigest error.
9. If the Post Object request contains the Header signature or URL signature, the OSS does not check these signatures.
10. If the request contains a form field prefixed with x-oss-meta-, the form field is considered as the user meta, for example, x-oss-meta-location. An object may have multiple similar parameters, but the total size of the user-defined Object Meta cannot exceed 8 KB.
11. The total length of the PostObject request body must not exceed 5 GB. When the object length is too large, the system returns the error code: EntityTooLarge.
12. If the x-oss-server-side-encryption header is specified when you upload an object, the value of this header must be set to AES256 or KMS. Otherwise, the system returns 400 and the error code: InvalidEncryptionAlgorithmError. If this parameter is specified in the request header, the response header also contains this parameter, and OSS stores the uploaded object after encryption. When this object is downloaded, the response header contains x-oss-server-side-encryption, the value of which is set to the encryption algorithm of this object.
13. Form fields are case-insensitive, but their values are case-sensitive.

Examples

Sample request:

```
POST / HTTP/1.1
Host: ***.regionid.example.com
Content-Length: 344606
Content-Type: multipart/form-data; boundary=9431149156168
--9431149156168
Content-Disposition: form-data; name="key"
/user/a/${filename}
--9431149156168
Content-Disposition: form-data; name="success_action_status"
200
--9431149156168
Content-Disposition: form-data; name="Content-Disposition"
content_disposition
--9431149156168
Content-Disposition: form-data; name="x-oss-meta-uuid"
uuid
--9431149156168
Content-Disposition: form-data; name="x-oss-meta-tag"
metadata
--9431149156168
Content-Disposition: form-data; name="OSSAccessKeyId"
44CF9590006BF252F707
--9431149156168
Content-Disposition: form-data; name="policy"
eyJleHBpcmF0aW9uIjoiMjAxMy0xMi0wMVQxMjowMDowMFoiLCJjb25kaXRpb25zIjpbWyJjb250ZW50LWxlbmd0
aC1yYW5nZSIsIDAsIDEwNDg1NzYwXSx7ImJ1Y2tldCI6ImFoYWhhIn0sIHsiQSI6ICJhIn0seyJrZXkiOiAiQUJDIn1df
Q==
--9431149156168
Content-Disposition: form-data; name="Signature"
k***0+d***k=
--9431149156168
Content-Disposition: form-data; name="file"; filename="MyFilename.txt"
Content-Type: text/plain
abcdefg
--9431149156168
Content-Disposition: form-data; name="submit"
Upload to OSS
--9431149156168--
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 6***e
Date: Fri, 24 Feb 2014 06:03:28 GMT
ETag: 5***E
Connection: keep-alive
Content-Length: 0
Server: AliyunOSS
```

Post Policy

The policy form field requested by POST is used to verify the validity of the request. The policy is a JSON text encoded with UTF-8 and Base64. It states the conditions that a PostObject request must meet. Although the policy form field is optional for uploading public-read-write buckets, we recommend that you use this field to limit PostObject requests.

- Policy example

```
{ "expiration": "2014-12-01T12:00:00.000Z",
 "conditions": [
 {"bucket": "johnsmith" },
 ["starts-with", "$key", "user/eric/"]
 ]
}
```

  In the PostObject request, the policy must contain the expiration and conditions attributes.

- Expiration

  Expiration specifies the expiration time of the policy, which is expressed in ISO 8601 GMT. For example, 2014-12-01T12:00:00.000Z indicates that the Post Object request must be sent before 12:00 on December 1, 2014.

- Conditions

  Conditions specify the valid values of form fields in the PostObject request. Note: The value of a form field is extended after OSS checks the policy. Therefore, the valid value of the form field set in the policy is equivalent to the value of the form field before extension. For example, if the key form field is set to user/user1/${filename} and the user's file name is a.txt, the policy form field in the PostObject request must be set to ["eq","$key","user/user1/\${filename}"], instead of ["eq","$key","$key","user/user1/a.txt]. The following table lists the conditions supported by the policy:

Conditions

Name	Description
content-length-range	The acceptable maximum and minimum sizes of the uploaded file. This condition supports the content-length-range matching method.

Name	Description
Cache-Control, Content-Type, Content-Disposition, Content-Encoding, and Expires	HTTP request headers. This condition supports the exact and starts-with matching methods.
key	The name of the object you want to upload. This condition supports the exact and starts-with matching methods.
success_action_redirect	The URL to which the client is redirected after successful upload. This condition supports the exact and starts-with matching methods.
success_action_status	The status code returned after successful upload if success_action_redirect is not specified. This condition supports the exact and starts-with matching methods.
x-oss-meta-*	The user meta set by the user. This condition supports the exact and starts-with matching methods.

If the PostObject request contains other form fields, these extra form fields can be added to conditions of the policy. OSS does not check validity of the form fields that are not contained in conditions.

- Condition matching methods

Condition matching methods	Description
Exact match	The value of a form field must be exactly the same as the value declared in the conditions. For example, if the value of the key form field must be a, the conditions must be {"key" : "a"} or ["eq", "$key", "a"].
Starts With	The value of a form field must start with the specified value. For example, if the value of the key form field must start with /user/user1, the conditions must be ["starts-with", "$key", "/user/user1"].
Specified file size	The maximum and minimum sizes of the file that can be uploaded. For example, if the acceptable file size is 1-10 bytes, the conditions must be [“content-length-range” , 1, 10].

- Escape characters

  In the policy form field of the Post Object request, $ is used to indicate a variable. Therefore, to describe $, the escape character must be used. In addition, some characters in JSON strings are escaped. The following chart describes characters in the JSON string of the policy form field of a Post Object request.

Escape characters

Escape character	Description
\/	Slash
\	Backslash
\"	Double quotation marks
\$	Dollar sign
Space	Blank
\f	Form feed
\n	Line feed
\r	Enter
\t	Horizontal tab
\uxxxx	Unicode character

Post Signature

For signature authentication, the HTML form must contain policy and Signature. Policy specifies which values are valid in the request. The procedure for calculating a signature is as follows:

1. Create a UTF-8 encoded policy.
2. Encode the policy with Base64. The encoding result is the value of the policy form field, and this value is used as the string to be signed.
3. Use AccessKeySecret to sign the string. The signing method is the same as the signature calculation method in the header; that is, by replacing the string to be signed with the policy form field.

2.4.1.7.12. PutSymlink

You can call PutSymlink to create a symbolic link.

Request syntax

```
PUT /ObjectName? symlink HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
x-oss-symlink-target: TargetObjectName
```

Request header

Request header

Name	Description
x-oss-symlink-target	The target link to which the symbolic link points. Type: string. Valid value: The naming rules are the same as those for objects.

Detail analysis

1. As with ObjectName, TargetObjectName must be URL-encoded.
2. The target object type of a symbolic link cannot be the symbolic link.
3. When creating a symbolic link, do not perform the following checks:
   - Whether the target object exists.
   - Whether the storage class of the target object is valid.
   - Whether the user has permission to access the target object.

   The foregoing checks are deferred until GetObject must access the API of the target object.
4. If the object to be added already exists and you have the permission to access the object, the new object overwrites the existing object, and OSS returns the 200 OK message.
5. If the PutSymlink request carries a parameter prefixed with x-oss-meta-, the parameter is treated as user meta, such as x-oss-meta-location. An object may have multiple similar parameters, but the total size of the user-defined Object Meta cannot exceed 8 KB.

Examples

Sample request:

```
PUT /link-to-oss? symlink HTTP/1.1
Host: ***.regionid.example.com
Cache-control: no-cache
Content-Disposition: attachment;filename=oss_download.jpg
Date: Tue, 08 Nov 2016 02:00:25 GMT
Authorization: OSS q***:k***=
x-oss-symlink-target: oss.jpg
```

Sample response:

```
HTTP/1.1 200 OK
Server: AliyunOSS
Date: Tue, 08 Nov 2016 02:00:25 GMT
Content-Length: 0
Connection: keep-alive
x-oss-request-id: 5***5
ETag: "0***6"
```

2.4.1.7.13. GetSymlink

You can call GetSymlink to obtain a symbolic link. Before you call GetSymlink, you must have the read permission on a symbolic link.

Request syntax

```
GET /ObjectName? symlink HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Response header

Response header

Name	Description
x-oss-symlink-target	The target object to which the symbolic link points. Type: string.

Detail analysis

If the object does not exist, OSS returns the 404 Not Found message. Error code: NoSuchKey.

Examples

Sample request:

```
GET /link-to-oss.jpg? symlink HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 06:38:30 GMT
Authorization: OSS q***:U***=
```

Sample response:

```
HTTP/1.1 200 OK
Server: AliyunOSS
Date: Fri, 24 Feb 2012 06:38:30 GMT
Last-Modified: Fri, 24 Feb 2012 06:07:48 GMT
Content-Length: 0
Connection: keep-alive
x-oss-request-id: 5***A
x-oss-symlink-target: oss.jpg
ETag: "A***2"
```

2.4.1.7.14. Callback

To enable OSS to return callback information of an object to an application server after the object is uploaded to OSS, you need only to include a callback parameter in the upload request sent to OSS. This topic describes how to implement upload callback in detail.

Note The API operations that support upload callback include PutObject, PostObject, and CompleteMultipartUpload. For more information about callback, see Add signatures on the server, configure upload callback, and directly transfer data.

Step 1: Construct parameters

- Construct a callback parameter.

  A callback parameter is a Base64-encoded string (field) in JSON format. To construct a callback parameter, you must specify the URL (callbackUrl) of the server to which the callback information is sent and the content (callbackBody) of the callback information.

  The following table describes the JSON fields included in a callback parameter.

Field	Description	Required
callbackUrl	○ After an object is uploaded, OSS sends a callback request by using the POST method to this URL. The body of the request is the content specified in callbackBody. In normal cases, the URL returns an `HTTP/1.1 200 OK` response. The response body must be in JSON format, and the Content-Length header of the response is a valid value that is not greater than 3 MB. ○ You can configure up to five URLs separated by semicolons (;) for a request. OSS sends requests to each URL until the first success response is returned. ○ If no URLs are configured or the value of this field is null, OSS determines that the callback function is not configured. ○ HTTPS-based URLs are supported. ○ To ensure that Chinese characters can be correctly processed, the callback URL must be encoded. For example, if the value of callbackUrl is `http://example.com/ChineseCharacters.php?key=value&ChineseName=ChineseValue`, the value must be encoded into `http://example.com/%E4%B8%AD%E6%96%87.php?key=value&%E4%B8%AD%E6%96%87%E5%90%8D%E7%A7%B0=%E4%B8%AD%E6%96%87%E5%80%BC`.	Yes

Field	Description	Required
callbackHost	○ The value of the Host header in the callback request. This field is valid only when callbackUrl is specified. ○ If callbackHost is not specified, the hosts are resolved from the URLs of the callbackUrl field and are specified as the value of callbackHost.	No
callbackBody	○ The value of the callback request body. Example: key=$(object)&etag=$(etag)&my_var=$(x:my_var). ○ System variables, custom variables, and constants are supported for this field. The following table lists the supported system variables. Custom variables are passed by using the callback-var parameter in the PutObject and CompleteMultipart operations and by using form fields in the PostObject operation.	Yes
callbackBodyType	○ The Content-Type header in the callback request. Valid values: application/x-www-form-urlencoded and application/json. Default value: application/x-www-form-urlencoded. ○ If the value of callbackBodyType is application/x-www-form-urlencoded, variables in callbackBody are replaced by the encoded URLs. If the value of callbackBodyType is application/json, the variables are replaced in JSON format.	No

Examples of the JSON fields in a callback parameter are as follows:

```
{
"callbackUrl":"121.101.166.30/test.php",
"callbackHost":"oss-cn-hangzhou.aliyuncs.com",
"callbackBody":"{\"mimeType\":${mimeType},\"size\":${size}}",
"callbackBodyType":"application/json"
}
```

```
{
"callbackUrl":"121.43.113.8:23456/index.html",
"callbackBody":"bucket=${bucket}&object=${object}&etag=${etag}&size=${size}&mimeType=${mimeType}&imageInfo.height=${imageInfo.height}&imageInfo.width=${imageInfo.width}&imageInfo.format=${imageInfo.format}&my_var=${x:my_var}"
}
```

The following table describes the system parameters you can configure for callbackBody.

System parameter	Description
bucket	The bucket that contains the requested object.
object	The name of the requested object.
etag	The ETag field configured for the object and returned to the requester.
size	The size of the requested object, which is the total size of the entire object in CompleteMultipartUpload operations.
mimeType	The resource type. For example, the resource type of JPEG images is image/jpeg.
imageInfo.height	The height of the image.
imageInfo.width	The width of the image.
imageInfo.format	The format of the image. Example: JPG or PNG.

> **Note** Only an image object supports the imageInfo parameter. If the object is not an image, the values of imageInfo.height, imageInfo.width, and imageInfo.format are null.

- Construct custom parameters by using callback-var.

  You can configure custom parameters by using the callback-var parameter. Custom parameters are key-value pairs in Map. You can add required parameters to the map. When a POST callback request is initiated, OSS adds these custom parameters and the system parameters described in the preceding section to the body of the POST request. This method allows these parameters to be easily obtained by the requester.

  You can construct a custom parameter the way you construct a callback parameter. Each parameter has a key-value pair, which is a map that consists of key-value pairs of all custom parameters.

  > **Note** The key of a custom parameter must start with x: and be in lowercase letters. Otherwise, OSS returns an error.

  Assume that you need to configure two custom parameters x:var1 and x:var2. The value of x:var1 is value1. The value of x:var2 is value2. The constructed JSON string is as follows:

```
{
"x:var1":"value1",
"x:var2":"value2"
}
```

Note If the input callback parameter or callback-var parameter is invalid, HTTP status code 400 is returned with the InvalidArgument error code. This error occurs in the following scenarios:

- URLs and headers are passed in at the same time to the callback parameter (x-oss-callback) or the callback-var parameter (x-oss-callback-var) in PutObject and CompleteMultipartUpload operations.
- The size of the callback or callback-var parameter exceeds 5 KB. This does not occur in PostObject operations because the callback-var parameter is not available in PostObject operations.
- The callback or callback-var parameter is not Base64-encoded or is not in the valid JSON format after being decoded.
- The callbackUrl field decoded from the callback parameter includes more than five URLs, or the port in the URL is invalid. Example:

```
{"callbackUrl":"10.101.166.30:test",
  "callbackBody":"test"}
```

- The callbackBody field decoded from the callback parameter is null.
- The value of the callbackBodyType field decoded from the callback parameter is not `application/x-www-form-urlencoded` or `application/json`.
- The variables in the callbackBody field decoded from the callback parameter are not in the valid format of ${var}.
- The variables in the callbackBody field decoded from the callback-var parameter are not in the expected JSON format of `{"x:var1":"value1","x:var2":"value2"...}`.

Step 2: Construct a callback request

After you construct the callback and callback-var parameters, you must add the parameters to the callback request sent to OSS.

You can use the following methods to add parameters:

- Add the parameters to the URL.
- Add the parameters to the header.
- Add the parameters to the form fields in the body of a POST request.

Note You can use only this method to specify callback parameters when you upload objects by using POST requests.

You can only use one of the preceding three methods at a time. If you use more than one method, OSS returns the InvalidArgument error code.

To add the parameters to a request sent to OSS, you must use Base64 to encode the JSON string constructed in the preceding section, and then add the parameters as follows:

- To add the parameters to the URL, add `callback=[CallBack]` or `callback-var=[CallBackVar]` to the request as a URL parameter. When the CanonicalizedResource field in the signature is calculated, callback or callback-var is used as a subresource.
- To add the parameters to the header, add `x-oss-callback=[CallBack]` or `x-oss-callback-var=[CallB`

ackVar] to the request as a header. When the CanonicalizedOSSHeaders field in the signature is calculated, include x-oss-callback-var and x-oss-callback. Examples:

```
PUT /test.txt HTTP/1.1
Host: callback-test.oss-test.aliyun-inc.com
Accept-ncoding: identity
Content-Length: 5
x-oss-callback-var: eyJ4Om15X3ZhciI6ImZvci1jYWxsYmFjay10ZXN0In0=
User-Agent: aliyun-sdk-python/0.4.0 (Linux/2.6.32-220.23.2.ali1089.el5.x86_64/x86_64;2.5.4)
x-oss-callback: eyJjYWxsYmFja1VybCI6IjEyMS40My4xMTMuODoyMzQ1Ni9pbmRleC5odG1sIiwgICJjYWxsY
mFja0JvZHkiOiJidWNrZXQ9JHtidWNrZXR9Jm9iamVjdD0ke29iamVjdH0mZXRhZz0ke2V0YWd9JnNpemU9JHtz
aXplfSZtaW1lVHlwZT0ke21pbWVUeXBlfSZpbWFnZUluZm8uaGVpZ2h0PSR7aW1hZ2VJbmZvLmhlaWdodH
0maW1hZ2VJbmZvLndpZHRoPSR7aW1hZ2VJbmZvLndpZHRofSZpbWFnZUluZm8uZm9ybWF0PSR7aW1hZ
2VJbmZvLmZvcm1hdH0mbXlfdmFyPSR7eDpteV92YXJ9In0=
Host: callback-test.oss-test.aliyun-inc.com
Expect: 100-Continue
Date: Mon, 14 Sep 2015 12:37:27 GMT
Content-Type: text/plain
Authorization: OSS mlepou3zr4u7b14:5a74vhd4UXpmyuudV14Kaen5****
Test
```

- Add the parameters to the form fields in the body of a POST request.
  - It is slightly complicated to add the callback parameter when the POST method is used to upload an object because the callback parameter must be added by using a separate form field. Example:

```
--9431149156168
Content-Disposition: form-data; name="callback"
eyJjYWxsYmFja1VybCI6IjEwLjEwMS4xNjYuMzA6ODA4My9jYWxsYmFjay5waHAiLCJjYWxsYmFja0hvc3Qi
OiIxMC4xMDEuMTY2LjMwIiwiY2FsbGJhY2tCb2R5IjoiZmlsZW5hbWU9JChmaWxlbmFtZSkmdGFibGU9JHt4
OnRhYmxlfSIsImNhbGxiYWNrQm9keVR5cGUiOiJhcHBsaWNhdGlvbi94LXd3dy1mb3JtLXVybGVuY29kZWQi
fQ==
```

- Each custom parameter uses a separate form field. You cannot add the callback-var parameter to existing fields. For example, if the JSON string for the custom parameter is as follows:

```
{
"x:var1":"value1",
"x:var2":"value2"
}
```

The form fields in the POST request are as follows:

```
--9431149156168
Content-Disposition: form-data; name="callback"
eyJjYWxsYmFja1VybCI6IjEwLjEwMS4xNjYuMzA6ODA4My9jYWxsYmFjay5waHAiLCJjYWxsYmFja0hvc3Qi
OiIxMC4xMDEuMTY2LjMwIiwiY2FsbGJhY2tCb2R5IjoiZmlsZW5hbWU9JChmaWxlbmFtZSkmdGFibGU9JHt4
OnRhYmxlfSIsImNhbGxiYWNrQm9keVR5cGUiOiJhcHBsaWNhdGlvbi94LXd3dy1mb3JtLXVybGVuY29kZWQi
fQ==
--9431149156168
Content-Disposition: form-data; name="x:var1"
value1
--9431149156168
Content-Disposition: form-data; name="x:var2"
value2
```

You can also add callback conditions in the policy (if callback parameters are not added, upload verification is not performed on policy). Example:

```
{ "expiration": "2014-12-01T12:00:00.000Z",
  "conditions": [
    {"bucket": "johnsmith" },
    {"callback": "eyJjYWxsYmFja1VybCI6IjEwLjEwMS4xNjYuMzA6ODA4My9jYWxsYmFjay5waHAiLCJjYWx
sYmFja0hvc3QiOiIxMC4xMDEuMTY2LjMwIiwiY2FsbGJhY2tCb2R5IjoiZmlsZW5hbWU9JChmaWxlbmFtZSki
LCJjYWxsYmFja0JvZHlUeXBlIjoiYXBwbGljYXRpb24veC13d3ctZm9ybS11cmxlbmNvZGVkIn0="},
    ["starts-with", "$key", "user/eric/"],
  ]
}
```

Step 3: Initiate a callback request

If an object is uploaded, OSS sends the content specified by the callback and callback-var parameters in the request to the application server by using the POST method. Example:

```
POST /index.html HTTP/1.0
Host: 121.43.113.8
Connection: close
Content-Length: 181
Content-Type: application/x-www-form-urlencoded
User-Agent: http-client/0.0.1
bucket=callback-test&object=test.txt&etag=D8E8FCA2DC0F896FD7CB4CB0031BA249&size=5&mimeType=t
ext%2Fplain&imageInfo.height=&imageInfo.width=&imageInfo.format=&x:var1=for-callback-test
```

Step 4 (optional): Sign the callback request

If the callback parameter is configured in the request, OSS uses POST to send a callback request to the application server based on the specified callback URL. To verify whether the callback request received by the application server is initiated by OSS, you can sign the callback request.

- Generate a signature.

  A callback request is signed by OSS by using the RSA asymmetric algorithm.

  To generate a signature, encrypt the callback string with a private key. Example:

  ```
  authorization = base64_encode(rsa_sign(private_key, url_decode(path) + query_string + '\n' + body, m
  d5))
  ```

  > **Note** In the preceding code, private_key is a private key only known by OSS, path is the resource path included in the callback request, query_string is the query string, and body is the message body specified in the callback request.

  A callback request is signed in the following steps:

  i. Obtain the callback string to sign, which consists of the resource path that is obtained by decoding the URL, the original query string, a carriage return, and the callback message body.
  ii. Sign the callback string by using the RSA encryption algorithm. Use the private key to encrypt the signature string. The hash function used for the signature is MD5.
  iii. Use Base64 to encode the signed result to obtain the final signature and add the signature to the Authorization header in the callback request.

  Example:

```
POST /index.php? id=1&index=2 HTTP/1.0
Host: 121.43.113.8
Connection: close
Content-Length: 18
authorization: kKQeGTRccDKyHB3H9vF+xYMSrmhMZjzzl2/kdD1ktNVgbWEfYTQG0G2SU/RaHBovRCE8Ok
QDjC3uG33esH2t****
Content-Type: application/x-www-form-urlencoded
User-Agent: http-client/0.0.1
x-oss-pub-key-url: aHR0cDovL2dvc3NwdWJsaWMuYWxpY2RuLmNvbS9jYWxsYmFja19wdWJfa2V5X3YxLn
BlbQ==
bucket=yonghu-test
```

In the preceding code, path is set to `/index.php`, query_string is set to `? id=1&index=2`, the body is set to `bucket=yonghu-test`. The final signature is `kKQeGTRccDKyHB3H9vF+xYMSrmhMZjzzl2/kdD1ktNVgbWEfYTQG0G2SU/RaHBovRCE8OkQDjC3uG33esH2txA==`.

- Verify the signature.

  Signature verification is an inverse process of signing a request. The signature is verified by the application server as follows:

  ```
  Result = rsa_verify(public_key, md5(url_decode(path) + query_string + '\n' + body), base64_decode(au
  thorization))
  ```

  The fields in the preceding code have the same meanings as they are used to sign the request. public_key indicates the public key and authorization indicates the signature in the callback request header. The signature is verified as follows:

  i. The x-oss-pub-key-url header in the callback request stores the Base64-encoded URL of the public key. Therefore, you must decode the Base64-encoded URL to obtain the public key.

  ```
  public_key = urlopen(base64_decode(x-oss-pub-key-url header))
  ```

  > **Note** To ensure that the public key is issued by OSS, you must verify whether the value of the `x-oss-pub-key-url` header starts with `http://gosspublic.alicdn.com/` or `https://gosspublic.alicdn.com/`.

  ii. Obtain the signature decoded in Base64.

  ```
  signature = base64_decode(authorization header)
  ```

  iii. Obtain the string to sign the way described in the process of signing the callback request.

  ```
  sign_str = url_decode(path) + query_string + '\n' + body
  ```

  iv. Verify the signature.

  ```
  result = rsa_verify(public_key, md5(sign_str), signature)
  ```

The preceding code is used as an example:

i. Obtain the URL of the public key by decoding `aHR0cDovL2dvc3NwdWJsaWMuYWxpY2RuLmNvbS9jYWxsYmFja19wdWJfa2V5X3YxLnBlbQ==` in Base64. The decoded URL is `http://gosspublic.alicdn.com/callback_pub_key_v1.pem`.

ii. Decode signature header `kKQeGTRccDKyHB3H9vF+xYMSrmhMZjzzl2/kdD1ktNVgbWEfYTQG0G2SU/RaHBovRCE8OkQDjC3uG33esH2txA==` in Base64. The decoded result cannot be displayed because it is a nonprintable string.

iii. Obtain the string to sign, which is url_decode("index.php") + "? id=1&index=2" + "\n" + "bucket=yonghu-test", and perform MD5 verification on the string.

iv. Verify the signature.

- Application server example

  The following Python code shows you how an application server verifies a signature. Before you run the code, the M2Crypto library must be installed.

```
import httplib
import base64
import md5
import urllib2
from BaseHTTPServer import BaseHTTPRequestHandler, HTTPServer
from M2Crypto import RSA
from M2Crypto import BIO
def get_local_ip():
    try:
        csock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
        csock.connect(('8.8.8.8', 80))
        (addr, port) = csock.getsockname()
        csock.close()
        return addr
    except socket.error:
        return ""
class MyHTTPRequestHandler(BaseHTTPRequestHandler):
    '''
    def log_message(self, format, *args):
        return
    '''
    def do_POST(self):
        #get public key
        pub_key_url = ''
        try:
            pub_key_url_base64 = self.headers['x-oss-pub-key-url']
            pub_key_url = pub_key_url_base64.decode('base64')
            if not pub_key_url.startswith("http://gosspublic.alicdn.com/") and not pub_key_url.startswith("
```

```
        if not pub_key_url.startswith("http://gosspublic.alicdn.com/") and not pub_key_url.startswith(
https://gosspublic.alicdn.com/"):
            self.send_response(400)
            self.end_headers()
            return
        url_reader = urllib2.urlopen(pub_key_url)
        #you can cache it
        pub_key = url_reader.read()
      except:
        print 'pub_key_url : ' + pub_key_url
        print 'Get pub key failed!'
        self.send_response(400)
        self.end_headers()
        return
      #get authorization
      authorization_base64 = self.headers['authorization']
      authorization = authorization_base64.decode('base64')
      #get callback body
      content_length = self.headers['content-length']
      callback_body = self.rfile.read(int(content_length))
      #compose authorization string
      auth_str = ''
      pos = self.path.find('?')
      if -1 == pos:
        auth_str = urllib2.unquote(self.path) + '\n' + callback_body
      else:
        auth_str = urllib2.unquote(self.path[0:pos]) + self.path[pos:] + '\n' + callback_body
      print auth_str
      #verify authorization
      auth_md5 = md5.new(auth_str).digest()
      bio = BIO.MemoryBuffer(pub_key)
      rsa_pub = RSA.load_pub_key_bio(bio)
      try:
        result = rsa_pub.verify(auth_md5, authorization, 'md5')
      except:
        result = False
      if not result:
        print 'Authorization verify failed!'
        print 'Public key : %s' % (pub_key)
        print 'Auth string : %s' % (auth_str)
        self.send_response(400)
        self.end_headers()
```

```
            return
        #do something according to callback_body
        #response to OSS
        resp_body = '{"Status":"OK"}'
        self.send_response(200)
        self.send_header('Content-Type', 'application/json')
        self.send_header('Content-Length', str(len(resp_body)))
        self.end_headers()
        self.wfile.write(resp_body)
class MyHTTPServer(HTTPServer):
    def __init__(self, host, port):
        HTTPServer.__init__(self, (host, port), MyHTTPRequestHandler)
if '__main__' == __name__:
    server_ip = get_local_ip()
server_port = 23451
server = MyHTTPServer(server_ip, server_port)
server.serve_forever()
```

The code for the server in other programming languages is as follows:

Java:

- Click here to download the code.
- Running method: Decompress the package and run `java -jar oss-callback-server-demo.jar 9000`. 9000 is the port number and can be specified as needed.

PHP:

- Click here to download the code.
- Running method: Deploy the code to an Apache environment because some headers in the PHP code depend on the environment. You can modify the example code based on the environment.

Python:

- Click here to download the code.
- Running method: Decompress the package and run `python callback_app_server.py`. Before you run the code, RSA dependencies must be installed.

.NET:

- Click here to download the code.
- Running method: Decompress the package and follow `README.md`.

Go:

- Click here to download the code.
- Running method: Decompress the package and follow `README.md`.

Ruby:

- Click here to download the code.
- Running method: Run the ruby aliyun_oss_callback_server.rb command.

Step 5: Return the callback result

The application server returns the response to OSS.

The response to the callback request is as follows:

```
HTTP/1.0 200 OK
Server: BaseHTTP/0.3 Python/2.7.6
Date: Mon, 14 Sep 2015 12:37:27 GMT
Content-Type: application/json
Content-Length: 9
{"a":"b"}
```

> **Note** The response returned by the application server to OSS must contain the Content-Length header. The size of the response body cannot exceed 1 MB.

Step 6: Return the upload result

OSS returns the information that is returned by the application server to the user.

An example of the returned response is as follows:

```
HTTP/1.1 200 OK
Date: Mon, 14 Sep 2015 12:37:27 GMT
Content-Type: application/json
Content-Length: 9
Connection: keep-alive
ETag: "D8E8FCA2DC0F896FD7CB4CB0031BA249"
Server: AliyunOSS
x-oss-bucket-version: 1442231779
x-oss-request-id: 55F6BF87207FB30F2640C548
{"a":"b"}
```

Note

- The body of responses for some requests such as CompleteMultipartUpload contains content, such as information in XML format. If you use the upload callback function, the original body content is overwritten such as `{"a":"b"}`. Exercise caution when you implement upload callback.
- If the upload callback fails, HTTP status code 203 is returned with error code CallbackFailed. This response indicates that the object is successfully uploaded to OSS, but the callback fails. A callback failure only indicates that OSS does not receive the expected callback response. It does not indicate that the application server does not receive a callback request. For example, a callback failure will occur if the response returned by the application server is not in JSON format.

2.4.1.7.15. RestoreObject

You can call this operation to restore archived objects.

Versioning

Different versions of an object may have different storage classes. By default, the RestoreObject operation restores the current version of an object. To restore a specific version of the object, specify the version ID.

Note

- The RestoreObject operation applies only to archived objects. This operation does not apply to standard or Infrequent Access (IA) objects.
- When the RestoreObject operation is called on an object for the first time, HTTP status code 202 is returned.
- When you call the RestoreObject operation that was called on a restored object, 200 OK is returned.

Restore archived objects

The status of an archived object throughout the restoration process is described as follows:

1. By default, the archived object is in the frozen state.
2. After you submit a restoration request, the object is in the restoring state. It takes about one minute to four hours to complete the restoration task.
3. After the server completes the restoration task, the object enters the restored state and you can read the object. By default, the restored state lasts 24 hours and can be extended by another 24 hours after you call RestoreObject again. During one restoration process, RestoreObject can be called on an object for up to seven times. In other words, an object can remain in the restored state for up to seven days.
4. After the restored state expires, the object returns to the frozen state.

Billing

The fees generated when an object is converted between different states are described as follows:

- Data retrieval fees are generated when the restore operation is performed on a frozen object.
- The restored state can be extended to up to seven days. During this period, data retrieval fees are not generated.
- After the restored state expires, the object returns to the frozen state. Data retrieval fees are generated if you perform the restore operation on the object again.

Request syntax

```
POST /ObjectName? restore HTTP/1.1
Host: archive-bucket.oss-cn-hangzhou.aliyuncs.com
Date: GMT Date
Authorization: SignatureValue
```

Examples

- Submit a restoration request for a frozen object

  Sample requests

  ```
  POST /oss.jpg? restore HTTP/1.1
  Host: oss-archive-example.oss-cn-hangzhou.aliyuncs.com
  Date: Sat, 15 Apr 2017 07:45:28 GMT
  Authorization: OSS e1Unnbm1rgdnpI:y4eyu+4yje5ioRCr****
  ```

  Sample success responses

  ```
  HTTP/1.1 202 Accepted
  Date: Sat, 15 Apr 2017 07:45:28 GMT
  Content-Length: 0
  Connection: keep-alive
  Server: AliyunOSS
  x-oss-request-id: 5374A2880232A65C23002D74
  ```

- Submit a restoration request for a restoring object

  Sample requests

  ```
  POST /oss.jpg? restore HTTP/1.1
  Host: oss-archive-example.oss-cn-hangzhou.aliyuncs.com
  Date: Sat, 15 Apr 2017 07:45:29 GMT
  Authorization: OSS e1Unnbm1rgdnpI:21qtGJ+ykDVmdy4eyu+N****
  ```

  Sample success responses

```
HTTP/1.1 409 Conflict
Date: Sat, 15 Apr 2017 07:45:29 GMT
Content-Length: 556
Connection: keep-alive
Server: AliyunOSS
x-oss-request-id: 5374A2880232A65C23002D74
<? xml version="1.0" encoding="UTF-8"? >
<Error>
 <Code>RestoreAlreadyInProgress</Code>
 <Message>The restore operation is in progress. </Message>
 <RequestId>58EAF141461FB42C2B000008</RequestId>
 <HostId>10.101.200. ***</HostId>
</Error>
```

- Submit a restoration request for a restored object

  Sample requests

```
POST /oss.jpg? restore HTTP/1.1
Host: oss-archive-example.oss-cn-hangzhou.aliyuncs.com
Date: Sat, 15 Apr 2017 07:45:29 GMT
Authorization: OSS e1Unnbm1rgdnpI:u6O6FMJnn+WuBwbByZxm1+y4eyu+N****
```

  Sample success responses

```
HTTP/1.1 200 Ok
Date: Sat, 15 Apr 2017 07:45:30 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
x-oss-request-id: 5374A2880232A65C23002D74
```

- Specify the version ID when you call the restore operation on an object in a versioning-enabled bucket.

  Sample requests

```
POST /oss.jpg? restore&versionId=CAEQNRiBgMClj7qD0BYiIDQ5Y2QyMjc3NGZkODRlMTU5M2VkY2U3MW
RiNGRh**** HTTP/1.1
Host: oss-archive-example.oss-cn-hangzhou.aliyuncs.com
Date: Tue, 09 Apr 2019 06:50:48 GMT
Authorization: OSS o3shiyktjw16xw1:2JND5qqlAlaA1/kLO4kBbGTw****
```

  Sample success responses

```
HTTP/1.1 202 Accepted
Date: Tue, 09 Apr 2019 06:50:48 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
x-oss-version-id: CAEQNRiBgMClj7qD0BYiIDQ5Y2QyMjc3NGZkODRlMTU5M2VkY2U3MWRiNGRh****
x-oss-request-id: 5CAC40C8B7AEADE017000653
```

SDKs

The SDKs of the RestoreObject operation for various programming languages are as follows:

- Java
- Python
- PHP
- Go
- C
- .NET

Error codes

Error code	HTTP status code	Description
NoSuchKey	404	The error message returned because the requested object does not exist.
OperationNotSupported	400	The error message returned because the storage class of the requested object is not Archive.
RestoreAlreadyInProgress	409	The error message returned because the RestoreObject operation is called and the server is performing the restore operation. Do not call RestoreObject repeatedly.

2.4.1.7.16. SelectObject

You can call this operation to execute the SQL statement on the target object and obtain the query result.

> Note
>
> - You must have the read permissions on the object.
> - HTTP status code 206 is returned if the operation is successfully performed. If the SQL statements are not valid or cannot match any objects, HTTP status code 400 is returned.
> - For more information about the functions of SelectObject, see SelectObject in OSS Developer Guide.

Request syntax

Request syntax for either CSV or JSON objects.

- Request syntax for CSV objects

```
POST /object? x-oss-process=csv/select HTTP/1.1
HOST: BucketName.oss-cn-hangzhou.aliyuncs.com
Date: time GMT
Content-Length: ContentLength
Content-MD5: MD5Value
Authorization: Signature
<? xml version="1.0" encoding="UTF-8"? >
<SelectRequest>
  <Expression>base64 encode(Select * from OSSObject where ...) </Expression>
  <InputSerialization>
    <CompressionType>None|GZIP</CompressionType>
    <CSV>
      <FileHeaderInfo>
        NONE|IGNORE|USE
      </FileHeaderInfo>
      <RecordDelimiter>base64 encode</RecordDelimiter>
      <FieldDelimiter>base64 encode</FieldDelimiter>
      <QuoteCharacter>base64 encode</QuoteCharacter>
      <CommentCharacter>base64 encode</CommentCharacter>
      <Range>line-range=start-end|split-range=start-end</Range>
      <AllowQuotedRecordDelimiter>true|false</AllowQuotedRecordDelimiter>
    </CSV>
    </InputSerialization>
    <OutputSerialization>
       <CSV>
       <RecordDelimiter>base64 encode</RecordDelimiter>
       <FieldDelimiter>base64 encode</FieldDelimiter>

      </CSV>
      <KeepAllColumns>false|true</KeepAllColumns>
      <OutputRawData>false|true</OutputRawData>
      <EnablePayloadCrc>true</EnablePayloadCrc>
      <OutputHeader>false</OutputHeader>
  </OutputSerialization>
 <Options>
   <SkipPartialDataRecord>false</SkipPartialDataRecord>
   <MaxSkippedRecordsAllowed>
   max allowed number of records skipped
   </MaxSkippedRecordsAllowed>
```

```
    </Options>
</SelectRequest>
```

- Request syntax for JSON objects

```
POST /object? x-oss-process=json/select HTTP/1.1
HOST: BucketName.oss-cn-hangzhou.aliyuncs.com
Date: time GMT
Content-Length: ContentLength
Content-MD5: MD5Value
Authorization: Signature
<? xml  version="1.0"  encoding="UTF-8"? >
<SelectRequest>
  <Expression>
    Base64 encode of sql such as (select * from ossobject)
  </Expression>
  <InputSerialization>
    <CompressionType>None|GZIP</CompressionType>
    <JSON>
      <Type>DOCUMENT|LINES</Type>
      <Range>
      line-range=start-end|split-range=start-end
      </Range>
      <ParseJsonNumberAsString> true|false
      </ParseJsonNumberAsString>
    </JSON>
  </InputSerialization>
  <OutputSerialization>
    <JSON>
      <RecordDelimiter>
        Base64 of record delimiter
      </RecordDelimiter>
    </JSON>
    <OutputRawData>false|true</OutputRawData>
        <EnablePayloadCrc>true</EnablePayloadCrc>
  </OutputSerialization>
  <Options>
    <SkipPartialDataRecord>
      false|true
    </SkipPartialDataRecord>
    <MaxSkippedRecordsAllowed>
      max allowed number of records skipped
     </MaxSkippedRecordsAllowed>
    </Options>
</SelectRequest>
```

Request elements

Element	Type	Description
SelectRequest	Container	Specifies the container that stores the SelectObject request. Child node: Expression, InputSerialization, and OutputSerialization Parent node: none
Expression	String	The Base64-encoded SQL statement. Child node: none Parent node: SelectRequest
InputSerialization	Container	Optional. This element specifies the input serialization parameters. Child node: CompressionType, CSV, and JSON Parent node: SelectRequest
OutputSerialization	Container	Optional. This element specifies the output serialization parameters. Child node: CSV, JSON, and OutputRawData Parent node: SelectRequest
CSV(InputSerialization)	Container	Optional. This element specifies the input serialization parameters when the CSV object is queried. Child node: FileHeaderInfo, RecordDelimiter, FieldDelimiter, QuoteCharacter, CommentCharacter, and Range Parent node: InputSerialization
CSV(OutputSerialization)	Container	Optional. This element specifies the output serialization parameters when the CSV object is queried. Child node: RecordDelimiter and FieldDelimiter Parent node: OutputSerialization
JSON(InputSerialization)	Container	Optional. This element specifies the input serialization parameters when the JSON object is queried. Child node: Type, Range, and ParseJsonNumberAsString

Element	Type	Description
JSON(OutputSerialization)	Container	Optional. This element specifies the output serialization parameters when the JSON object is queried. Child node: RecordDelimiter
Type	Enumeration	Specifies the type of the input JSON object: DOCUMENT or LINES.
OutputRawData	Boolean (false by default)	Optional. This element specifies the output data as raw data. Child node: none Parent node: OutputSerialization Note • If OutputRawData is specified in the request, OSS returns data accordingly. • If OutputRawData is not specified in the request, OSS automatically selects a format and returns it in the response. • If OutputRawData is set to True and the SQL statement takes a long time to return data, the HTTP request may time out.
CompressionType	Enumeration	Specifies the compression type of the object: None|GZIP. Child node: none Parent node: InputSerialization

Element	Type	Description
FileHeaderInfo	Enumeration	Optional. This element specifies the header information of the CSV object. Valid values: • Use: indicates that the CSV object contains header information. You can use the column name in the CSV object as the column name in the SelectObject operation. • Ignore: indicates that the CSV object contains header information. However, you cannot use the column name in the CSV object as the column name in the SelectObject operation. • None: the default value, indicating that the CSV object does not contain header information. Child node: none Parent node: CSV (input)
RecordDelimiter	String	Optional. This element specifies a Base64-encoded delimiter. Default value: `\n`. The value of this element before being encoded can be an ANSI value of up to two characters in length. For example, `\n` is used to indicate a line break in Java code. Child node: none Parent node: CSV (input and output) and JSON (output)
FieldDelimiter	String	Optional. This element specifies a Base64-encoded delimiter used to separate columns in the CSV object. Default value: `,`. The value of this element before being encoded must be a one-character ANSI value. For example, `,` is used to indicate a comma in Java code. Child node: none Parent node: CSV (input and output)

Element	Type	Description
QuoteCharacter	String	Optional. This element specifies a Base64-encoded quote character used in the CSV object. Default value: `\"`. In a CSV object, line breaks and column delimiters enclosed in quotation marks are processed as normal characters. The value of this element before being encoded must be a one-character ANSI value. For example, `\"` is used to indicate a quote character in Java code. Child node: none Parent node: CSV (input)
CommentCharacter	String	Specifies the comment character used in the CSV object. The value of this element must be Base64-encoded. The default value is null.
Range	String	Optional. This element specifies the query range. The following two query methods are supported: Note Select Meta must be created for objects that are queried based on Range. For more information about Select Meta, see CreateSelectObjectMeta. • Query by row: line-range=start-end. For example, line-range=10-20 indicates that rows 10 to 20 will be scanned. • Query by split: split-range=start-end. For example, split-range=10-20 indicates that splits 10 to 20 will be scanned. The start and end parameters of the preceding functions are both inclusive. The two preceding parameters have the same format as that of the range parameter in the range get function. This parameter can only be used when the object is in CSV format or when the JSON Type is LINES. Child node: none Parent node: CSV (input) and JSON (output)

Element	Type	Description
KeepAllColumns	Boolean	Optional. A value of true indicates that all columns in the CSV object are included in the returned result. The default value is false. However, only columns included in the SELECT clause have values. The columns in the returned result are sorted in ascending order of the column numbers. For example: `select _5, _1 from ossobject.` If you set KeepAllColumn to true and six columns are included in the CSV object, the following result is returned for the preceding SELECT clause: Value of 1st column,,,,Value of 5th column,\n Child node: none Parent node: OutputSerialization (CSV)
EnablePayloadCrc	Boolean	Indicates that each frame includes a CRC-32 value for verification. The client can calculate the CRC-32 value of each payload and compare it with the included CRC-32 value to verify data integrity. Child node: none Parent node: OutputSerialization
Options	Container	Specifies other optional parameters. Type: container Child node: SkipPartialDataRecord and MaxSkippedRecordsAllowed Parent node: SelectRequest
OutputHeader	Boolean	A value of true indicates that the header information of the CSV object is included in the beginning of the returned result. Type: Boolean. Default value: false. Child node: none Parent node: OutputSerialization

Element	Type	Description
SkipPartialDataRecord	Boolean	Specifies whether to ignore rows without data. If this parameter is set to false, OSS will process the row data as null without reporting errors. If this parameter is set to true, rows without data are skipped. If the number of skipped rows has exceeded the maximum allowed number, OSS reports an error and stops processing the data. Type: Boolean. Default value: false. Child node: none Parent node: Options
MaxSkippedRecordsAllowed	Int	Specifies the maximum allowed number of skipped rows. If a row does not match the type specified in the SQL statement, or if one or more columns in a row are missing and the value of SkipPartialDataRecord is True, the row is skipped. If the number of skipped rows has exceeded the value of this parameter, OSS reports an error and stops processing the data. Note If a row in a CSV object is not properly formatted, OSS stops processing the data and reports an error because this format error may result in incorrect resolution to the CSV object. For example, a column in the row includes continual odd numbered quote characters. This parameter can be used to adjust the tolerance for irregular data but cannot be applied to invalid CSV objects. Type: int. Default value: 0. Child node: none Parent node: Options

Element	Type	Description
ParseJsonNumberAsString	Boolean	Parses integer and floating-point numbers in a JSON object into strings. The precision of floating-point numbers in a JSON object degrades when the numbers are parsed. Therefore, we recommend that you set the value of this parameter to true if you want to retain the raw data. To use the parsed numbers in calculations, you can use the CAST function in an SQL statement to convert the parsed data into the required type, such as int, double, or decimal. Default value: false Child node: none Parent node: JSON
AllowQuotedRecordDelimiter	Boolean	Specifies whether the CSV object contains line breaks in quotation marks ("). For example, the value of a column is "abc\ndef" and \n is a line break, you must set this value to true. If this parameter is set to false, SelectObject allows you to specify a range in the request header for more efficient multipart query. Default value: true Child node: none Parent node: InputSerialization

Response body

- If the HTTP status code included in the response is 4xx, it indicates that the request has not passed the SQL syntax check or that the request contains error. In this case, the body format of the returned error message is the same as that of the error message returned for a GetObject request.
- If the HTTP status code included in the response is 5xx, it indicates that an error occurs in the server. In this case, the body format of the returned error message is the same as that of the error message returned for a GetObject request.
- HTTP status code 206 is returned when the operation is successfully performed. In this case:
  - If the value of header x-oss-select-output-raw is true, it indicates that the object data (not including frame-based data) was successfully returned. The client can obtain the data in the same manner as the GetObject operation.
  - If the value of x-oss-select-output-raw is false, the result is returned as frames.
- A returned frame is in `Version|Frame-Type | Payload Length | Header Checksum | Payload | Payload Checksum<1 byte><--3 bytes--><---4 bytes----><-------4 bytes--><variable><----4bytes----------->` format.

Note The Checksum is CRC-32 in all frames. All integers in a frame are big-endian. Currently, the value of Version is 1.

Frame type

The following table describes three frame types supported by SelectObject.

Frame type	Value	Payload format	Description
Data Frame	8388609	offset | data<-8 bytes> <---variable->	A data frame includes the data returned for the SelectObject request. The offset parameter is an 8-bit integer that indicates the current scanning location (the offset from the file header) and is used to report the progress of the operation.
Continuous Frame	8388612	offset<----8 bytes-->	A continuous frame is used to report the progress of an operation and keep an HTTP connection. If no data is returned for a query request within 5 seconds, a continuous frame is returned.

Frame type	Value	Payload format	Description
End Frame	8388613	offset | total scanned bytes | http status code | error message<--8bytes-><--8bytes--------><----4 bytes--------><-variable------>	An end frame is used to return the final status of an operation, including the scanned bytes and the possible error messages. • The offset parameter indicates the final location offset after scanning. • The total scanned bytes parameter indicates the size of the scanned data. • The http status code parameter indicates the final status of the operation. Note SelectObject is a stream operation. Only the first data block is processed when the response header is sent. If the first data block matches the SQL statement, the HTTP status code in the response header is 206, which indicates that the operation was successful. However, the final status code may not be 206 because the subsequent data blocks may be invalid. The status code in the response header cannot be modified. Therefore, HTTP status code is included in the end frame to indicate the final status of the operation. The client uses the status code included in the end frame to determine whether the operation is successful. • The error message parameter includes error messages, including the number of each skipped row and the total number of skipped rows. Note The format of error messages included in an end frame is `ErrorCodes.DetailMessage`. The ErrorCodes section contains one or more ErrorCodes separated by commas (,). The ErrorCodes and DetailMessage are separated by a period (.).

Sample requests

Sample requests for either CSV or JSON objects.

- Sample request for CSV objects

```
POST /oss-select/bigcsv_normal.csv? x-oss-process=csv%2Fselect HTTP/1.1
Date: Fri, 25 May 2018 22:11:39 GMT
Content-Type:
Authorization: OSS LTAIJPLocA0fD:FC/9JRbBGRw4o2QqdaL246Px****
User-Agent: aliyun-sdk-dotnet/2.8.0.0(windows 16.7/16.7.0.0/x86;4.0.30319.42000)
Content-Length: 748
Expect: 100-continue
Connection: keep-alive
Host: host name
<? xml version="1.0"? >
<SelectRequest>
  <Expression>c2VsZWN0IGNvdW50KCopIGZyb20gb3Nzb2JqZWN0IHdoZXJlIF80ID4gNDU=
  </Expression>
  <InputSerialization>
    <Compression>None</Compression>
    <CSV>
      <FileHeaderInfo>Ignore</FileHeaderInfo>
      <RecordDelimiter>Cg==</RecordDelimiter>
      <FieldDelimiter>LA==</FieldDelimiter>
      <QuoteCharacter>Ig==</QuoteCharacter>
      <CommentCharacter>Iw==</CommentCharacter/>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <RecordDelimiter>Cg==</RecordDelimiter>
      <FieldDelimiter>LA==</FieldDelimiter>
      <QuoteCharacter>Ig==</QuoteCharacter>
    </CSV>
    <KeepAllColumns>false</KeepAllColumns>
      <OutputRawData>false</OutputRawData>
  </OutputSerialization>
</SelectRequest>
```

- Sample request for JSON objects

```
POST /oss-select/sample_json.json? x-oss-process=json%2Fselect HTTP/1.1
Host: host name
Accept-Encoding: identity
User-Agent: aliyun-sdk-python/2.6.0(Darwin/16.7.0/x86_64;3.5.4)
Accept: */*
Connection: keep-alive
date: Mon, 10 Dec 2018 18:28:11 GMT
authorization: OSS AccessKeySignature
Content-Length: 317
<SelectRequest>
  <Expression>c2VsZWN0ICogZnJvbSBvc3NvYmplY3Qub2JqZWN0c1sqXSB3aGVyZSBwYXJ0eSA9ICdEZW1
vY3JhdCc=
  </Expression>
  <InputSerialization>
  <JSON>
    <Type>DOCUMENT</Type>
  </JSON>
  </InputSerialization>
  <OutputSerialization>
  <JSON>
    <RecordDelimiter>LA==</RecordDelimiter>
  </JSON>
  </OutputSerialization>
  <Options />
</SelectRequest>
```

Regular expressions in an SQL statement

The regular expression in an SQL statement is `SELECT select-list from table where_opt limit_opt` .

> **Note** SELECT, OSSOBJECT, and WHERE are keywords that cannot be modified.

```
select_list: column name
        | column index (example: _1, _2. column index applies only to CSV objects)
        | json path (example: s.contacts.firstname. json path applies only to JSON objects)
        | function(column index | column name)
        | function(json_path) (applies only to JSON objects)
        | select_list AS alias
```

> **Note** The following functions are supported: AVG, SUM, MAX, MIN, COUNT, and CAST (type conversion function). You can use only the wildcard (*) after COUNT.

table: OSSOBJECT

| OSSOBJECT json_path (applies only to JSON objects)

For CSV objects, the table must be OSSOBJECT. For JSON objects (including DOCUMENT and LINES type objects), you can specify a json_path after OSSOBJECT.

json_path: ['string '] (The quotation marks around string can be deleted if the string does not include a space or a wildcard (*). In this case, ['string '] is equivalent to .'string '.

| [n] (Used to indicate the nth element in an array. The value of 0 is counted from 0.)

| [*] (Used to indicate any child element in an array or object.)

| .'string ' (The quotation marks around string can be deleted if the string does not include a space or a wildcard (*).)

| json_path jsonpath (You can concatenate multiple elements in a json path, such as [n].property1.attributes[*].)

Where_opt:
| WHERE expr
expr:
| literal value
| column name
| column index
| json path (applies only to JSON objects)
| expr op expr
| expr OR expr
| expr AND expr
| expr IS NULL
| expr IS NOT NULL
| (column name | column index | json path) IN (value1, value2,...)
| (column name | column index | json path) NOT in (value1, value2,...)
| (column name | column index | json path) between value1 and value2
| NOT (expr)
| expr op expr
| (expr)
| cast (column index |column name | json path | literal as INT|DOUBLE|)

- op: includes the following operators: `>`, `<`, `>=`, `<=`, `!=`, `=`, `,`, `LIKE`, `+`, `-`, `*`, `/`, `%`, and `||`.
- cast: You can use the CAST function to convert data in a column from one type into another.
- The combination of an aggregation function and limit: `Select avg(cast(_1 as int)) from ossobject limit 100`. The preceding statement calculates the average values of the first columns in the first 100 rows. This function differs from the MySQL statement because only a single row is returned for an aggregation function in SelectObject operations. This makes it unnecessary to limit the output. Limit is performed before aggregation functions in SelectObject operations.

Limits for SQL statements

Limits for SQL statements are as follows:

- Only text objects encoded in UTF-8 and UTF-8 text objects compressed in GZIP format are supported. The deflate format is not supported for GZIP objects.
- An SQL statement can only query a single object. The following clauses are not supported: JOIN, ORDER BY, GROUP BY, and HAVING.
- A WHERE clause cannot include aggregation conditions. For example, the following clause is not allowed: WHERE max(cast(age as int)) > 100.
- A maximum of 1,000 columns can be specified for an SQL statement. The column name in an SQL statement can be up to 1,024 bytes in length.
- A maximum of five wildcards (%) are supported in a LIKE clause. Both the percent sign (%) and the asterisk (*) are wildcards that represent zero or more characters. The ESCAPE keyword is supported in SQL LIKE clauses, and is used to escape the special characters, such as percent signs (%), asterisks (*), and question marks (?), into normal strings.
- A maximum of 1,024 constants are supported in an IN clause.
- The Projection after SELECT can be a column name, a CSV column index (such as _1 and _2), an aggregation function, or a CAST function. Other expressions are not supported, such as select _1 + _2 from ossobject.
- The maximum column size and row size for a CSV object are 256 KB.
- The json path after FROM supports a JSON node with a maximum size of 512 KB. The path can contain up to 10 levels, and an array can contain a maximum of 5,000 elements. The fields after SELECT and WHERE must be from the nodes corresponding to the json path after FROM.
- In SQL statements for a JSON object, the SELECT or WHERE expressions cannot include the array wildcard ([*]). The array wildcard ([*]) can only be included in the json path after FROM. For example, select * from ossobject.contacts[*] instead of select s.contacts[*] from ossobject s is supported.
- The maximum size of an SQL statement is 16 KB. A maximum of 20 expressions can be added after WHERE. Each statement supports up to 10 levels and 100 aggregation operations.

Data error handling

The following section lists common methods for handling data errors.

- Some columns are missing in some rows in a CSV object.

  If the value of SkipPartialDataRecord is not specified or is set to False, OSS calculates the expressions in the SQL statement by processing the values of the missing columns as null.

If the value of SkipPartialDataRecord is set to True, OSS ignores the rows in which some columns are missing. In this case, if the value of MaxSkippedRecordsAllowed is not specified or is set to a value smaller than the number of skipped rows, OSS reports an error by sending HTTP status code 400 or including status code 400 in the end frame.

Assume that the SQL statement is `select _1, _3 from ossobject` and the data in a row of the CSV object is "John, company A".

- If the value of SkipPartialDataRecord is set to False, "John,\n" is returned.
- If the value of SkipPartialDataRecord is set to True, this row is skipped.

- Some keys are missing in a JSON object.

  Some objects in the JSON object may not include the keys specified in the SQL statement.

  - If the value of SkipPartialDataRecord is not specified or is set to False, OSS calculates the expressions in the SQL statement by processing the missing keys as null.
  - If the value of SkipPartialDataRecord is True, OSS skips the data in the JSON node. In this case, if the value of MaxSkippedRecordsAllowed is not specified or is set to a value smaller than the number of skipped rows, OSS reports an error by sending HTTP status code 400 or including status code 400 in the end frame.

  Assume that the SQL statement is `select s.firstName, s.lastName , s.age from ossobject.contacts[*] s` and the value of a JSON node is {"firstName":"John", "lastName":"Smith"}.

  - If the value of SkipPartialDataRecord is not specified or is set to False, {"firstName":"John", "lastName":"Smith"} is returned.
  - If the value of SkipPartialDataRecord is set to True, this row is skipped.

Note For keys in the returned data of a request for JSON objects, the output JSON objects can only be LINES. The Key value in the output result is determined based on the following rules.

- Assume that the SQL statement is `select * from ossobject...`. If * corresponds to a JSON object ({...}), it is returned. If * corresponds to a String or an Array, it is returned as a DummyKey _1.

  When the data is {"Age":5} `select * from ossobject.Age s where s = 5`, {"_1":5} is returned because 5 that corresponds to * is not a JSON object. When the SQL statement is `select * from ossobject s where s.Age = 5`, {"Age":5} corresponding to * is returned.

- If the SQL statement does not use select * but specifies columns, the returned content is in `{"{Column 1}": Value, "{Column 2}": Value...}` format. {Column n} can be generated in the following ways:
  - If the Alias of the column is specified in the SELECT clause, the Alias applies.
  - If the column is the key of a JSON object, this key is used as the output key value.
  - If the column is an element of a JSON array or an aggregate function, prefix the column with serial number (starting from 1) plus _ as the output key value.

  Assume that the data is {"contacts":{"Age":35, "Children":["child1", "child2", "child3"]}}:

  - When the SQL statement is `select s.contacts.Age, s.contacts.Children[0] from ossobject`, Age is the key of the input JSON object, and Children[0] indicates the first element of Children of the array type and is the second column in the output content. {"Age":35, "_2":"child1"} is returned.
  - When the SQL statement is `select max(cast(s.Age as int)) from ossobject.contacts s`, and the selected column is an aggregate function, the column is prefixed with _ *1* plus its serial number in the output. {"_1":35} is returned.
  - When the Alias of the column is specified in the SQL statement `select s.contacts.Age, s.contacts.Children[0] as firstChild from ossobject`, {"Age":35, "firstChild":"child1"} is returned.

- Keys matching in JSON objects and SQL statements are case-sensitive. For example, "select s. Age" and "select s. age" are different.

- **The data type of some columns in a CSV object does not match the SQL statement.**

  If the data type of a row in a CSV object does not match the type specified in the SQL statement, the row is skipped. If the number of skipped rows has exceeded the value of MaxSkippedRecordsAllowed, OSS stops processing data and returns HTTP status code 400.

  Assume that the SQL statement is `select _1, _3 from ossobject where _3 > 5`. If the value of a row in the CSV object is `John, Company A, To be hired`, this row is skipped because the third column in the row is not of the integer type.

- **The data type of some keys in a JSON object does not match the SQL statement.**

Assume that the SQL statement is `select s.name from ossobject s where s.aliren_age > 5`. If the value of a JSON node is `{"Name":"John", "aliren_age":To be hired}`, this node is skipped.

CreateSelectObjectMeta

You can call this operation to obtain information about the target CSV object, such as the total number of rows, the total number of columns in CSV objects, and the number of splits. If the information does not exist in the object, the whole CSV object is scanned to analyze and record the preceding information. The information obtained in the first API call is used when the API is called again, so that the entire CSV object does not need to be scanned again.

> **Note**
>
> - You must have the write permissions on the target object before performing the CreateSelectObjectMeta operation.
> - HTTP status code 200 is returned if the operation is successfully performed. If the target object is not a valid CSV or JSON LINES object, or the specified delimiter does not match any CSV objects, HTTP status code 400 is returned.

- Request syntax
  - Request syntax for CSV objects

```
POST  /samplecsv? x-oss-process=csv/meta
<CsvMetaRequest>
  <InputSerialization>
    <CompressionType>None</CompressionType>
    <CSV>
      <RecordDelimiter>base64 encode</RecordDelimiter>
      <FieldDelimiter>base64 encode</FieldDelimiter>
      <QuoteCharacter>base64 encode</QuoteCharacter>
    </CSV>
  </InputSerialization>
  <OverwriteIfExists>false|true</OverwriteIfExists>
</CsvMetaRequest>
```

- Request syntax for JSON objects

```
POST  /samplecsv? x-oss-process=json/meta
<JsonMetaRequest>
  <InputSerialization>
    <CompressionType>None</CompressionType>
    <JSON>
      <Type>LINES</Type>
    </JSON>
  </InputSerialization>
  <OverwriteIfExists>false|true</OverwriteIfExists>
</JsonMetaRequest>
```

- Request elements

Element	Type	Description
CsvMetaRequest	Container	Specifies the container that stores the Select csv Meta request. Child node: InputSerialization Parent node: none
JsonMetaRequest	Container	Specifies the container that stores the Select json Meta request. Child node: InputSerialization Parent node: none
InputSerialization	Container	Optional. This element specifies the input serialization parameters. Child node: CompressionType, CSV, and JSON Parent node: CsvMetaRequest and JsonMetaRequest
OverwriteIfExists	Boolean	Optional. This element specifies whether to recalculate the SelectMeta and overwrite the existing data. A value of false indicates that the result is directly returned if the Select Meta already exists. The default value is false. Child node: none Parent node: CsvMetaRequest and JsonMetaRequest

Element	Type	Description
CompressionType	Enumeration	Optional. This element specifies the compression type of the object. Only None is supported currently. Child node: none Parent node: InputSerialization
RecordDelimiter	String	Optional. This element specifies a Base64-encoded delimiter used to separate rows in the CSV object. The default value is \n. The value of this element before being encoded can be an ANSI value of up to two characters. For example, *\n* is used to indicate a line break in Java code. Child node: none Parent node: CSV
FieldDelimiter	String	Optional. This element specifies a Base64-encoded delimiter used to separate columns in the CSV object. Default value: `,`. The value of this element before being encoded must be a one-character ANSI value. For example, `,` is used to indicate a comma in Java code. Child node: none Parent node: CSV (input and output)
QuoteCharacter	String	Optional. This element specifies a Base64-encoded quote character used in the CSV object. Default value: \". In a CSV object, line breaks and column delimiters enclosed in quotation marks are processed as normal characters. The value of this element before being encoded must be a one-character ANSI value. For example, \"is used to indicate a quote character in Java code. Child node: none Parent node: CSV (input)
CSV	Container	Specifies the format of the input CSV object. Child node: RecordDelimiter, FieldDelimiter, and QuoteCharacter Parent node: InputSerialization

Element	Type	Description
JSON	Container	Specifies the format of the input JSON object. Child node: Type Parent node: InputSerialization
Type	Enumeration	Specifies the type of the JSON object. Valid values: LINES

- Response body

  Similar to SelectObject, the results for CreateSelectObjectMeta are also returned as frames.

Frame type	Value	Payload format	Description
Meta End Frame (CSV)	8388614	offset | total scanned bytes | status| splits count | rows count | columns count | error message <-8 bytes><------8 bytes-------><--4bytes><--4 bytes--><--8 bytes><--4 bytes---><variable size>	Reports the final status of the CreateSelectObjectMeta operation. ◦ offset: an 8-bit integer, indicates the offset when the scanning is complete. ◦ total scanned bytes: an 8-bit integer, indicates the size of the scanned data. ◦ status: a 4-bit integer, indicates the final status of the operation. ◦ splits_count: a 4-bit integer, indicates the total number of splits. ◦ rows_count: an 8-bit integer, indicates the total number of rows. ◦ cols_count: a 4-bit integer, indicates the total number of columns. ◦ error_message: includes detailed error messages. If no error occurs, the value of this parameter is null.

Frame type	Value	Payload format	Description
Meta End Frame (JSON)	8388615	offset | total scanned bytes | status| splits count | rows count | error message <-8 bytes><------8 bytes------><--4bytes><--4 bytes--><--8 bytes><variable size>	Reports the final status of the CreateSelectObjectMeta operation. ○ offset: an 8-bit integer, indicates the offset when the scanning is complete. ○ total scanned bytes: an 8-bit integer, indicates the size of the scanned data. ○ status: a 4-bit integer, indicates the final status of the operation. ○ splits_count: a 4-bit integer, indicates the total number of splits. ○ rows_count: an 8-bit integer, indicates the total number of rows. ○ error_message: includes detailed error messages. If no error occurs, the value of this parameter is null.

- Sample requests

- Sample request for CSV objects

```
POST /oss-select/bigcsv_normal.csv? x-oss-process=csv%2Fmeta HTTP/1.1
Date: Fri, 25 May 2018 23:06:41 GMT
Content-Type:
Authorization: OSS AccessKeySignature
User-Agent: aliyun-sdk-dotnet/2.8.0.0(windows 16.7/16.7.0.0/x86;4.0.30319.42000)
Content-Length: 309
Expect: 100-continue
Connection: keep-alive
Host: Host
<? xml version="1.0"? >
<CsvMetaRequest>
  <InputSerialization>
    <CSV>
      <RecordDelimiter>Cg==</RecordDelimiter>
      <FieldDelimiter>LA==</FieldDelimiter>
      <QuoteCharacter>Ig==</QuoteCharacter>
    </CSV>
  </InputSerialization>
  <OverwriteIfExisting>false</OverwriteIfExisting>
</CsvMetaRequest>
```

- Sample request for JSON objects

```
POST /oss-select/sample.json? x-oss-process=json%2Fmeta HTTP/1.1
Date: Fri, 25 May 2018 23:06:41 GMT
Content-Type:
Authorization: OSS AccessKeySignature
User-Agent: aliyun-sdk-dotnet/2.8.0.0(windows 16.7/16.7.0.0/x86;4.0.30319.42000)
Content-Length: 309
Expect: 100-continue
Connection: keep-alive
Host: Host
<? xml version="1.0"? >
<JsonMetaRequest>
  <InputSerialization>
    <JSON>
      <Type>LINES</Type>
    </JSON>
  </InputSerialization>
  <OverwriteIfExisting>false</OverwriteIfExisting>
</JsonMetaRequest>
```

Supported time formats

You can convert any of the following listed formats into a timestamp without specifying the time format. For example, the string cast('20121201' as timestamp) is automatically parsed as a timestamp: December 1, 2012.

The following table describes the recognized time formats.

Format	Description
YYYYMMDD	year month day
YYYY/MM/DD	year/month/day
DD/MM/YYYY/	day/month/year
YYYY-MM-DD	year-month-day
DD-MM-YY	day-month-year
DD.MM.YY	day.month.year
HH:MM:SS.mss	hour:minute:second.millisecond
HH:MM:SS	hour:minute:second
HH MM SS mss	hour minute second millisecond

Format	Description
HH.MM.SS.mss	hour. minute. second.millisecond
HHMM	hour minute
HHMMSSmss	hour minute second millisecond
YYYYMMDD HH:MM:SS.mss	year month day hour:minute:second.millisecond
YYYY/MM/DD HH:MM:SS.mss	year/month/day hour:minute:second.millisecond
DD/MM/YYYY HH:MM:SS.mss	day/month/year hour:minute:second.millisecond
YYYYMMDD HH:MM:SS	year month day hour:minute:second
YYYY/MM/DD HH:MM:SS	year/month/day hour:minute:second
DD/MM/YYYY HH:MM:SS	day/month/year hour:minute:second
YYYY-MM-DD HH:MM:SS.mss	year-month-day hour:minute:second.millisecond
DD-MM-YYYY HH:MM:SS.mss	day-month-year hour:minute:second.millisecond
YYYY-MM-DD HH:MM:SS	year-month-day hour:minute:second
YYYYMMDDTHH:MM:SS	year month day T hour:minute:second
YYYYMMDDTHH:MM:SS.mss	year month day T hour:minute:second.millisecond
DD-MM-YYYYTHH:MM:SS.mss	day-month-year T hour:minute:second.millisecond
DD-MM-YYYYTHH:MM:SS	day-month-year T hour:minute:second
YYYYMMDDTHHMM	year month day T hour minute
YYYYMMDDTHHMMSS	year month day T hour minute second
YYYYMMDDTHHMMSSMSS	year month day T hour minute second millisecond
ISO8601-0	year-month-day T hour:minute+hour:minute, or year-month-day T hour:minute-hour:minute "+" indicates that the time in the current time zone is ahead of standard UTC time. "-" indicates that the time in the current time zone is behind the standard UTC time. In this format, ISO 8601-0 can be used.

Format	Description
ISO8601-1	year-month-day T hour:minute+hour:minute, or year-month-day T hour:minute-hour:minute "+" indicates that the time in the current time zone is in front of standard UTC time. "-" indicates that the time in the current time zone is behind the stand UTC time. In this format, ISO 8601-1 can be used.
CommonLog	Example: 28/Feb/2017:12:30:51 +0700
RFC822	Example: Tue, 28 Feb 2017 12:30:51 GMT
?D/?M/YY	day/month/year, in which the day and month can be one or two digits.
?D/?M/YY ?H:?M	day month year hour:minute, in which the day, month, hour, and minute can be one or two digits.
?D/?M/YY ?H:?M:?S	day month year hour:minute:second, in which the day, month, hour, minute, and second can be one or two digits.

The formats in the following table are ambiguous. You must specify a time format when using strings in these formats. For example, the cast('20121201' as timestamp format 'YYYYDDMM') statement incorrectly parses the string 20121201 as January 12, 2012.

Format	Description
YYYYDDMM	year day month
YYYY/DD/MM	year/day/month
MM/DD/YYYY	month/day/year
YYYY-DD-MM	year-day-month
MM-DD-YYYY	month-day-year
MM.DD.YYYY	month. day.year

Error codes

SelectObject returns error codes in the following two ways:

- The HTTP status code is included in the response header and the error code is included in the response body, which is the same as other OSS requests. Error code returned in this manner indicates that the SQL statement contained input or data errors, such as an invalid SQL statement.
- Error code is included in the end frame of the response body. Error code returned in this manner indicates that the data is not correct or does not match the SQL statement. For example, a string exists in a column of which the type is specified as integer in the SQL statement. In this

case, a part of data is processed and returned to the client, and the HTTP status code is 206.

Some error codes such as InvalidCSVLine can be returned as an HTTP status code in the response header or the end frame based on the location of the error row within the CSV object.

Error code	Description	HTTP status code	HTTP status code in end frame
InvalidSqlParameter	Invalid SQL parameter. Indicates that the SQL statement in the request is null, the SQL statement size has exceeded the limit, or the SQL statement is not Base64-encoded.	400	None
InvalidInputFieldDelimiter	Invalid column delimiter in the input CSV object. Indicates that the parameter is not Base64-encoded or that the size of the parameter is greater than 1 byte after being decoded.	400	None
InvalidInputRecordDelimiter	Invalid row delimiter in the input CSV object. Indicates that the parameter is not Base64-encoded or that the size of the parameter is greater than 2 bytes after being decoded.	400	None
InvalidInputQuote	Invalid quote character in the input CSV object. Indicates that the parameter is not Base64-encoded or that the size of the parameter is greater than 1 byte after being decoded.	400	None
InvalidOutputFieldDelimiter	Invalid column delimiter in the output CSV object. Indicates that the parameter is not Base64-encoded or that the size of the parameter is greater than 1 byte after being decoded.	400	None
InvalidOutputRecordDelimiter	Invalid column delimiter in the output CSV object. Indicates that the parameter is not Base64-encoded or that the size of the parameter is greater than 2 bytes after being decoded.	400	None
UnsupportedCompressionFormat	Invalid Compression parameter. Indicates that the value of the parameter is not NONE or GZIP (case-insensitive).	400	None
InvalidCommentCharacter	Invalid comment character in the CSV object. Indicates that the parameter is not Base64-encoded or that the size of the parameter is greater than 1 byte after being decoded.	400	None
InvalidRange	Invalid Range parameter. Indicates that the parameter is not prefixed with line-range= or split-range=, or that the range value does not meet the HTTP standard for Range.	400	None

Error code	Description	HTTP status code	HTTP status code in end frame
DecompressFailure	Indicates that the value of Compression is GZIP and that the object cannot be decompressed.	400	None
InvalidMaxSkippedRecordsAllowed	Indicates that the value of MaxSkippedRecordsAllowed is not an integer.	400	None
SelectCsvMetaUnavailable	Indicates that the Range parameter is specified and the CreateSelectObjectMeta operation has been called, but the target object does not include CSV Meta.	400	None
InvalidTextEncoding	Indicates that the object is not UTF-8 encoded.	400	None
InvalidOSSSelectParameters	Indicates that the EnablePayloadCrc and OutputRawData parameters are both set to True, which results in conflicts.	400	None
InternalError	Indicates that an OSS system error has occurred.	500 or 206	None or 500
SqlSyntaxError	Indicates that the syntax of the Base64-decoded SQL statement is invalid.	400	None
SqlExceedsMaxInCount	Indicates that the number of values included in the SQL IN clause has exceeded 1,024.	400	None
SqlExceedsMaxColumnNameLength	Indicates that the size of the column name has exceeded 1,024 bytes.	400	None
SqlInvalidColumnIndex	Indicates that the column index in the SQL statement is less than 1 byte or greater than 1,000 bytes in length.	400	None
SqlAggregationOnNonNumericType	Indicates that an aggregation function is used in a non-numeric column.	400	None
SqlInvalidAggregationOnTimestamp	Indicates that the SUM or AVG aggregation function is used in the timestamp column.	400	None
SqlValueTypeOfInMustBeSame	Indicates that values of different types are included in the SQL IN clause.	400	None
SqlInvalidEscapeChar	Indicates that an invalid escape character such as a question mark (?), percent sign (%), or an asterisk (*) was specified in the SQL LIKE clause.	400	None
SqlOnlyOneEscapeCharIsAllowed	Indicates that the size of the escape character in the SQL LIKE clause is greater than 1 byte in length.	400	None

Error code	Description	HTTP status code	HTTP status code in end frame
SqlNoCharAfterEscapeChar	Indicates that there are no characters after the escape character in the SQL LIKE clause.	400	None
SqlInvalidLimitValue	Indicates that the number after the SQL Limit clause is smaller than 1.	400	None
SqlExceedsMaxWildCardCount	Indicates that the number of wildcards, (*) or (%), has exceeded the limit in the SQL LIKE clause.	400	None
SqlExceedsMaxConditionCount	Indicates that the number of conditional expressions in the SQL WHERE clause has exceeded the limit.	400	None
SqlExceedsMaxConditionDepth	Indicates that the depth of the conditional tree in the SQL WHERE clause has exceeded the limit.	400	None
SqlOneColumnCastToDifferentTypes	Indicates that a column was converted into different types by including the CAST function in the SQL statement.	400	None
SqlOperationAppliedToDifferentTypes	Indicates that an operator was used for two objects of different types in the SQL statement. For example, this error code is returned if col1 in _col1 > 3 is a string.	400	None
SqlInvalidColumnName	Indicates that a column name used in the SQL statement was not included in the header of the CSV object.	400	None
SqlNotSupportedTimestampFormat	Indicates that the timestamp format specified in the SQL CAST clause is not supported.	400	None
SqlNotMatchTimestampFormat	Indicates that the timestamp format specified in the SQL CAST clause does not match the timestamp string.	400	None
SqlInvalidTimestampValue	Indicates that no timestamp format is specified in the SQL CAST clause and that the provided string cannot be converted into a timestamp.	400	None
SqlInvalidLikeOperand	Indicates that column names or indexes are not specified in the SQL LIKE clause, that the specified column is not of the string type, or that the right column in the LIKE clause is of the string type.	400	None
SqlInvalidMixOfAggregationAndColumn	Indicates that the SQL SELECT clause includes column names and indexes for both aggregation functions and non-aggregation functions at the same time.	400	None

Error code	Description	HTTP status code	HTTP status code in end frame
SqlExceedsMaxAggregationCount	Indicates that the number of aggregation functions included in the SQL SELECT clause has exceeded the limit.	400	None
SqlInvalidMixOfStarAndColumn	Indicates that an asterisk (*), a column name, and a column index are included within the same SQL statement.	400	None
SqlInvalidKeepAllColumnsWithAggregation	Indicates that the SQL statement includes aggregation functions while the KeepAllColumns parameter is set to True.	400	None
SqlInvalidKeepAllColumnsWithDuplicateColumn	Indicates that the SQL statement includes repeated column names or column indexes while the KeepAllColumns parameter is set to True.	400	None
SqlInvalidSqlAfterAnalysis	Indicates that the SQL statement is not supported because it is too complex to resolve.	400	None
InvalidArithmeticOperand	Indicates that the SQL statement contains arithmetical operations performed on non-numeric constants or columns.	400	None
SqlInvalidAndOperand	Indicates that the expressions connected by the AND operator in the SQL statement are not of the Boolean type.	400	None
SqlInvalidOrOperand	Indicates that the expressions connected by the OR operator in the SQL statement are not of the Boolean type.	400	None
SqlInvalidNotOperand	Indicates that the expressions connected by the NOT operator in the SQL statement are not of the Boolean type.	400	None
SqlInvalidIsNullOperand	Indicates that the SQL statement contains the IS NULL operator performed on a constant.	400	None
SqlComparerOperandTypeMismatch	Indicates that the SQL statement contains the comparison operator performed on two objects of different types.	400	None
SqlInvalidConcatOperand	Indicates that the SQL statement contains two constants connected by the concatenation operator (||).	400	None
SqlUnsupportedSql	Indicates that the SQL statement is too complex so that the size of the generated SQL plan has exceeded the limit.	400	None

Error code	Description	HTTP status code	HTTP status code in end frame
HeaderInfoExceedsMaxSize	Indicates that the size of the header information specified in the SQL statement has exceeded the limit.	400	None
OutputExceedsMaxSize	Indicates that a row of output results has exceeded the size limit.	400	None
InvalidCsvLine	Indicates that a row in the CSV object is invalid or has exceeded the size limit, or that the number of skipped rows has exceeded the value of MaxSkippedRecordsAllowed.	206 or 400	400 or None
NegativeRowIndex	Indicates that the value of the array index in the SQL statement is a negative number.	400	None
ExceedsMaxNestedColumnDepth	Indicates that the nested levels of the JSON object in the SQL statement have exceeded the level limit.	400	None
NestedColumnNotSupportInCsv	Indicates that the SQL statement contains nested columns that include periods (.) or arrays with brackets ([]), which are not supported for SQL statements of CSV objects.	400	None
TableRootNodeOnlySupportInJson	Indicates that the root node path can only be specified after From ossobject in JSON objects.	400	None
JsonNodeExceedsMaxSize	Indicates that the size of the root node in the JSON object has exceeded the limit.	400 or 206	None or 400
InvalidJsonData	Indicates that the JSON data is formatted incorrectly.	400 or 206	None or 400
ExceedsMaxJsonArraySize	Indicates that the number of elements in an array in the root node of the JSON object has exceeded the limit.	400 or 206	None or 400
WildCardNotAllowed	Indicates that the wildcard (*) cannot be used in SQL SELECT clauses or SQL WHERE clauses in the JSON object. For example, the following statement is not supported: `select s.a.b[*] from ossobject where a.c[*] > 0` .	400	None
JsonNodeExceedsMaxDepth	Indicates that the depth of the root node of the JSON object has exceeded the limit.	400 or 206	None or 400

2.4.1.7.17. PutObjectTagging

You can call this operation to configure object tagging.

Request syntax

```
PUT /objectname? tagging
Content-Length: 114
Host: bucketname.oss-cn-hangzhou.aliyuncs.com
Date: GMT Date
Authorization: SignatureValue
<Tagging>
 <TagSet>
  <Tag>
   <Key>Key</Key>
   <Value>Value</Value>
  </Tag>
 </TagSet>
</Tagging>
```

Request elements

Element	Type	Required	Description
Tagging	Container	Yes	Child node: TagSet
TagSet	Container	Yes	Parent node: Tagging Child node: Tag
Tag	Container	No	Parent node: TagSet Child node: Key and Value
Key	String	No	Parent node: Tag Child node: none
Value	String	No	Parent node: Tag Child node: none

Detail analysis

- The requester must have the permission to call the PutObjectTagging operation.
- When you modify tagging configurations for an object, the time when the object is last modified remains the same.

- The key and value of a tag can contain letters, digits, spaces, and special characters such as + - =. _ : /

Examples

- Sample requests

```
PUT /objectname? tagging
Content-Length: 114
Host: bucketname.oss-cn-hangzhou.aliyuncs.com
Date: Mon, 18 Mar 2019 08:25:17 GMT
Authorization: OSS **********:**********
<Tagging>
 <TagSet>
  <Tag>
   <Key>a</Key>
   <Value>1</Value>
  </Tag>
  <Tag>
   <Key>b</Key>
   <Value>2</Value>
  </Tag>
 </TagSet>
</Tagging>
```

- Sample success responses

```
200 (OK)
content-length: 0
server: AliyunOSS
x-oss-request-id: 5C8F55ED461FB4A64C000004
date: Mon, 18 Mar 2019 08:25:17 GMT
```

2.4.1.7.18. GetObjectTagging

Obtains the tags of an object.

Request syntax

```
GET /objectname?tagging
Host: bucketname.oss-cn-hangzhou.aliyuncs.com
Date: GMT Date
Authorization: SignatureValue
```

Response elements

Element	Type	Description
Tagging	Container	Sub-node: TagSet
TagSet	Container	Parent node: Tagging Sub-node: Tag
Tag	Container	Parent node: TagSet Sub-node: Key, Value
Key	String	Parent node: Tag Sub-node: None
Value	String	Parent node: Tag Sub-node: None

Examples

- Request example:

```
GET /objectname?tagging
Host: bucketname.oss-cn-hangzhou.aliyuncs.com
Date: Wed, 20 Mar 2019 02:02:36 GMT
Authorization: OSS ************:**********
```

- Response example:

```
200 (OK)
content-length: 209
server: AliyunOSS
x-oss-request-id: 5C919F38461FB42826000002
date: Wed, 20 Mar 2019 02:02:32 GMT
content-type: application/xml
<?xml version="1.0" encoding="UTF-8"?>
<Tagging>
 <TagSet>
  <Tag>
   <Key>a</Key>
   <Value>1</Value>
  </Tag>
  <Tag>
   <Key>b</Key>
   <Value>2</Value>
  </Tag>
 </TagSet>
</Tagging>
```

2.4.1.7.19. DeleteObjectTagging

Deletes the tag of a specified object.

Request syntax

```
DELETE /objectname?tagging
Host: bucketname.oss-cn-hangzhou.aliyuncs.com
Date: GMT Date
Authorization: SignatureValue
```

Examples

- Request example:

```
DELETE /objectname?tagging
Host: bucketname.oss-cn-hangzhou.aliyuncs.com
Date: Tue, 09 Apr 2019 03:00:33 GMT
Authorization: OSS LTAIbsTkySSptaz****/Zr0o6BKgAl7iiBtHN2JMC****
```

- Response example:

```
204 (No Content)
content-length: 0
server: AliyunOSS
x-oss-request-id: 5CAC0AD16D0232E2051B****
date: Tue, 09 Apr 2019 03:00:33 GMT
```

2.4.1.8. Multipart upload-relevant operations

2.4.1.8.1. Overview

Aside from the PutObject API, OSS also provides multipart upload for you to upload objects. You can use the multipart upload method in many scenarios, including but not limited to:

- Resumable upload is required.
- The object to be uploaded is larger than 100 MB.
- The OSS server is frequently disconnected due to poor network conditions.
- The size of the object to be uploaded is unknown.

2.4.1.8.2. InitiateMultipartUpload

Before transmitting data in the Multipart Upload mode, you must call the InitiateMultipartUpload API to require OSS to initiate a Multipart Upload event. This API returns a globally unique upload ID created by the OSS server to identify this MultipartUpload task. You can initiate operations based on this upload ID, such as abort or query the MultipartUpload task.

Request syntax

```
POST /ObjectName? uploads HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT date
Authorization: SignatureValue
```

Request parameters

The encoding-type parameter can be specified in the CompleteMultipartUpload request. OSS uses the specified encoding type to encode Key in the response.

Request parameters

Name	Description

Name	Description
encoding-type	The encoding type of the key in the response. Currently, URL encoding is supported. The Key is UTF-8-encoded, but the XML 1.0 Standard does not support parsing certain control characters, such as the characters with ASCII values from 0 to 10. If the key contains control characters not supported by the XML 1.0 Standard, you can set the encoding-type parameter to encode the returned Key. Type: string. Default value: none. Valid value: url.

Request header

Name	Description
Cache-Control	The Webpage caching behavior when the object is downloaded. For more information, see RFC2616. Type: string. Default value: none.
Content-Disposition	Specifies the name of the object when the object is downloaded. For more information, see RFC2616. Type: string. Default value: none.
Content-Encoding	The content encoding format when the object is downloaded. For more information, see RFC2616. Type: string. Default value: none.
Expires	The expiration time in milliseconds. For more information, see RFC2616. Type: integer. Default value: none.

Name	Description
x-oss-server-side-encryption	The encryption algorithm that OSS uses to encrypt each uploaded part of an object before storage. Type: string. Valid values: AES256 and KMS. Note You must purchase and enable Key Management Service (KMS) to use the KMS encryption algorithm. Otherwise, OSS returns the KmsServiceNotEnabled error code.

Response elements

Response elements

Name	Description
Bucket	The name of the bucket for which the MultipartUpload task is initiated. Type: string. Parent element: InitiateMultipartUploadResult.
InitiateMultipartUploadResult	The container that stores the response of the InitiateMultipartUpload request. Type: container. Child elements: Bucket, Key, and UploadId. Parent element: none.
Key	The name of the object for which the MultipartUpload task is initiated. Type: string. Parent element: InitiateMultipartUploadResult.
UploadId	The unique ID of the MultipartUpload task. Type: string. Parent element: InitiateMultipartUploadResult.
EncodingType	The encoding type of the key in the response. If the encoding-type parameter is specified in the request, the key is encoded in the response. Type: string. Parent element: container.

Detail analysis

1. When performing this operation to calculate the authentication signature, you must add you must add ?uploads to CanonicalizedResource.
2. The Initiate Multipart Upload request supports the following standard HTTP request headers: Cache-Control, Content-Disposition, Content-Encoding, Content-Type, Expires, and custom headers starting with x-oss-meta-. For the specific meaning of these headers, see the PUT Object API.
3. The InitiateMultipartUpload request does not affect an existing object with the same name.
4. When receiving an Initiate Multipart Upload request, the server returns a request body in the XML format. The request body contains three elements: Bucket, Key, and UploadID. You must record the UploadID for subsequent Multipart operations.
5. If the x-oss-server-side-encryption header is set in the Initiate Multipart Upload request, the server returns this header in the response header. During the upload of each part, the server automatically stores the part after entropy encryption. Currently, the OSS server only supports AES256. If another standard is specified, the OSS server returns the 400 Bad Request message and the error code InvalidEncryptionAlgorithmError. Therefore, you do not need to set the x-oss-server-side-encryption request header for the upload of each part. If this request header is specified, OSS returns the error code 400 and the error message InvalidArgument.

Examples

Sample request:

```
POST /multipart.data? uploads HTTP/1.1
Host: ***.regionid.example.com
Date: Wed, 22 Feb 2012 08:32:21 GMT
Authorization: OSS q***4=
```

Sample response:

```
HTTP/1.1 200 OK
Content-Length: 230
Server: AliyunOSS
Connection: keep-alive
x-oss-request-id: 4***8
Date: Wed, 22 Feb 2012 08:32:21 GMT
Content-Type: application/xml

<? xml version="1.0" encoding="UTF-8"? >
<InitiateMultipartUploadResult xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
  <Bucket> multipart_upload</Bucket>
  <Key>multipart.data</Key>
  <UploadId>0***D</UploadId>
</InitiateMultipartUploadResult>
```

2.4.1.8.3. UploadPart

After initializing a MultipartUpload task, you can call UploadPart to upload data in parts based on the specified object name and upload ID. Each uploaded part has a number that identifies it. (The part number ranges from 1 to 10,000.) For the same upload ID, this part number identifies not only data in this part of, but also the location of this part in the entire object. If you upload new data with the same part number, OSS overwrites the existing data identified by this part number. Aside from the last part, the minimum size of each part is 100 KB. The size of the last part is not restricted.

Request syntax

```
PUT /ObjectName? partNumber=PartNumber&uploadId=UploadId HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Content-Length: Size
Authorization: SignatureValue
```

Detail analysis

1. Before calling this API to upload a part, you must call the InitiateMultipartUpload API to obtain an upload ID issued by the OSS server.
2. In the multipart upload mode, except the last part, each of all other parts must be larger than 100 KB. However, the UploadPart API does not immediately verify the size of the uploaded part (because it cannot immediately determine which part is the last one). It verifies the size of the uploaded part only when multipart upload is completed.
3. OSS includes the MD5 value of the data for each part received by the server in the ETag header and returns it to the user.
4. The part number ranges from 1 to 10,000. If a part number is beyond this range, OSS returns the InvalidArgument error code.

5. If the x-oss-server-side-encryption request header is specified when the InitiateMultipartUpload API is called, OSS encrypts the uploaded part and returns the x-oss-server-side-encryption header in the UploadPart response header. The value of x-oss-server-side-encryption indicates the server-side encryption algorithm used for this part. For more information, see the InitiateMultipartUpload API. 6 To ensure that the data transmitted over the network is free of errors, the SDK automatically sets the Content-MD5 value. OSS calculates the MD5 value of the uploaded data and compares it with the MD5 value calculated by the SDK. If they are inconsistent, OSS returns the InvalidDigest error code.

Examples

Sample request:

```
PUT /multipart.data? partNumber=1&uploadId=0***6 HTTP/1.1
Host: ***.regionid.example.com
Content-Length: 6291456
Date: Wed, 22 Feb 2012 08:32:21 GMT
Authorization: OSS q***I=
[6291456 bytes data]
```

Sample response:

```
HTTP/1.1 200 OK
Server: AliyunOSS
Connection: keep-alive
ETag: 7***9
x-oss-request-id: 3***a
Date: Wed, 22 Feb 2012 08:32:21 GMT
```

2.4.1.8.4. UploadPartCopy

You can call UploadPartCopy to copy data from an existing object to upload a part. You can add an x-oss-copy-source header in the UploadPart request to call this API. When copying an object larger than 1 GB, you must use the Upload Part Copy method. If you want to copy an object that is smaller than 1 GB by a single operation, you can refer to Copy Object.

Request syntax

```
PUT /ObjectName? partNumber=PartNumber&uploadId=UploadId HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Content-Length: Size
Authorization: SignatureValue
x-oss-copy-source: /SourceBucketName/SourceObjectName
x-oss-copy-source-range:bytes=first-last
```

Request header

Except the common request header, other headers in the Upload Part Copy request are used to specify the address of the copied source object and copying range.

Request header

Name	Description
x-oss-copy-source	The source IP address for object copy. The requester must have the permission to read the source object. Type: string. Default value: none.
x-oss-copy-source-range	Copying range of the copied source object. For example, if this parameter is set to bytes=0-9, OSS transfers byte 0 to byte 9. This request header is not required when the entire source object is copied. Type: integer. Default value: none.

The following request header is used for the source object specified by the x-oss-copy-source parameter.

Request header

Name	Description
x-oss-copy-source-if-match	The object copy condition. If the ETag value of the source object is equal to the ETag value specified in the request, OSS copies the object. Otherwise, OSS returns the 412 Precondition Failed error. Type: string. Default value: none.
x-oss-copy-source-if-none-match	The object copy condition. If the ETag value of the source object is not equal to the ETag value specified in the request, OSS copies the object. Otherwise, OSS returns the 412 Precondition Failed error. Type: string. Default value: none.
x-oss-copy-source-if-unmodified-since	The object copy condition. If the specified time is equal to or later than the actual object modification time, OSS transfers the object and returns the 200 OK message. Otherwise, OSS returns the 412 Precondition Failed message. Type: string. Default value: none.

Name	Description
x-oss-copy-source-if-modified-since	The object copy condition. If the source object has been modified since the time specified in the request, OSS copies the object. Otherwise, OSS returns the 412 Precondition Failed error. Type: string. Default value: none.

Response elements

Response elements

Name	Description
x-oss-copy-source-if-match	The object copy condition. If the ETag value of the source object is equal to the ETag value specified in the request, OSS copies the object. Otherwise, OSS returns the 412 Precondition Failed error. Type: string. Default value: none.
x-oss-copy-source-if-none-match	The object copy condition. If the ETag value of the source object is not equal to the ETag value specified in the request, OSS copies the object. Otherwise, OSS returns the 412 Precondition Failed error. Type: string. Default value: none.
x-oss-copy-source-if-unmodified-since	The object copy condition. If the specified time is equal to or later than the actual object modification time, OSS transfers the object and returns the 200 OK message. Otherwise, OSS returns the 412 Precondition Failed message. Type: string. Default value: none.
x-oss-copy-source-if-modified-since	The object copy condition. If the source object has been modified since the time specified in the request, OSS copies the object. Otherwise, OSS returns the 412 Precondition Failed error. Type: string. Default value: none.

Detail analysis

1. Before calling this API to upload a part, you must call the InitiateMultipartUpload API to obtain an upload ID issued by the OSS server.
2. In the multipart upload mode, except the last part, each of all other parts must be larger than 100 KB. However, the UploadPart API does not immediately verify the size of the uploaded part (because it cannot immediately determine which part is the last one). It verifies the size of the uploaded part only when multipart upload is completed.

3. If the x-oss-copy-source-range request header is not specified, the entire source object is copied. If the request header is specified, the returned message includes the length of the entire file and the COPY range. For example, if the returned message is Content-Range: bytes 0-9/44 indicates that the length of the entire file is 44 and the copying range is 0-9. If the specified range does not conform to the range rules, OSS copies the entire file and does not contain Content-Range in the result.
4. If the x-oss-server-side-encryption request header is specified when the InitiateMultipartUpload API is called, OSS encrypts the uploaded part and returns the x-oss-server-side-encryption header in the UploadPart response header. The value of x-oss-server-side-encryption indicates the server-side encryption algorithm used for this part. For more information, see the InitiateMultipartUpload API.
5. CopyObject cannot be used to copy the objects created by using AppendObject.

Examples

Sample request:

```
PUT /multipart.data? partNumber=1&uploadId=0***6 HTTP/1.1
Host: ***.regionid.example.com
Content-Length: 6291456
Date: Wed, 22 Feb 2012 08:32:21 GMT
Authorization: OSS q***l=
x-oss-copy-source: /oss-example/ src-object
x-oss-copy-source-range:bytes=100-6291756
```

Sample response:

```
HTTP/1.1 200 OK
Server: AliyunOSS
Connection: keep-alive
x-oss-request-id: 3***a
Date: Thu, 17 Jul 2014 06:27:54 GMT'
<? xml version="1.0" encoding="UTF-8"? >
<CopyPartResult xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
 <LastModified>2014-07-17T06:27:54.000Z </LastModified>
 <ETag>"5***E"</ETag>
</CopyPartResult>
```

2.4.1.8.5. CompleteMultipartUpload

After all parts of an object are uploaded, CompleteMultipartUpload must be used to complete the upload of the entire object. The CompleteMultipartUpload request must contain a list of all valid parts (including the part numbers and ETag values) of the object. After receiving the request, OSS verifies the validity of each part. After all the data parts have been verified, OSS combines these parts into a complete object.

Request syntax

```
POST /ObjectName? uploadId=UploadId HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Content-Length: Size
Authorization: Signature

<CompleteMultipartUpload>
<Part>
<PartNumber>PartNumber</PartNumber>
<ETag>ETag</ETag>
</Part>
...
</CompleteMultipartUpload>
```

Request parameters

The encoding-type parameter can be specified in the CompleteMultipartUpload request. OSS uses the specified encoding type to encode Key in the response.

Request parameters

Name	Description
encoding-type	The encoding type of the key in the response. Currently, URL encoding is supported. The Key is UTF-8-encoded, but the XML 1.0 Standard does not support parsing certain control characters, such as the characters with ASCII values from 0 to 10. If the key contains control characters not supported by the XML 1.0 Standard, you can set the encoding-type parameter to encode the returned Key. Type: string. Default value: none. Valid value: url.

Request elements

Request elements

Name	Description
CompleteMultipartUpload	The container that stores the content of the CompleteMultipartUpload request. Type: container. Child element: one or more part elements. Parent element: none.

Name	Description
ETag	The ETag value returned by OSS after parts are successfully uploaded. Type: string. Parent element: Part.
Part	The container that stores the uploaded parts. Type: container. Child elements: ETag and PartNumber. Parent element: InitiateMultipartUploadResult.
PartNumber	The number of parts. Type: integer. Parent element: Part.

Response elements

Response elements

Name	Description
Bucket	The bucket name. Type: string. Parent element: CompleteMultipartUploadResult.
CompleteMultipartUploadResult	The container that stores the response of the CompleteMultipartUpload request. Type: container. Child elements: Bucket, Key, ETag, and Location. Location Parent element: none.
ETag	The entity tag that is created during the generation of an object and used to identify the content of the object. For an object that is created using the Complete Multipart Upload request, the value of ETag is the UUID of the object content. The ETag value of an object can be used to check whether the object content has changed. Type: string. Parent element: CompleteMultipartUploadResult.
Location	The URL of the created object. Type: string. Parent element: CompleteMultipartUploadResult.

Name	Description
Key	The name of the created object. Type: string. Parent element: CompleteMultipartUploadResult.
EncodingType	The encoding type of the key in the response. If the encoding-type parameter is specified in the request, the key is encoded in the response. Type: string. Parent element: container.

Detail analysis

1. For an object that is created using the Complete Multipart Upload request, OSS verifies that all parts except the last part are larger than 100 KB and checks each part number and ETag in the part list submitted by the user. Therefore, when uploading data parts, the client needs to record the part number and the ETag value returned by the OSS each time a part is uploaded successfully.
2. It takes a while for the OSS to process the Complete Multipart Upload request. During this time, if the client is disconnected from the OSS, the OSS continues to complete the request.
3. The part numbers listed in the request can be non-consecutive. For example, the first part number is 1 and the second part number is 5.
4. After OSS successfully processes the Complete Multipart Upload request, the corresponding Upload ID becomes invalid.
5. An object may have different upload IDs. Upload tasks with corresponding upload IDs do not affect each other.
6. If the x-oss-server-side-encryption header field is specified in the InitiateMultipartUpload request, OSS returns the x-oss-server-side-encryption header field in the CompleteMultipartUpload response.
7. If the Content-MD5 field value is specified in the request header, OSS calculates the Content-MD5 field value in the request body and checks whether the two values are the same. If they are different, OSS returns the InvalidDigest error.

Examples

Sample request:

```
POST /multipart.data? uploadId=0***4  HTTP/1.1
Host: ***.regionid.example.com
Content-Length: 1056
Date: Fri, 24 Feb 2012 10:19:18 GMT
Authorization: OSS q***0=

<CompleteMultipartUpload>
   <Part>
      <PartNumber>1</PartNumber>
      <ETag>"3***9"</ETag>
   </Part>
   <Part>
      <PartNumber>5</PartNumber>
      <ETag>"8***A"</ETag>
   </Part>
   <Part>
      <PartNumber>8</PartNumber>
      <ETag>"8***2"</ETag>
   </Part>
</CompleteMultipartUpload>
```

Sample response:

```
HTTP/1.1 200 OK
Server: AliyunOSS
Content-Length: 329
Content-Type: Application/xml
Connection: keep-alive
x-oss-request-id: 5***e
Date: Fri, 24 Feb 2012 10:19:18 GMT

<? xml version="1.0" encoding="UTF-8"? >
<CompleteMultipartUploadResult xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
   <Location>http://***.regionid.example.com /multipart.data</Location>
   <Bucket>oss-example</Bucket>
   <Key>multipart.data</Key>
   <ETag>B***D-3</ETag>
</CompleteMultipartUploadResult>
```

2.4.1.8.6. AbortMultipartUpload

You can call AbortMultipartUpload to abort a MultipartUpload task based on the upload ID. If a MultipartUpload task is aborted, you cannot use the upload ID to perform any operation any longer and the uploaded part is deleted.

Request syntax

```
DELETE /ObjectName? uploadId=UploadId HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: Signature
```

Detail analysis

1. If you stop a Multipart Upload event, you cannot delete parts that are being uploaded. Therefore, if concurrent access exists, you must call the AbortMultipartUpload API several times to completely release the space of OSS.
2. If the entered Upload ID does not exist, OSS returns an error 404 with the error code: NoSuchUpload.

Examples

Sample request:

```
Delete /multipart.data? &uploadId=0***E  HTTP/1.1
Host: ***.regionid.example.com
Date: Wed, 22 Feb 2012 08:32:21 GMT
Authorization: OSS q***I=
```

Sample response:

```
HTTP/1.1 204
Server: AliyunOSS
Connection: keep-alive
x-oss-request-id: 0***d
Date: Wed, 22 Feb 2012 08:32:21 GMT
```

2.4.1.8.7. ListMultipartUploads

You can call ListMultipartUploads to list all ongoing MultipartUpload tasks, namely, multipart upload tasks that have been initialized but not completed or aborted. The list returned by OSS contains a maximum of 1,000 multipart upload tasks. If you want to specify the number of Multipart Upload messages in the listing result returned by OSS, you can add the max-uploads parameter to the request. In the response returned by OSS, the IsTruncated element indicates whether the response contains all the ongoing MultipartUpload tasks.

Request syntax

```
Get /? uploads HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: Signature
```

Request parameters

Request parameters

Name	Description
delimiter	The delimiter used to group objects by name. CommonPrefixes specify a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter. Type: string.
max-uploads	The maximum number of MultipartUpload tasks returned for one request. If this parameter is not specified, the default value is 1,000. The max-uploads value cannot exceed 1,000. Type: string.
key-marker	The starting position of the returned results. This parameter is used together with the upload-id-marker parameter. l If the upload-id-marker parameter is not set, OSS returns the list of all MultipartUpload tasks whose object names start with a letter that comes after the key-marker value in the alphabetic order. l If the upload-id-marker parameter is set, the query result includes Multipart tasks in which the lexicographic orders of all object names are greater than the value of the key-marker parameter and all Multipart Upload tasks in which the object names are the same as the value of the key-marker parameter but the Upload but the upload IDs are greater than the value of the upload-id-marker parameter. Type: string.
prefix	The prefix that must be contained in the names (key) of the returned objects. Note that if you use a prefix to make a query, the returned key values still contain the prefix. Type: string.
upload-id-marker	Used together with the key-marker parameter to specify the starting position of the returned results. l If the key-marker parameter is not specified, OSS ignores the upload-id-marker parameter. l If the key-marker parameter is set, the query result includes Multipart tasks in which the lexicographic orders of all object names are greater than the value of the key-marker parameter and all Multipart Upload tasks in which the object names are the same as the value of the key-marker parameter but the upload IDs are greater than the value of the upload-id-marker parameter. Type: string.

Name	Description
encoding-type	The encoding type of the key in the response. Delimiter, KeyMarker, Prefix, NextKeyMarker, and Key use UTF-8 characters, 1.0 Standard does not support parsing certain control characters, such as the characters with ASCII values from 0 to 10. If some elements in the response contain control encoding-type can be specified to encode these elements, such as Delimiter, KeyMarker, Prefix, NextMarker, and Key. Type: string. Default value: none.

Response elements

Response elements

Name	Description
ListMultipartUploadsResult	The container that stores the response of the ListMultipartUpload request. Type: container. Child elements: Bucket, KeyMarker, UploadIdMarker, NextKeyMarker, NextUploadIdMarker, MasUploads, Delimiter, Prefix, CommonPrefixes, IsTruncated, and Upload. Parent element: none.
Bucket	The bucket name. Type: string. Parent element: ListMultipartUploadsResult.
EncodingType	The encoding type of the key in the response. If encoding-type is specified in the request, those elements including Delimiter, KeyMarker, Prefix, NextKeyMarker, and Key are encoded in the returned result. Type: string. Parent element: ListMultipartUploadsResult.
KeyMarker	The position of the starting object on the list. Type: string. Parent element: ListMultipartUploadsResult.
UploadIdMarker	The position of the starting upload ID on the list. Type: string. Parent element: ListMultipartUploadsResult.

Name	Description
NextKeyMarker	Indicates that this response does not contain all results discovered by OSS and specifies the starting position of the list in the response to the next request. Type: string. Parent element: ListMultipartUploadsResult.
NextUploadMarker	Indicates that this response does not contain all results discovered by OSS and specifies the starting position of the list in the response to the next request. Type: string. Parent element: ListMultipartUploadsResult.
MaxUploads	The maximum number of upload tasks returned by OSS. Type: integer. Parent element: ListMultipartUploadsResult.
IsTruncated	Specifies whether the MultipartUpload task list returned in this response is truncated. "true" indicates that this response does not contain all the parts discovered by OSS. "false" indicates that this response contains all the parts discovered by OSS. Type: enumeration. Valid values: false and true. Default value: false. Parent element: ListMultipartUploadsResult.
Upload	The container that stores the information about MultipartUpload tasks. Type: container. Child elements: Key, UploadId, Initiated Parent element: ListMultipartUploadsResult.
Key	The object name in an initialized MultipartUpload task. Type: string. Parent element: Upload.
UploadId	The ID of the MultipartUpload task. Type: string. Parent element: Upload.

Name	Description
Initiated	The time a MultipartUpload task is initialized. Type: date. Parent element: Upload.

Detail analysis

1. The maximum value of the max-uploads parameter is 1000.
2. The results returned by the OSS are listed in ascending order based on the lexicographic orders of object names; for the same object, the results are listed in ascending time order.
3. Using the prefix parameter, you can flexibly manage objects in a bucket in groups (similar to the folder function).
4. The List Multipart Uploads request supports five request parameters: prefix, marker, delimiter, upload-id-marker, and max-uploads. Based on the combinations of these parameters, you can set rules for querying Multipart Uploads events to obtain the expected query results.

Examples

Sample request:

```
Get /? uploads  HTTP/1.1
Host:***.regionid.example.com
Date: Thu, 23 Feb 2012 06:14:27 GMT
Authorization: OSS q***Y=
```

Sample response:

```
HTTP/1.1 200
Server: AliyunOSS
Connection: keep-alive
Content-length: 1839
Content-type: application/xml
x-oss-request-id: 5***a
Date: Thu, 23 Feb 2012 06:14:27 GMT

<? xml version="1.0" encoding="UTF-8"? >
<ListMultipartUploadsResult xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
  <Bucket>oss-example</Bucket>
  <KeyMarker></KeyMarker>
  <UploadIdMarker></UploadIdMarker>
  <NextKeyMarker>oss.avi</NextKeyMarker>
  <NextUploadIdMarker>0***F</NextUploadIdMarker>
  <Delimiter></Delimiter>
  <Prefix></Prefix>
  <MaxUploads>1000</MaxUploads>
  <IsTruncated>false</IsTruncated>
  <Upload>
    <Key>multipart.data</Key>
    <UploadId>0***8</UploadId>
    <Initiated>2012-02-23T04:18:23.000Z</Initiated>
  </Upload>
  <Upload>
    <Key>multipart.data</Key>
    <UploadId>0***5</UploadId>
    <Initiated>2012-02-23T04:18:23.000Z</Initiated>
  </Upload>
  <Upload>
    <Key>oss.avi</Key>
    <UploadId>0***F</UploadId>
    <Initiated>2012-02-23T06:14:27.000Z</Initiated>
  </Upload>
</ListMultipartUploadsResult>
```

2.4.1.8.8. ListParts

You can call List Parts to list all successfully uploaded parts mapped to a specific upload ID.

Request syntax

```
GET /ObjectName? uploadId=UploadId HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: Signature
```

Request parameters

Request parameters

Name	Description
uploadId	The ID of the MultipartUpload task. Type: string. Default value: none.
max-parts	The maximum number of parts listed in the OSS response. Type: integer. Default: 1,000
part-number-marker	The starting position of a specific list. All the parts with the part numbers greater than the value of this parameter are listed. Type: integer. Default value: none.
encoding-type	The encoding type of the key in the response. The Key is UTF-8-encoded, but the XML 1.0 Standard does not support parsing certain control characters, such as the characters with ASCII values from 0 to 10. Therefore, OSS needs to encrypt the key based on the specified encoding type before returning it. If the key contains control characters not supported by the XML 1.0 Standard, you can set the encoding-type parameter to encode the returned Key. Type: string. Default value: none. Valid value: url.

Response elements

Response elements

Name	Description

Name	Description
ListPartsResult	The container that stores the response of the ListParts request. Type: container. Child elements: Bucket, Key, UploadId, PartNumberMarker, NextPartNumberMarker, MaxParts, IsTruncated, and Part. Parent element: none.
Bucket	The bucket name. Type: string. Parent element: ListPartsResult.
EncodingType	The encoding type of the key in the response. If the encoding-type parameter is specified in the request, the key is encoded in the response. Type: string. Parent element: ListPartsResult.
Key	The object name. Type: string. Parent element: ListPartsResult.
UploadId	The ID of an upload task. Type: string. Parent element: ListPartsResult.
PartNumberMarker	The starting position of the list in this response. Type: integer. Parent element: ListPartsResult.
NextPartNumberMarker	Indicates that this response does not contain all the results discovered by OSS and specifies the starting position of the list in the response to the next request. Type: integer. Parent element: ListPartsResult.
MaxParts	The maximum number of parts in this response. Type: integer. Parent element: ListPartsResult.

Name	Description
IsTruncated	Indicates whether the part list returned in this response is truncated. "true" indicates that this response does not contain all the parts discovered by OSS. "false" indicates that this response contains all the parts discovered by OSS. Type: enumeration. Valid values: true and false. Parent element: ListPartsResult.
Part	The container that stores part information. Type: string. Child elements: PartNumber, LastModified, ETag, and Size. Parent element: ListPartsResult.
PartNumber	The number that identifies a part. Type: integer. Parent element: ListPartsResult.Part.
LastModified	The time a part is uploaded. Type: date. Parent element: ListPartsResult.Part.
ETag	The ETag value in the content of an uploaded part. Type: string. Parent element: ListPartsResult.Part.
Size	The size of an uploaded part. Type: integer. Parent element: ListPartsResult.Part.

Detail analysis

1. ListParts supports two request parameters: max-parts and part-number-marker.
2. The maximum value of the max-parts parameter is 1,000; its default value is also 1,000.
3. The results returned by the OSS are listed in ascending order based on the part numbers.
4. Because errors may occur in network transmission, it is not recommended that you use the result (part number and ETag value) of List Parts to generate the final part list of Complete Multipart.

Examples

Sample request:

```
Get  /multipart.data? uploadId=0***5  HTTP/1.1
Host: ***.regionid.example.com
Date: Thu, 23 Feb 2012 07:13:28 GMT
Authorization: OSS q***8=
```

Sample response:

```
HTTP/1.1 200
Server: AliyunOSS
Connection: keep-alive
Content-length: 1221
Content-type: application/xml
x-oss-request-id: 1***c
Date: Thu, 23 Feb 2012 07:13:28 GMT

<? xml version="1.0" encoding="UTF-8"? >
<ListPartsResult xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
  <Bucket>multipart_upload</Bucket>
  <Key>multipart.data</Key>
  <UploadId>0***5</UploadId>
  <NextPartNumberMarker>5</NextPartNumberMarker>
  <MaxParts>1000</MaxParts>
  <IsTruncated>false</IsTruncated>
  <Part>
    <PartNumber>1</PartNumber>
    <LastModified>2012-02-23T07:01:34.000Z</LastModified>
    <ETag>&amp;quot;3***9&amp;quot;</ETag>
    <Size>6291456</Size>
  </Part>
  <Part>
    <PartNumber>2</PartNumber>
    <LastModified>2012-02-23T07:01:12.000Z</LastModified>
    <ETag>&amp;quot;3***9&amp;quot;</ETag>
    <Size>6291456</Size>
  </Part>
  <Part>
    <PartNumber>5</PartNumber>
    <LastModified>2012-02-23T07:02:03.000Z</LastModified>
    <ETag>&amp;quot;7***9&amp;quot;</ETag>
    <Size>1024</Size>
  </Part>
</ListPartsResult>
```

2.4.1.9. CORS

2.4.1.9.1. Overview

CORS allows Web applications to access resources in other regions. With the CORS support, the OSS allows users to develop more flexible Web applications. OSS provides APIs for developers to conveniently control CORS permissions.

2.4.1.9.2. PutBucketcors

You can call PutBucketcors to set a new CORS rule for a specified bucket. The original rule, if any, is overwritten.

Request syntax

```
PUT /? cors HTTP/1.1
Date: GMT Date
Content-Length: ContentLength
Content-Type: application/xml
Host: BucketName.regionid.example.com
Authorization: SignatureValue

<? xml version="1.0" encoding="UTF-8"? >
<CORSConfiguration>
  <CORSRule>
    <AllowedOrigin>the origin you want allow CORS request from</AllowedOrigin>
    <AllowedOrigin>... </AllowedOrigin>
    <AllowedMethod>HTTP method</AllowedMethod>
    <AllowedMethod>... </AllowedMethod>
     <AllowedHeader> headers that allowed browser to send</AllowedHeader>
      <AllowedHeader>... </AllowedHeader>
      <ExposeHeader> headers in response that can access from client app</ExposeHeader>
      <ExposeHeader>... </ExposeHeader>
      <MaxAgeSeconds>time to cache pre-fight response</MaxAgeSeconds>
  </CORSRule>
  <CORSRule>
    ...
  </CORSRule>
...
</CORSConfiguration >
```

Request elements

Request elements

Name	Description	Required

Name	Description	Required
CORSRule	The container that stores CORS rules. Each bucket allows 10 rules at most. Type: container. Parent element: CORSConfiguration.	Yes
AllowedOrigin	The origin allowed for CORS requests. You can use multiple elements to specify multiple allowed origins. Up to one wildcard (*) is allowed. If this parameter is set to a wildcard (*), CORS requests of all origins are allowed. Type: string. Parent element: CORSRule.	Yes
AllowedMethod	The allowed method for cross-origion requests. Type: enumeration (GET, PUT, DELETE, POST, and HEAD). Parent element: CORSRule.	Yes
AllowedHeader	The setting that controls whether the headers specified by Access-Control-Request-Headers in the OPTIONS prefetch command are allowed. Each header specified by Access-Control-Request-Headers must match a value of AllowedHeader. Up to one wildcard (*) is allowed. Type: string. Parent element: CORSRule.	No
ExposeHeader	The response headers that allow users to access from an application (for example, a Javascript XMLHttpRequest object). No wildcard (*) is allowed. Type: string. Parent element: CORSRule.	No
MaxAgeSeconds	The cache time for the response of a browser prefetch (OPTIONS) request for a specific resource, in seconds. One CORSRule allows not more than one such parameter. Type: integer. Parent element: CORSRule.	No
CORSConfiguration	The CORS rule configuration container for the bucket. Type: container. Parent element: none.	Yes

Detail analysis

1. CORS is disabled for buckets by default. The origins of all cross-origion requests are forbidden.

2. To use CORS in applications, for example, accessing the OSS from www.a.com through the XMLHttpRequest function of the browser, you need to manually upload a CORS rule through this API to enable CORS. This rule is described in an XML document.
3. The CORS setting for each bucket is specified by multiple CORS rules. Each bucket allows a maximum of 10 rules. The uploaded XML document cannot be larger than 16 KB.
4. When OSS receives a cross-origin request (or an OPTIONS request), it reads the bucket's CORS rules and then checks the relevant permissions. OSS matches the rules one by one. When OSS finds the first match, it returns a corresponding header. If none of the rules match, OSS does not attach any CORS header.
5. Successful CORS rule matching must satisfy three conditions. First, the request Origin must match the AllowedOrigin. Second, the request method (for example, GET, PUT) or the method corresponding to the Access-Control-Request-Method header in an OPTIONS request must match the AllowedMethod. Third, each header contained in the Access-Control-Request-Headers in an OPTIONS request must match the AllowedHeader.
6. If the Content-MD5 field value is specified in the request header, OSS calculates the Content-MD5 field value in the request body and checks whether the two values are the same. If they are different, OSS returns the InvalidDigest error.

Examples

Example of adding a bucket CORS rule:

```
PUT /? cors HTTP/1.1
Host: ***.regionid.example.com
Content-Length: 186
Date: Fri, 04 May 2012 03:21:12 GMT
Authorization: OSS q***A=

<? xml version="1.0" encoding="UTF-8"? >
<CORSConfiguration>
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>PUT</AllowedMethod>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>Authorization</AllowedHeader>
  </CORSRule>
  <CORSRule>
    <AllowedOrigin>http://www.a.com</AllowedOrigin>
    <AllowedOrigin>http://www.b.com</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader> Authorization</AllowedHeader>
    <ExposeHeader>x-oss-test</ExposeHeader>
    <ExposeHeader>x-oss-test1</ExposeHeader>
    <MaxAgeSeconds>100</MaxAgeSeconds>
  </CORSRule>
</CORSConfiguration >
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***F
Date: Fri, 04 May 2012 03:21:12 GMT
Content-Length: 0
Connection: keep-alive
Server: AliyunOSS
```

2.4.1.9.3. GetBucketcors

You can call GetBucketcors to obtain the current CORS rules of a specified bucket.

Request syntax

```
GET /? cors HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Response elements

Response elements

Name	Description
CORSRule	The container that stores CORS rules. Each bucket allows 10 rules at most. Type: container. Parent element: CORSConfiguration.
AllowedOrigin	The origin allowed for CORS requests. You can use multiple elements to specify multiple allowed origins. Up to one wildcard (*) is allowed. If this parameter is set to a wildcard (*), CORS requests of all origins are allowed. Type: string. Parent element: CORSRule.
AllowedMethod	The allowed method for cross-origion requests. Type: enumeration (GET, PUT, DELETE, POST, and HEAD). Parent element: CORSRule.
AllowedHeader	Indicates whether the headers specified by Access-Control-Request-Headers in the OPTIONS prefetch command are allowed. Each header specified by Access-Control-Request-Headers must match a value of AllowedHeader. Up to one wildcard (*) is allowed. Type: string. Parent element: CORSRule.
ExposeHeader	Specify the response headers allowing users to access from an application (for example, a Javascript XMLHttpRequest object). No wildcard (*) is allowed. Type: string. Parent element: CORSRule.
MaxAgeSeconds	The cache time for the response of a browser prefetch (OPTIONS) request for a specific resource, in seconds. One CORSRule allows not more than one such parameter. Type: integer. Parent element: CORSRule.

Name	Description
CORSConfiguration	The CORS rule configuration container for the bucket. Type: container. Parent element: none.

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. Only the bucket owner can obtain CORS rules. Otherwise, OSS returns the 403 Forbidden message. Error code: AccessDenied.
3. If CORS rules do not exist, OSS returns the "404 Not Found" error with the error code: NoSuchCORSConfiguration.

Examples

Sample request:

```
Get /? cors HTTP/1.1
Host: ***.regionid.example.com
Date: Thu, 13 Sep 2012 07:51:28 GMT
Authorization: OSS q***w=
```

Sample response with CORS rules already set:

```
HTTP/1.1 200
x-oss-request-id: 5***F
Date: Thu, 13 Sep 2012 07:51:28 GMT
Connection: keep-alive
Content-Length: 218
Server: AliyunOSS

<? xml version="1.0" encoding="UTF-8"? >
<CORSConfiguration>
  <CORSRule>
   <AllowedOrigin>*</AllowedOrigin>
   <AllowedMethod>GET</AllowedMethod>
   <AllowedHeader>*</AllowedHeader>
   <ExposeHeader>x-oss-test</ExposeHeader>
   <MaxAgeSeconds>100</MaxAgeSeconds>
  </CORSRule>
</CORSConfiguration>
```

2.4.1.9.4. DeleteBucketcors

You can call DeleteBucketcors to disable CORS for a specified bucket and delete all the rules.

Request syntax

```
DELETE /? cors HTTP/1.1
Host: BucketName.regionid.example.com
Date: GMT Date
Authorization: SignatureValue
```

Detail analysis

1. If the bucket does not exist, OSS returns the 404 Not Found message. Error code: NoSuchBucket.
2. Only the owner of the bucket can delete the CORS rules corresponding to the bucket. If you try to operate a bucket that does not belong to you, OSS returns the 403 Forbidden message. Error code: AccessDenied.

Examples

Sample request:

```
DELETE /? cors HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 05:45:34 GMT
Authorization: OSS q***g=
```

Sample response:

```
HTTP/1.1 204 No Content
x-oss-request-id: 5***C
Date: Fri, 24 Feb 2012 05:45:34 GMT
Connection: keep-alive
Content-Length: 0
Server: AliyunOSS
```

2.4.1.9.5. OptionObject

Before sending a cross-origion request, the browser sends a preflight request (OPTIONS) containing a specific origin, HTTP method, and header information to OSS to determine whether to send a real request. OSS enables you to use the Put Bucket cors API to enable CORS support for buckets. OSS determines whether to allow the preflight request of the browser based on the specified rules after CORS is enabled. If OSS does not allow this request or CORS is disabled, the error 403 Forbidden is returned.

Request syntax

```
OPTIONS /ObjectName HTTP/1.1
Host: BucketName.regionid.example.com
Origin:Origin
Access-Control-Request-Method:HTTP method
Access-Control-Request-Headers:Request Headers
```

Request header

Request header

Name	Description
Origin	The origin of a request, used to identify a cross-origion request. Type: string. Default value: none.
Access-Control-Request-Method	The methods to be used in an actual request. Type: string. Default value: none.
Access-Control-Request-Headers	The header fields, except simple ones, to be used in an actual request. Type: string. Default value: none.

Response header

Response header

Name	Description
Access-Control-Allow-Origin	The Origin contained in a request. If the field is not allowed in a request, the request does not contain it. Type: string.
Access-Control-Allow-Methods	The HTTP method used by a request. If the field is not allowed in a request, the request does not contain it. Type: string.
Access-Control-Allow-Headers	The list of header fields carried in a request. If the request contains a forbidden header field, this header field is not contained and the request is rejected. Type: string.

Name	Description
Access-Control-Expose-Headers	The list of header fields that are accessible to JavaScript applications on a client. Type: string.
Access-Control-Max-Age	The maximum duration for the browser to cache preflight results, in seconds. Type: integer.

Examples

Sample request:

```
OPTIONS /testobject HTTP/1.1
Host: ***.regionid.example.com
Date: Fri, 24 Feb 2012 05:45:34 GMT
Origin:http://www.example.com
Access-Control-Request-Method:PUT
Access-Control-Request-Headers:x-oss-test
```

Sample response:

```
HTTP/1.1 200 OK
x-oss-request-id: 5***C
Date: Fri, 24 Feb 2012 05:45:34 GMT
Access-Control-Allow-Origin: http://www.example.com
Access-Control-Allow-Methods: PUT
Access-Control-Expose-Headers: x-oss-test
Connection: keep-alive
Content-Length: 0
Server: AliyunOSS
```

2.4.1.10. OSS error response

If an error occurs when you access OSS, OSS returns the error code and error message so that you can easily locate and rectify the error.

OSS error response format

If an error occurs when you access OSS, OSS returns an HTTP status code 3xx, 4xx, or 5xx and a message body in application/xml format.

Example of an error response body:

```
<? xml version="1.0" ? >
<Error xmlns=" http://doc.oss-cn-hangzhou.aliyuncs.com" >
 <Code>
 AccessDenied
 </Code>
 <Message>
 Query-string authentication requires the Signature, Expires, and OSSAccessKeyId parameters
 </Message>
 <RequestId>
 1D842BC5425544BB
 </RequestId>
 <HostId>
 regionid.example.com
 </HostId>
</Error>
```

All error message bodies include the following elements:

- Code: the error code that OSS returns to the user.
- Message: the detailed error message provided by OSS.
- RequestId: the UUID of a request. If you need help from OSS development engineers to handle an exception, provide them with the Request ID.
- HostId: the ID of a host in the accessed OSS cluster, which is the same as the host ID specified in the request.

For special error information elements, see specific request descriptions.

OSS error codes

The following table lists the OSS error codes.

OSS error codes

Error code	Description	HTTP status code
AccessDenied	The error message returned when the access is denied.	403
BucketAlreadyExists	The error message returned when the bucket already exists.	409
BucketNotEmpty	The error message returned when the bucket is not empty.	409
EntityTooLarge	The error message returned when the entity is too large.	400
EntityTooSmall	The error message returned when the entity is too small.	400
FieldItemTooLong	The error message returned when the total length of all form fields in the post request exceeds the limit.	400

Error code	Description	HTTP status code
FilePartInterity	The error message returned when the object part has changed.	400
FilePartNotExist	The error message returned when the object part does not exist.	400
FilePartStale	The error message returned when the object part has expired.	400
IncorrectNumberOfFilesInPOSTRequest	The error message returned when the number of objects in the post request is incorrect.	400
InvalidArgument	The error message returned when the parameter format is incorrect.	400
InvalidAccessKeyId	The error message returned when the AccessKey ID does not exist.	403
InvalidBucketName	The error message returned when the bucket name is invalid.	400
InvalidDigest	The error message returned when the digest is invalid.	400
InvalidEncryptionAlgorithmError	The specified entropy coding-based encryption algorithm is incorrect.	400
InvalidObjectName	The error message returned when the object name is invalid.	400
InvalidPart	The error message returned when the part is invalid.	400
InvalidPartOrder	The error message returned when the part sequence is invalid.	400
InvalidPolicyDocument	The error message returned when the policy document is invalid.	400
InvalidTargetBucketForLogging	The error message returned when the logging operation involves an invalid target bucket.	400
InternalError	The error message returned when an internal error occurs in OSS.	500
MalformedXML	The error message returned when the XML format is invalid.	400
MalformedPOSTRequest	The error message returned when the format of the post request body is invalid.	400
MaxPOSTPreDataLengthExceededError	The error message returned when the post request body, excluding the object content uploaded, is too large.	400
MethodNotAllowed	The error message returned when the method is not supported.	405
MissingArgument	The error message returned when a parameter is not specified.	411
MissingContentLength	The error message returned when the content length is not configured.	411

Error code	Description	HTTP status code
NoSuchBucket	The error message returned when no such bucket exists.	404
NoSuchKey	The error message returned when no such object exists.	404
NoSuchUpload	The error message returned when no such multipart upload ID exists.	404
NotImplemented	The error message returned when the method cannot be implemented.	400
PreconditionFailed	The error message returned when the preconditioning fails.	412
RequestTimeTooSkewed	The error message returned when the duration between the request sending time and the server responding time exceeds 15 minutes.	403
RequestTimeout	The error message returned when the request timed out.	400
RequestIsNotMultiPartContent	The error message returned when the content-type value specified in the post request is invalid.	400
SignatureDoesNotMatch	The error message returned when the signature is incorrect.	403
TooManyBuckets	The error message returned when the number of the user's buckets exceeds the limit.	400

Operations not supported by OSS

If an operation not supported by OSS is performed to access a resource, OSS returns the 405 Method Not Allowed error.

Example of an invalid request:

```
ABC /1.txt HTTP/1.1
Host: bucketname.regionid.example.com
Date: Thu, 11 Aug 2016 03:53:40 GMT
Authorization: signatureValue
```

Sample response:

```
HTTP/1.1 405 Method Not Allowed
Server: AliyunOSS
Date: Thu, 11 Aug 2016 03:53:44 GMT
Content-Type: application/xml
Content-Length: 338
Connection: keep-alive
x-oss-request-id: 57ABF6C8BC4D25D86CBA5ADE
Allow: GET DELETE HEAD PUT POST OPTIONS
<? xml version="1.0" encoding="UTF-8"? >
<Error>
 <Code>MethodNotAllowed</Code>
 <Message>The specified method is not allowed against this resource. </Message>
 <RequestId>57ABF6C8BC4D25D86CBA5ADE</RequestId>
 <HostId>bucketname.regionid.example.com</HostId>
 <Method>abc</Method>
 <ResourceType>Bucket</ResourceType>
</Error>
```

Note If the accessed resource is /bucket/, ResourceType must be set to bucket. If the accessed resource is /bucket/object, ResourceType must be set to object.

Operations supported by OSS but not supported by parameters

If parameters not supported by OSS are added to an operation request supported by OSS (For example, the If-Modified-Since parameter is added to the PUT operation request.), OSS returns the 400 Bad Request error.

Example of an invalid request:

```
PUT /abc.zip HTTP/1.1
Host: bucketname.regionid.example.com
Accept: */*
Date: Thu, 11 Aug 2016 01:44:50 GMT
If-Modified-Since: Thu, 11 Aug 2016 01:43:51 GMT
Content-Length: 363
```

Sample response:

```
HTTP/1.1 400 Bad Request
Server: AliyunOSS
Date: Thu, 11 Aug 2016 01:44:54 GMT
Content-Type: application/xml
Content-Length: 322
Connection: keep-alive
x-oss-request-id: 57ABD896CCB80C366955187E
x-oss-server-time: 0
<? xml version="1.0" encoding="UTF-8"? >
<Error>
 <Code>NotImplemented</Code>
 <Message>A header you provided implies functionality that is not implemented. </Message>
 <RequestId>57ABD896CCB80C366955187E</RequestId>
 <HostId>bucketname.regionid.example.com</HostId>
 <Header>If-Modified-Since</Header>
</Error>
```

2.4.1.11. S3 API compatibility instructions

OSS provides S3 API compatibility that allows seamless migration of data from Amazon S3 to Alibaba Cloud OSS. After data is migrated from Amazon S3 to OSS, you can still use S3 APIs to access OSS. You only need to configure your S3 client application as follows:

1. Acquire the AccessKeyId and AccessKeySecret of your OSS primary account and sub-account, and configure the acquired AccessKeyID and AccessKeySecret in the client and SDK you use.
2. Configure the endpoint for client connection to OSS endpoint.

Use S3 APIs to access OSS after migration

Take note of the following when you use S3 APIs to access OS after the migration from S3 to OSS.

- Path style and virtual hosted style

  Virtual hosted style supports accessing OSS by placing the bucket into the host header. For security reasons, OSS only supports virtual hosted style access. Therefore, configurations on your client application are required after the migration from S3 to OSS. Some S3 tools use path style access by default, which also requires proper configurations. Otherwise, OSS may return errors and prohibit access.

- Permissions defined by OSS are not quite the same as those defined by S3. OSS supports only three canned ACL modes in S3: private, public-read, and public-read-write. Adjust the permissions as required after the migration. For more information about their differences, see Comparison of permission definitions between OSS and S3.

Comparison of permission definitions between OSS and S3

Object	Amazon S3 permissions	Amazon S3	Apsara Stack OSS
Bucket	READ	With the List permission on the bucket.	For all objects in the bucket, if no object permission is set for an object, the object is readable.
	WRITE	Objects in the bucket are writable or overwritable.	- If objects do not exist in a bucket, you can write the objects to the bucket directly. - If objects already exist in a bucket and no object permission is set for the objects, you can overwrite the objects. - initiate multipart upload is allowed.
	READ_ACP	Read bucket ACLs.	Only the bucket owner and the authorized sub-account have the permission of reading bucket ACLs.
	WRITE_ACP	Set the ACL for a bucket.	Only the bucket owner and the authorized sub-account have the permission of configuring bucket ACLs.
Object	READ	Objects are readable.	Objects are readable.
	WRITE	N/A	Objects are overwritable.
	READ_ACP	Read object ACLs.	Only the bucket owner and the authorized sub-account have the permission of reading object ACLs.
	WRITE_ACP	Set the ACL for an object.	Only the bucket owner and the authorized sub-account have the permission of configuring object ACLs.

- Storage Type

  OSS supports the Standard, IA, and Archive storage classes, which correspond to STANDARD, STANDARD_IA, and GLACIER, respectively, in Amazon S3.

  Different from Amazon S3, OSS does not support specifying the storage class directly when uploading an object. The storage class of the object is determined by that of the bucket. OSS supports three bucket storage classes: Standard, IA, and Archive. You can use the lifecycle rules to automatically transition objects between storage classes.

  To read an Archive object in OSS, restore it first by initiating a restore request. Different from S3, OSS does not allow setting the lifetime of the restored (active) copy. Therefore, OSS ignores the lifetime (Days) set in the S3 API. The restored state lasts for one day by default, and can be prolonged to seven days at most. After that, the object enters the frozen state again.

- ETag

- For objects uploaded by using the PUT method, the ETag of an OSS object and that of an Amazon S3 object differ in case sensitivity. The ETag is in upper case for an OSS object and in lower case for an S3 object. If ETag validation is available in your client, ignore the case sensitivity.
- For objects uploaded by using the multipart upload method, OSS uses an ETag calculation method different from that used by S3.

S3 APIs compatible with OSS

- Bucket operations:
  - Delete Bucket
  - Get Bucket (list objects)
  - Get Bucket ACL
  - Get Bucket lifecycle
  - Get Bucket location
  - Get Bucket logging
  - Head Bucket
  - Put Bucket
  - Put Bucket ACL
  - Put Bucket lifecycle
  - Put Bucket logging
- Object operations:
  - Delete Object
  - Delete Objects
  - Get Object
  - Get Object ACL
  - Head Object
  - Post Object
  - Put Object
  - Put Object Copy
  - Put Object ACL
- Multipart operations:
  - Abort Multipart Upload
  - Complete Multipart Upload
  - Initiate Multipart Upload
  - List Parts
  - Upload Part
  - Upload Part Copy

2.4.2. SDK reference

2.4.2.1. Java SDK

2.4.2.1.1. Preface

Download the SDK

- The latest version of Java SDK 2.5.0: aliyun_java_sdk_20170222.zip
- GitHub URL:

Overview

- The OSS Java SDK is applicable to JDKs V6 and later.
- This document describes how to install and use the OSS Java SDK and relevant precautions.
- This document assumes that you have enabled Apsara Stack OSS and created an AccessKey ID and AccessKey Secret.

Compatibility

For SDKs V2.x.x:

- API: compatible
- Namespace: compatible

For SDKs V1.0.x:

- API: compatible
- Namespace: incompatible

  In SDKs V2.0.0, the Table Store-relevant code included in V1.0.x has been removed, the package structure has been adjusted, and the package names *com.aliyun.openservices.** and *com.aliyun.openservices.oss.** are replaced with *com.aliyun.oss.**.

2.4.2.1.2. Installation

Preparation

Applicable to JDK 6 and later.

Installation methods

Method 1 (recommended): Add a dependency to your Maven project.

To use the OSS Java SDK in Maven, you need only to add the corresponding dependencies to the pom.xml file. Take OSS Java SDK 2.5.0 as an example. Add the following content to the dependencies tag:

```
<dependency>
    <groupId>com.aliyun.oss</groupId>
    <artifactId>aliyun-sdk-oss</artifactId>
    <version>2.5.0</version>
</dependency>
```

Method 2: Import a JAR package to your Eclipse project.

Take OSS Java SDK 2.5.0 as an example. Perform the following steps:

1. Download the Java SDK: aliyun_java_sdk_20170222.zip.
2. Decompress the SDK.
3. Copy the *aliyun-sdk-oss-<versionId>.jar* file and all files in the lib folder in the decompressed package to your project.
4. Select your project in Eclipse, right-click, and choose **Properties > Java Build Path > Add JARs** from the shortcut menu.
5. Select all JAR packages that you have copied in Step 3.

When you have completed the preceding steps, you can use the OSS Java SDK in Eclipse.

Sample project

The OSS Java SDK provides Maven- and Ant-based sample projects. You can compile and run the sample projects on a local device. You can also develop your own applications based on the sample projects.

- Maven sample project: aliyun-oss-java-sdk-demo-mvn.zip
- Ant sample project: aliyun-oss-java-sdk-demo-ant.zip

> **Note**
>
> - Before compiling and running the project, set *HelloOSS.java* in `endpoint/accessKeyId/accessKeySecret/bucketName` to your real information.
> - For more information about how to compile and run the project, see *README.md* in the project directory.

Sample program

The OSS Java SDK provides a variety of sample programs for your reference or use. You can obtain a sample program by using either of the following methods:

- View and download the required project on GitHub. The src/samples directory in the OSS Java SDK on github contains sample programs.
- Download the OSS Java SDK, such as aliyun_java_sdk_20170222.zip. Decompress the package to obtain sample programs in aliyun_java_sdk_20170222/samples.

The following table describes the sample files in the sample program.

Sample file	Content
GetStartedSample.java	Shows basic upload and download operations.
SimpleGetObjectSample.java	Shows how to download objects.
ListObjectsSample.java	Shows how to list objects.
DeleteObjectsSample.java	Shows how to delete objects simultaneously.
AppendObjectSample.java	Shows how to use append upload.
ObjectMetaSample.java	Shows how to use Object Metadata.

Sample file	Content
CreateFolderSample.java	Shows how to create a folder. For more information about OSS folders, see the folder.
UploadSample.java	Shows how to use resumable upload.
DownloadSample.java	Shows how to use resumable download.
ImageSample.java	Shows how to use the image service.
PostObjectSample.java	Shows how to use PostObject. The implementation is not dependent on the Java SDK.
GetProgressSample.java	Shows how to use upload and download progress bars.
CallbackSample.java	Shows how to perform upload callback.
CRCSample.java	Shows how to perform CRC verification for uploads and downloads.
BucketOperationsSample.java	Shows how to set a bucket, including the ACL, lifecycle, access logging, hotlinking, and CORS.
MultipartUploadSample.java	We recommend that you use resumable upload (uploadFile) for concurrent uploads implemented by the multipart upload API.
ConcurrentGetObjectSample.java	We recommend that you use resumable download (downloadFile) for concurrent downloads implemented by downloads within a specified range.
UploadPartCopySample.java	Shows how to perform the multipart copy operation for large objects.

2.4.2.1.3. Initialization

OssClient is the Java client of OSS. It provides a series of APIs for you to interact with OSS and operate and manage OSS resources such as buckets and objects. To use the Java SDK to initiate a request, you must initialize an OssClient instance and modify the default configuration items of ClientConfiguration as needed.

Set an AccessKey

To access Apsara Stack OSS, you need a pair of valid access keys (AccessKey ID and AccessKey Secret) for signature authentication.

After obtaining the AccessKey ID and AccessKey Secret, follow the steps for initialization.

Create an OssClient instance

Create an OssClient instance based on the OSS endpoint.

The following code provides an example of how to create an OssClient instance:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient client = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Access OSS.
// Close your client.
client.shutdown();
```

Note

- You can create one or more OssClient instances for your project.
- OssClient instances can be used concurrently.
- OSS supports HTTPS. Use HTTPS to meet higher security requirements.
- The OssClient instance becomes unavailable after it is closed.

Create an OssClient instance based on the IP address.

You need to use an IP address as the endpoint under some special circumstances (such as a private domain name). OSS Java SDK V2.1.2 and later automatically detect IP addresses, and it is no longer required to call setSLDEnabled for configurations. In OSS Java SDK V2.1.2 and earlier, the following code must be used to set setSLDEnabled during IP address initialization:

```
// Fill in the actual IP address.
String endpoint = "http://10. *. *. 10";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create a ClientConfiguration instance and modify the default parameters based on your requirements
ClientConfiguration conf = new ClientConfiguration();
// Enable the second-level domain access to the OSS. This option is disabled by default
conf.setSLDEnabled(true)
// Create an OssClient instance.
OSSClient client = new OSSClient(endpoint, accessKeyId, accessKeySecret, conf);
// Access OSS.
// Close your client.
client.shutdown();
```

Create an OssClient instance through STS.

The following code provides an example of how to use STS to create an OssClient instance:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// Set accessKeyId, accessKeySecret, and securityToken for a temporary account.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
String securityToken = "<yourSecurityToken>";
// Create an OssClient instance.
OSSClient client = new OSSClient(endpoint, accessKeyId, accessKeySecret, securityToken);
// Access OSS.
// Close your client.
client.shutdown();
```

Set the OssClient instance

To modify the default configuration of the OssClient instance, import the ClientConfiguration instance when creating the OssClient instance. ClientConfiguration is an OssClient configuration class, which can be used to set parameters such as the proxy, connection timeout value, and maximum number of connections. The following table lists the configurable parameters of ClientConfiguration.

Parameter	Description	Method
MaxConnections	The maximum number of HTTP connections allowed to be established. Default value: 1,024.	ClientConfiguration.setMaxConnections
SocketTimeout	The timeout value for data transmission at the socket layer, in milliseconds. Default value: 50,000.	ClientConfiguration.setSocketTimeout
ConnectionTimeout	Specifies the timeout time in milliseconds when connections are established. Default value: 50,000.	ClientConfiguration.setConnectionTimeout
ConnectionRequestTimeout	Specifies the timeout time in milliseconds for obtaining connections from the connection pool. No timeout is configured by default. No timeout is configured by default.	ClientConfiguration.setConnectionRequestTimeout
IdleConnectionTime	If the idle time exceeds the specified value of this parameter, the connection is closed. Unit: milliseconds. Default value: 60,000.	ClientConfiguration.setIdleConnectionTime

Parameter	Description	Method
MaxErrorRetry	Specifies the maximum number of retry attempts in the case of a request error. Default value: 3.	ClientConfiguration.setMaxErrorRetry
SupportCname	Specifies whether CNAME can be used to set an endpoint. CNAME is used by default.	ClientConfiguration.setSupportCname
SLDEnabled	Specifies whether access with the second-level domain is enabled. Access with the second-level domain is disabled by default.	ClientConfiguration.setSLDEnabled
Protocol	The protocol (HTTP or HTTPS) used to connect to OSS. Default value: HTTP.	ClientConfiguration.setProtocol
UserAgent	The user agent (the User-Agent field in the HTTP header). Default value: aliyun-sdk-java.	ClientConfiguration.setUserAgent
ProxyHost	The IP address to access the proxy host.	ClientConfiguration.setProxyHost
ProxyPort	The port for the proxy host.	ClientConfiguration.setProxyPort
ProxyUsername	The username verified by the proxy host.	ClientConfiguration.setProxyUsername
ProxyPassword	The password verified by the proxy host.	ClientConfiguration.setProxyPassword

The following code provides an example of how to use ClientConfiguration to set the OssClient parameters:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create a ClientConfiguration instance.
ClientConfiguration conf = new ClientConfiguration();
// Set the maximum number of connections used by the OssClient instance. The default value is 1,024.
conf.setMaxConnections(200);
// Set the request timeout value. The default value is 50 seconds.
conf.setSocketTimeout(10000);
// Set the number of retries after a failed request. The default value is three retries.
conf.setMaxErrorRetry(5);
// Create an OssClient instance.
OSSClient client = new OSSClient(endpoint, accessKeyId, accessKeySecret, conf);
// Access OSS.
// Close your client.
client.shutdown();
```

2.4.2.1.4. Quick start

This topic describes how to quickly use the OSS Java SDK to complete routine operations, such as create buckets, upload objects, and download objects.

Initialize OssClient

Before sending an HTTP request to OSS, you must create an OssClient instance.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";

// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);

// Access OSS.

// Close your client.
ossClient.shutdown();
```

Create a bucket

A bucket is a global namespace in OSS used to store objects. It is equivalent to a data container. The following code provides an example of how to create a bucket:

```
ossClient.createBucket("<bucketName>");
```

Upload an object

The following code provides an example of how to upload an object to OSS:

```
String content = "Hello OSS";
ossClient.putObject("<bucketName>", "<key>", new ByteArrayInputStream(content.getBytes()));
```

> **Note** You can use the Java SDK to upload the object to OSS through InputStream.

Download an object

The following code provides an example of how to obtain the text content of an object:

```
OSSObject ossObject = ossClient.getObject("<bucketName>", "<key>"));
InputStream in = ossObject.getObjectContent();
if (content ! = null) {
   BufferedReader reader = new BufferedReader(new InputStreamReader(content));
   while (true) {
      String line = reader.readLine();
      if (line == null) break;
      System.out.println("\n" + line);
   }
   content.close();
}
```

Note

- Call `OSSClient.GetObject` to return an OSSObject instance which contains the object content and its Object Meta.
- Call `OSSObject.GetObjectContent` to obtain the input stream of an object. You can read the input stream to obtain the object content. Close the stream after use.

List objects

After uploading objects to a bucket, you may need to view the objects in the bucket. The following code provides an example of how to list the objects in a specified bucket:

```
ObjectListing objectListing = ossClient.listObjects("<bucketName>");
for (OSSObjectSummary objectSummary : objectListing.getObjectSummaries()) {
   System.out.println(" - " + objectSummary.getKey() + "  " +
         "(size = " + objectSummary.getSize() + ")");
}
```

Call `OSSClient#listObjects` to return an ObjectListing instance which contains the response of the listObject request. Call `ObjetListing#getObjectSummaries` to obtain all object descriptive information.

Note The preceding code can be used to list 100 objects by default.

Delete an object

The following code provides an example of how to delete a specified object:

```
ossClient.deleteObject("<bucketName>", "<key>")
```

Note

- If no exceptions are thrown when the OSS Java SDK completes the operation, the returned value is valid. If an exception is thrown, the operation failed and the returned data is invalid.
- For the complete code, see GitHub.

2.4.2.1.5. Manage buckets

Create a bucket

You can use OSSClient.createBucket to create a bucket. The following code provides an example of how to create a bucket:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";

// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);

// Create a bucket.
String bucketName = "<your-oss-bucket-name>";
ossClient.createBucket(bucketName);

// Close your client.
ossClient.shutdown();
```

Note The bucket name must be globally unique.

The ACL of the bucket created by the preceding code is private. When creating a bucket, you can specify the ACL of the bucket. The following code provides an example:

```
CreateBucketRequest createBucketRequest= new CreateBucketRequest(bucketName);
// Set the ACL for a bucket.
createBucketRequest.setCannedACL(CannedAccessControlList.PublicRead);
ossClient.createBucket(createBucketRequest);
```

List buckets

You can use `OSSClient.listBuckets` to list buckets of a specified user.

- Simple list

  The following code provides an example of how to list the buckets of a specified user in the simple mode:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirem
ents.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";

// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);

// List buckets.
List<Bucket> buckets = ossClient.listBuckets();
for (Bucket bucket : buckets) {
   System.out.println(" - " + bucket.getName());
}

// Close your client.
ossClient.shutdown();
```

  You can use the preceding code to return a maximum of 100 buckets to meet your needs. When listing buckets, you can specify the prefix, marker, and maxkeys parameters to filter the list of buckets and implement flexible query features.

Parameter	Description
prefix	Only the buckets whose names match a specified prefix are returned. If this parameter is not specified, prefix information is not used as a filter.
marker	The starting position of the object list. Objects are sorted in the alphabetical order and those objects following this marker are listed. If this parameter is not specified, all entries are returned from the start.
max keys	The maximum number of buckets returned for one request. If this parameter is not specified, the default value 100 is used. The maximum value cannot exceed 1,000.

- Specify a prefix for listing.

```
ListBucketsRequest listBucketsRequest = new ListBucketsRequest();
listBucketsRequest.setPrefix("<yourBucketPrefix>");
for (Bucket bucket : ossClient.listBuckets()) {
   System.out.println(" - " + bucket.getName());
}
```

- Specify the max keys for listing.

```
ListBucketsRequest listBucketsRequest = new ListBucketsRequest();
listBucketsRequest.setMaxKeys(500);
for (Bucket bucket : ossClient.listBuckets()) {
   System.out.println(" - " + bucket.getName());
}
```

Delete a bucket

You can use the OSSClient.deleteBucket API to delete a bucket. The following code provides an example of how to delete a bucket:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";

// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);

// Delete a bucket.
ossClient.deleteBucket("<bucketName>");

// Close your client.
ossClient.shutdown();
```

> Note
>
> - You cannot delete a non-empty bucket (which contains objects or parts from multipart upload).
> - To delete a non-empty bucket, you must first delete all objects and parts from it.

Determine whether a bucket exists

You can use the OSSClient.doesBucketExist API to determine whether a bucket exits. The following code provides an example of how to determine whether a specified bucket exists:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";

// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);

boolean exists = ossClient.doesBucketExist("<bucketName>");

// Close your client.
ossClient.shutdown();
```

Set the ACL for a bucket

Bucket ACLs are classified into three types: private, public-read, and public-read-write. You can use the OSSClient.setBucketAcl API to set the ACL for a bucket.

ACL	Java SDK value
private	CannedAccessControlList.Private
public-read	CannedAccessControlList.PublicRead
public-read-write	CannedAccessControlList.PublicReadWrite

The following code provides an example of how to set the ACL for a bucket:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";

// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);

// Set the ACL for a bucket.
ossClient.setBucketAcl("<bucketName>", CannedAccessControlList.Private);

// Close your client.
ossClient.shutdown();
```

Obtain the ACL of a bucket

You can use the OSSClient.getBucketAcl API obtain the ACL of a bucket. The following code provides an example of how to obtain the ACL of a bucket:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";

// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);

AccessControlList acl = ossClient.getBucketAcl("<bucketName>");
// Obtain the ACL of the bucket.
System.out.println(acl.toString());

// Close your client.
ossClient.shutdown();
```

Obtain the location of a bucket

The location of a bucket is the region to which this bucket belongs.

You can use `OSSClient.getBucketLocation` to obtain the ACL of a bucket. The following code provides an example of how to obtain the location of a bucket:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";

// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);

String location = ossClient.getBucketLocation("<bucketName>");
System.out.println(location);

// Close your client.
ossClient.shutdown();
```

Obtain the information about a bucket

The information about a bucket includes Location, CreationDate, Owner, and ACL. The following code provides an example of how to obtain the information about a bucket:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";

// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);

BucketInfo info = ossClient.getBucketInfo("<bucketName>");
// Obtain the location of the bucket.
info.getBucket().getLocation();
// Obtain the date when the bucket is created.
info.getBucket().getCreationDate();
// Obtain the owner of the bucket.
info.getBucket().getOwner();
// Obtain the ACL of the bucket.
info.getGrants();

// Close your client.
ossClient.shutdown();
```

2.4.2.1.6. Upload objects

Objects are the basic data units for user operations in OSS.

Upload methods

The OSS Java SDK provides a variety of object upload methods. You can upload an object through any of the following methods:

- Streaming upload
- Local file upload
- Append upload
- Multipart upload
- Resumable upload

The size of objects for streaming upload, local file upload, and append upload operations cannot exceed 5 GB. If the object size is large, use the multipart upload method. The total size of parts for multipart upload cannot exceed 48.8 TB. Resumable upload supports concurrent resumable upload tasks and customization of part sizes. Resumable upload is the encapsulated and enhanced version of multipart upload. We recommend that you use resumable upload to upload large objects.

Simple upload

Simple upload includes streaming upload and local file upload. Streaming upload uses InputStream as the source object. Local file upload uses a local file as the source object.

For the complete simple upload code, see GitHub.

- Streaming upload

  You can use `ossClient.putObject` to upload InputStream to OSS.

  - Upload a string

    Use the following code to upload a string:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Upload a string.
String content = "Hello OSS";
ossClient.putObject("<yourBucketName>", "<yourKey>", new ByteArrayInputStream(content.getByt
es()));
// Close your OSSClient.
ossClient.shutdown();
```

  - Upload a byte array

    Use the following code to upload a byte array:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId,accessKeySecret);
// Upload a byte array.
byte[] content = "Hello OSS".getBytes();
ossClient.putObject("<yourBucketName>", "<yourKey>", new ByteArrayInputStream(content));
// Close your OSSClient.
ossClient.shutdown();
```

- Upload a network stream

  Use the following code to upload a network stream:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Upload a network stream.
InputStream inputStream = new URL("https://www.aliyun.com/").openStream();
ossClient.putObject("<yourBucketName>", "<yourKey>", inputStream);
// Close your OSSClient.
ossClient.shutdown();
```

- Upload a file stream

  Use the following code to upload a file stream:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Upload a file stream.
InputStream inputStream = new FileInputStream("localFile");
ossClient.putObject("<yourBucketName>", "<yourKey>", inputStream);
// Close your OSSClient.
ossClient.shutdown();
```

- Local file upload

  Use the following code to upload a local file to OSS:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirem
ents.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Start to upload your local file.
ossClient.putObject("<yourBucketName>", "<yourKey>", new File("localFile"));
// Close your OSSClient.
ossClient.shutdown();
```

- Set object metadata

  Object metadata describes the attributes of objects uploaded to OSS. These attributes are classified into two types: HTTP standard attributes (HTTP headers) and User Meta (user-defined object metadata). You can set object metadata during object uploads in various modes (streaming upload, local file upload, append upload, multipart upload, and resumable upload) or object copy operations. The name of object metadata is case-insensitive.

  - HTTP standard attributes

    OSS allows you to customize fields in HTTP headers. For information about HTTP headers, see RFC 2616. The following table describes typical fields in HTTP headers.

Field	Description	Default value
Content-MD5	The MD5 value for object data verification. After this value is specified, OSS enables MD5 verification for the object content and compares the MD5 value that you have provided with the MD5 value of the object. OSS returns an error if any inconsistencies are found.	None.
Content-Type	The object MIME. It defines the object type and Webpage encoding mode and determines the form and encoding mode used by the browser to read the object. If not specified, the object MIME is generated based on the key or object name extension. If no extensions are available, the default value applies.	application/octet-stream.
Content-Disposition	The instructions for how the MIME user agent displays an attached object, whether it opens or downloads the attached object, and the object name.	None.
Content-Length	The length of the uploaded object. Excess length is truncated. If the data falls short of the length, the actual data length applies.	The validity period of the stream or object.
Expires	The expiration time of the cache. The time format is GMT.	None.

Field	Description	Default value
Cache-Control	The Webpage caching behavior specified when the object is downloaded.	None.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
String content = "Hello OSS";
// Create object metadata for the object to be uploaded.
ObjectMetadata meta = new ObjectMetadata();
// Set the length of the object to be uploaded.
meta.setContentLength(content.length());
// Set MD5 verification for the object to be uploaded.
String md5 = BinaryUtil.toBase64String(BinaryUtil.calculateMd5(content.getBytes()));
meta.setContentMD5(md5);
// Set the type of the uploaded content.
meta.setContentType("text/plain");
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Start to upload your local file.
ossClient.putObject("<yourBucketName>", "<yourKey>", new ByteArrayInputStream(content.getByt
es()), meta);
// Close your OSSClient.
ossClient.shutdown();
```

Note

- ObjectMetadata provides frequently-used HTTP header settings, such as Content-MD5, Content-Type, Content-Length, Content-Disposition, Content-Encoding, Expires, and x-oss-server-side-encryption.
- Use ObjectMetadata.setHeader(String key, Object value) to set the header.

- User Meta

  OSS allows you to customize object metadata to describe objects.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
String content = "Hello OSS";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Create object metadata for the object to be uploaded.
ObjectMetadata meta = new ObjectMetadata();
// Set the name of the User Meta to my-data.
meta.addUserMetadata("property", "property-value");
// Start to upload your local file.
ossClient.putObject("<yourBucketName>", "<yourKey>", new ByteArrayInputStream(content.getByt
es()), meta);
// Close your OSSClient.
ossClient.shutdown();
```

  Note

  - The preceding code defines a piece of User Meta named property with a value of property-value.
  - Use OSSClient.getObjectMetadata to obtain metadata of an object.
  - Object metadata is downloaded along with the object.
  - An object may contain multiple pieces of object metadata, the total size of which cannot exceed 8 KB.

- Create a simulated folder

  OSS does not use the folder concept. OSS stores all elements as objects. Creating a simulated folder is equivalent to creating an object with a size of 0. The object can then be uploaded and downloaded. The console displays any objects ending with a forward slash (/) as a folder.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirem
ents.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
final String keySuffixWithSlash = "parent_directory/";
ossClient.putObject("<bucketName>", keySuffixWithSlash, new ByteArrayInputStream(new byte[0]));
// Close your OSSClient.
ossClient.shutdown();
```

Note

- Creating a simulated folder is equivalent to creating an object whose name ends with a forward slash (/).
- This object can be uploaded and downloaded as a normal object, but the OSS console displays objects ending with a forward slash (/) as folders.
- To create a directory with multiple levels, you can directly specify the directory structure to the last level. For example, to create the dir1/dir2/dir3/ directory, you can directly create dir1/dir2/dir3/ instead of creating dir1/ and then dir1/dir2/.

Append upload

Through simple upload, multipart upload, and resumable upload, normal objects are created with fixed content. They are read-only and cannot be modified. If you want to modify the object content, you must upload an object of the same name to overwrite the existing one. This is a major difference between OSS and typical file systems. This feature is not suitable for scenarios such as video surveillance and live video streaming, because video data is constantly produced in real time.

OSS allows you to use append object to append content directly to the end of an object. Objects uploaded by using this method are appendable objects, whereas objects uploaded by using other methods are normal objects. The appended data is instantly readable.

You can use `OSSClient.appendObject` to enable append upload.

```
AppendObjectResult appendObject(AppendObjectRequest appendObjectRequest)
```

The following table describes the parameters that can be set for AppendObjectRequest.

Parameter	Description	Method
BucketName	The name of the bucket that stores the appendable object.	setBucketName(String bucketName)
Key	The name of the object saved in OSS.	setKey(String key)

Parameter	Description	Method
InputStream	The content to be appended. Either InputStream or File must be set.	setInputStream(InputStream inputStream)
File	The content to be appended. Either InputStream or File must be set.	setFile(File file)
ObjectMetadata	The object metadata. This parameter is valid from the first append.	setMetadata(ObjectMetadata metadata)
Position	The append position of the object.	setPosition(Long position)

The following table describes parameters of AppendObjectResult.

Parameter	Description	Method
nextPosition	The position that must be provided in the next request. The position indicates the current object length.	Long getNextPosition()
objectCRC64	The 64-bit CRC value of the object. This value is calculated based on ECMA-182.	String getObjectCRC64()

Note For the complete append upload code, see GitHub.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
String content = "Hello OSS";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
AppendObjectRequest appendObjectRequest = new AppendObjectRequest("<yourBucketName>",
    "<yourKey>", new ByteArrayInputStream(content.getBytes()));
// Start the first append.
appendObjectRequest.setPosition(0L);
AppendObjectResult appendObjectResult = ossClient.appendObject(appendObjectRequest);
// Start the second append.
appendObjectRequest.setPosition(appendObjectResult.getNextPosition());
appendObjectResult = ossClient.appendObject(appendObjectRequest);
// Start the third append.
appendObjectRequest.setPosition(appendObjectResult.getNextPosition());
appendObjectResult = ossClient.appendObject(appendObjectRequest);
// Close your OSSClient.
ossClient.shutdown();
```

Note

- You can append an object multiple times. The maximum object size is 5 GB. Use multipart upload to upload larger objects.
- You cannot use `copyObject` for appendable objects.

Resumable upload

You may fail to upload a large object if the network is unstable or the program stops responding. In this case, you have to upload the object again. You can use `OSSClient.uploadFile` to implement resumable upload. The request is UploadFileRequest and contains the following parameters.

Parameter	Description	Configuration method	Required
bucket	The name of the bucket.	Constructor	Yes
key	The name of the object to be uploaded to OSS.	Constructor	Yes

Parameter	Description	Configuration method	Required
uploadFile	The local file to be uploaded.	Constructor or setUploadFile	Yes
partSize	The size of each part to be uploaded. Unit: Byte. Valid values: 100 KB to 5 GB. Default value: 100 KB.	setPartSize	No
taskNum	The number of parts to be uploaded concurrently. Default value: 1.	setTaskNum	No
enableCheckpoint	Specifies whether to enable resumable upload. Default value: false.	setEnableCheckpoint.	No
checkpointFile	The file that stores the checkpoint information. When resumable upload is enabled, you need to record the multipart upload result in this local file. If the upload fails, the uploaded parts are not uploaded again. This file shares the same directory as the file to be uploaded.	setCheckpointFile. Default value: *uploadFile.ucp*.	No
objectMetadata	The metadata of the object.	setObjectMetadata	No
callback	The callback that is sent after the object is uploaded.	setCallback	No

The principle is to split the object to be uploaded into multiple parts and upload them sequentially. When all the parts are uploaded, the upload of the entire object is completed. During the upload, the upload progress is recorded in the checkpoint file. If the upload of any part fails, the next upload attempt starts from the position recorded in the checkpoint file. This method requires that the same checkpoint file used for the previous upload be used in the next call. The checkpoint file is deleted after the resumable upload is completed.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Configure the resumable upload request.
UploadFileRequest uploadFileRequest = new UploadFileRequest("<yourBucketName>", "<yourKey>");
// Specify the local file to be uploaded.
uploadFileRequest.setUploadFile("<yourLocalFile>");
// Specify the number of concurrent threads for the upload.
uploadFileRequest.setTaskNum(5);
// Specify the size of each part to be uploaded.
uploadFileRequest.setPartSize(1 * 1024 * 1024);
// Enable resumable upload.
uploadFileRequest.setEnableCheckpoint(true);
// Start resumable upload.
ossClient.uploadFile(uploadFileRequest);
// Close your OSSClient.
ossClient.shutdown();
```

Note

- Resumable upload is the encapsulated and enhanced version of multipart upload. It is implemented through multipart upload.
- We recommend that you use multipart upload when the object is large or the network environment is poor.
- You can specify a callback after the upload and object metadata for resumable upload.

Multipart upload

You can split a large object into multiple parts for uploads. Scenarios of multipart upload mode include but are not limited to:

- Resumable upload is required.
- The object to be uploaded is larger than 100 MB.
- The OSS server is frequently disconnected due to poor network conditions.
- The size of the object to be uploaded is unknown.

To enable multipart upload, perform the following steps:

1. Initialize a multipart upload event (InitiateMultipartUpload).
2. Upload the parts sequentially or concurrently (UploadPart).

3. Complete the multipart upload event (CompleteMultipartUpload) or cancel the multipart upload (AbortMultipartUpload) event.

The following section describes how to perform multipart upload:

- Complete multipart upload step by step

  For the complete multipart upload code, see GitHub.

  - Initialize a multipart upload event

    Before transmitting data in the multipart upload mode, you must call OSSClient.initiateMultipartUpload to require OSS to initiate a multipart upload event. The operation returns a globally unique upload ID created by the OSS server to identify this multipart upload event. You can initiate operations based on this upload ID, such as interrupting or querying the multipart upload event.

    The following code provides an example of how to call OSSClient.initiateMultipartUpload to initialize a multipart upload event.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
String bucketName = "<yourBucketName>";
String key = "yourKey";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
InitiateMultipartUploadRequest request = new InitiateMultipartUploadRequest(bucketName, key);
InitiateMultipartUploadResult result = ossClient.initiateMultipartUpload(request);
String uploadId = result.getUploadId();
```

    Note

    - InitiateMultipartUploadRequest is used to specify the name and bucket of the object to be uploaded.
    - In InitiateMultipartUploadRequest, you can set object metadata.
    - The results returned by InitiateMultipartUpload include the upload ID, which uniquely identifies a multipart upload event and will be used in subsequent operations.

  - Upload parts

After initializing a multipart upload event, you can call OSSClient.uploadPart to upload data in parts based on the specified object name and upload ID. Each uploaded part has a part number ranging from 1 to 10,000. For the same upload ID, this part number identifies not only this part of data but also the relevant location of this part in the entire object. If you upload data using the same part number, OSS overwrites the existing data identified by this part number. Aside from the last part, the minimum size of each part is 100 KB. The size of the last part is unlimited. Parts are not necessarily uploaded in order. They can be uploaded by different processes from different servers. OSS sorts the parts based on their part numbers and combines them to obtain the large object.

The following code provides an example of how to call OSSClient.uploadPart to upload parts:

```
List<PartETag> partETags = new ArrayList<PartETag>();
InputStream instream = new FileInputStream(new File("<localFile>"));
UploadPartRequest uploadPartRequest = new UploadPartRequest();
uploadPartRequest.setBucketName(bucketName);
uploadPartRequest.setKey(key);
uploadPartRequest.setUploadId(uploadId);
uploadPartRequest.setInputStream(instream);
// Set the part size. Aside from the last part, the size of each part must be larger than 100 KB.
uploadPartRequest.setPartSize(100 * 1024);
// Set the part number. The range is 1 to 10,000.
uploadPartRequest.setPartNumber(1);
UploadPartResult uploadPartResult = ossClient.uploadPart(uploadPartRequest);
partETags.add(uploadPartResult.getPartETag());
```

Note

- The UploadPart method requires that each part, except the last one, be larger than 100 KB. The UploadPart operation does not immediately verify the size of the uploaded part (because it cannot immediately determine which part is the last one). It verifies the size of the uploaded part only when the multipart upload event is completed.
- OSS includes the MD5 value of the data for each part received by the server in the ETag header and returns the ETag header to the user.
- To ensure that no errors occur during the data transmission over the network, the SDK automatically sets the Content-MD5 value. OSS calculates the MD5 value of the uploaded data and compares it with the MD5 value calculated by the SDK. If the two values are inconsistent, OSS returns the InvalidDigest error code.
- The part number ranges from 1 to 10,000. If a part number is beyond this range, OSS returns the InvalidArgument error code.
- When each part is uploaded, the stream is directed to the starting position of the uploaded part.
- After each part is uploaded, the response from OSS contains a PartETag which combines the ETag and part number of the uploaded part.
- You need to save the PartETag that will be used for completing the multipart upload event. Typically, the PartETag objects are stored in List.

- Complete the multipart upload event

  After uploading all data parts, you must call CompleteMultipartUpload to complete the multipart upload of the entire object. When performing this operation, you must provide a list of all the valid parts (including the part number and ETag). After receiving the list of submitted parts, OSS verifies the validity of all parts one by one. After all the data parts are verified, the OSS combines these parts into a complete object.

  The following code provides an example of how to call OSSClient.completeMultipartUpload to complete a multipart upload task:

```
Collections.sort(partETags, new Comparator<PartETag>() {
    @Override
    public int compare(PartETag p1, PartETag p2) {
        return p1.getPartNumber() - p2.getPartNumber();
    }
});
CompleteMultipartUploadRequest completeMultipartUploadRequest =
        new CompleteMultipartUploadRequest(bucketName, key, uploadId, partETags);
ossClient.completeMultipartUpload(completeMultipartUploadRequest);
```

  > **Note**
  >
  > - The partETags in the preceding code are the list of part ETags saved during multipart upload. They must be sequenced by part numbers in ascending order.
  > - Parts can be out of order.

- Cancel a multipart upload event

  You can call OSSClient.abortMultipartUpload to cancel a multipart upload event based on the upload ID. After a multipart upload event is canceled, you are not allowed to use this upload ID to perform any operations and the uploaded parts are deleted.

  The following code provides an example of how to call `OSSClient.abortMultipartUpload` to cancel a multipart upload event:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Upload a string.
String content = "Hello OSS";
ossClient.putObject("<yourBucketName>", "<yourKey>", new ByteArrayInputStream(content.getByt
es()));
// Cancel multipart upload. The upload ID is from initiateMultipartUpload.
AbortMultipartUploadRequest abortMultipartUploadRequest =
        new AbortMultipartUploadRequest("<yourBucketName>", "<yourKey>", "<uploadId>");
ossClient.abortMultipartUpload(abortMultipartUploadRequest);
// Close your OSSClient.
ossClient.shutdown();
```

- Obtain uploaded parts

  You can list all uploaded parts that are mapped to a specified upload ID. You can call `OSSClient.listParts` to obtain all uploaded parts of an upload event. The following table describes parameters of listParts.

Parameter	Description	Method
UploadId	The upload ID, which is obtained from the response of initiateMultipartUpload.	ListPartsRequest.setUploadId(String uploadId)
MaxParts	The maximum number of parts returned by OSS on each page.	ListPartsRequest.setMaxParts(int maxParts)
PartNumberMarker	The starting position of a specified list. All parts with the part numbers greater than the value of this parameter are listed.	ListPartsRequest.setPartNumberMarker(Integer partNumberMarker)

- Simple list

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// List uploaded parts. The upload ID is from initiateMultipartUpload.
ListPartsRequest listPartsRequest = new ListPartsRequest("<yourBucketName>", "<yourKey>", "<up
loadId>");
PartListing partListing = ossClient.listParts(listPartsRequest);
for (PartSummary part : partListing.getParts()) {
    // Obtain the part numbers, which are specified during the upload.
    part.getPartNumber();
    // Obtain the size of each part.
    part.getSize();
    // Obtain the ETag of each part.
    part.getETag();
    // Obtain the time when parts were last modified before they are uploaded.
    part.getLastModified();
}
// Close your OSSClient.
ossClient.shutdown();
```

> **Note**
>
> - By default, if a MultipartUpload event contains more than 1,000 parts in a bucket, OSS returns the first 1,000 parts. In the response, OSS sets IsTruncated to false and returns NextPartNumberMarker to indicate the next starting position to continue reading the data.
> - If all part upload events fail to be listed on one page, list them on more pages.

- Obtain all uploaded parts

  You can use listParts to list a maximum of 1,000 parts at a time by default. The following code provides an example of how to list more than 1,000 parts:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// List all uploaded parts.
PartListing partListing;
ListPartsRequest listPartsRequest = new ListPartsRequest("<yourBucketName>", "<yourKey>", "<up
loadId>");
do {
   partListing = ossClient.listParts(listPartsRequest);
   for (PartSummary part : partListing.getParts()) {
      // Obtain the part numbers, which are specified during the upload.
      part.getPartNumber();
      // Obtain the size of each part.
      part.getSize();
      // Obtain the ETag of each part.
      part.getETag();
      // Obtain the time when parts were last modified before they are uploaded.
      part.getLastModified();
   }
   listPartsRequest.setPartNumberMarker(partListing.getNextPartNumberMarker());
} while (partListing.isTruncated());
// Close your OSSClient.
ossClient.shutdown()
```

- Obtain all parts by page

  listParts can list 1,000 parts by default. The preceding *Obtain all uploaded parts* section is a special case where 1,000 parts are listed on each page. The following code provides an example of how to list a specified number of parts at a time:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// List all uploaded parts on one or more pages.
PartListing partListing;
ListPartsRequest listPartsRequest = new ListPartsRequest("<yourBucketName>", "<yourKey>", "<up
loadId>");
// Set the maximum number of parts that can be listed on each page to 100.
listPartsRequest.setMaxParts(100);
do {
    partListing = ossClient.listParts(listPartsRequest);
    for (PartSummary part : partListing.getParts()) {
        // Obtain the part numbers, which are specified during the upload.
        part.getPartNumber();
        // Obtain the size of each part.
        part.getSize();
        // Obtain the ETag of each part.
        part.getETag();
        // Obtain the time when parts were last modified before they are uploaded.
        part.getLastModified();
    }
    listPartsRequest.setPartNumberMarker(partListing.getNextPartNumberMarker());
} while (partListing.isTruncated());
// Close your OSSClient.
ossClient.shutdown();
```

- Obtain all multipart upload events of a bucket

  You can call OSSClient.listMultipartUploads to list all multipart upload tasks in execution, that is, the multipart upload tasks that have been initialized but not completed or canceled. The following table describes parameters for OSSClient.listMultipartUploads.

Parameter	Description	Method
Prefix	The prefix that the names of returned objects must contain. Note that if you use a prefix for a query, the returned object name contains the prefix.	ListMultipartUploadsRequest.setPrefix(String prefix)
Delimiter	The character used to group object names. The substring between the specified prefix and the occurrence of the first delimiter is a commonPrefix.	ListMultipartUploadsRequest.setDelimiter(String delimiter)
MaxUploads	The maximum number of multipart upload events returned for one request. The default value is 1,000. The maximum value is 1,000.	ListMultipartUploadsRequest.setMaxUploads(Integer maxUploads)
KeyMarker	The starting position of the multipart upload event list in the response. All multipart upload events whose object names start with a letter that comes after the KeyMarker value in the alphabetic order are listed. KeyMarker can be used together with the UploadIdMarker parameter to specify the starting position of the returned results.	ListMultipartUploadsRequest.setKeyMarker(String keyMarker)
UploadIdMarker	The starting position of the returned results. This parameter is used together with the KeyMarker parameter. If the KeyMarker parameter is not specified, the OSS instance ignores the UploadIdMarker parameter. If the KeyMarker parameter is specified, the query results contain all the multipart upload events that meet the following conditions: objects whose names start with a letter that comes after or is the same as the KeyMarker value in the alphabetical order. The value of the upload ID is greater than that of the UploadIdMarker parameter.	ListMultipartUploadsRequest.setUploadIdMarker(String uploadIdMarker)

The following code provides an example of how to call `OSSClient.listMultipartUploads` to retrieve all multipart upload events of a bucket.

- Simple list of multipart upload events

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
String bucketName = "<yourBucketName>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// List part upload events.
ListMultipartUploadsRequest listMultipartUploadsRequest = new ListMultipartUploadsRequest(buc
ketName);
MultipartUploadListing multipartUploadListing = ossClient.listMultipartUploads(listMultipartUploads
Request);
for (MultipartUpload multipartUpload : multipartUploadListing.getMultipartUploads()) {
   // Obtain the upload ID.
   multipartUpload.getUploadId();
   // Obtain the key of the object.
   multipartUpload.getKey();
   // Obtain the time part upload events were initiated.
   multipartUpload.getInitiated();
}
// Close your OSSClient.
ossClient.shutdown();
```

> **Note**
>
> - If a bucket contains more than 1,000 multipart upload events, OSS returns the first 1,000 events by default. In the response, OSS sets IsTruncated to false and returns NextKeyMarker and NextUploadIdMarker to indicate the next starting position to continue reading the data.
> - If all part upload events fail to be listed on one page, list them on more pages.

- List all upload events

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
String bucketName = "<yourBucketName>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// List part upload events.
MultipartUploadListing multipartUploadListing;
ListMultipartUploadsRequest listMultipartUploadsRequest = new ListMultipartUploadsRequest(buc
ketName);
do {
   multipartUploadListing = ossClient.listMultipartUploads(listMultipartUploadsRequest);
   for (MultipartUpload multipartUpload : multipartUploadListing.getMultipartUploads()) {
      // Obtain the upload ID.
      multipartUpload.getUploadId();
      // Obtain the key of the object.
      multipartUpload.getKey();
      // Obtain the time part upload events were initiated.
      multipartUpload.getInitiated();
   }
   listMultipartUploadsRequest.setKeyMarker(multipartUploadListing.getNextKeyMarker());
   listMultipartUploadsRequest.setUploadIdMarker(multipartUploadListing.getNextUploadIdMarker(
));
} while (multipartUploadListing.isTruncated());
// Close your OSSClient.
ossClient.shutdown();
```

- List part upload events on one or more pages

  You can use listMultipartUploads to list 1,000 upload events at a time by default. The preceding *list all upload events* operation is a special case where 1,000 events are listed. The following code provides an example of how to specify the number of events on each page, namely, the number of events listed at a time:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey pair, log on to https://ak-console.aliyun.com/#/.
String accessKeyId = "<yourAccessKeyId>";
String accessKeySecret = "<yourAccessKeySecret>";
String bucketName = "<yourBucketName>";
// Create an OSSClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// List part upload events.
MultipartUploadListing multipartUploadListing;
ListMultipartUploadsRequest listMultipartUploadsRequest = new ListMultipartUploadsRequest(buc
ketName);
// Set the maximum number of events that can be displayed on each page.
listMultipartUploadsRequest.setMaxUploads(50);
do {
   multipartUploadListing = ossClient.listMultipartUploads(listMultipartUploadsRequest);
   for (MultipartUpload multipartUpload : multipartUploadListing.getMultipartUploads()) {
      // Obtain the upload ID.
      multipartUpload.getUploadId();
      // Obtain the key of the object.
      multipartUpload.getKey();
      // Obtain the time part upload events were initiated.
      multipartUpload.getInitiated();
   }
   listMultipartUploadsRequest.setKeyMarker(multipartUploadListing.getNextKeyMarker());
   listMultipartUploadsRequest.setUploadIdMarker(multipartUploadListing.getNextUploadIdMarker(
));
} while (multipartUploadListing.isTruncated());
// Close your OSSClient.
ossClient.shutdown();
```

Form upload

Form upload uses an HTML form to upload a file to a specified bucket. The maximum size for each form upload is 5 GB. For the complete form upload code, see GitHub.

Use the following code for form upload:

```
public class PostObjectSample {
    // Upload your file.
    private String localFilePath = "<yourLocalFile>";
    // This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirem
ents.
    private String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
    // It is highly risky to log on with the AccessKey pair of an Alibaba Cloud account because the account
has permissions on all operations in OSS. We recommend that you log on as a RAM user to access the AP
I or perform routine operations and maintenance. To create a RAM user, log on to https://ram.console.al
iyun.com.
    private String accessKeyId = "<yourAccessKeyId>";
    private String accessKeySecret = "<yourAccessKeySecret>";
    // Specify the bucket name.
    private String bucketName = "<yourBucketName>";
    // Specify the object name.
    private String objectName = "<yourObjectName>";
    /**
     * Start form upload.
     * @throws Exception
     */
    private void PostObject() throws Exception {
        // Add the bucket name to the URL. The URL format is http://yourBucketName.oss-cn-hangzhou.aliy
uncs.com.
        String urlStr = endpoint.replace("http://", "http://" + bucketName+ ".") ;
        // Create Map for the form.
        Map<String, String> formFields = new LinkedHashMap<String, String>();
        // Specify the object name.
        formFields.put("key", this.objectName);
        // Configure Content-Disposition.
        formFields.put("Content-Disposition", "attachment;filename="
                + localFilePath);
        // Set callback parameters.
        Callback callback = new Callback();
        // Configure the IP address of the server you want to send the callback request to, such as http://o
ss-demo.aliyuncs.com:23450 or http://127.0.0.1:9090.
        callback.setCallbackUrl("<yourCallbackServerUrl>");
        // Configure the host field value in the callback request header, such as oss-cn-hangzhou.aliyuncs.c
om.
        callback.setCallbackHost("<yourCallbackServerHost>");
        // Configure the body field value for the callback request.
        callback.setCallbackBody("{\\\"mimeType\\\":${mimeType},\\\"size\\\":${size}}");
```

```
        Configure Content-Type for the callback request.
        callback.setCalbackBodyType(CalbackBodyType.JSON);
        // Configure the custom parameters used to send the callback request. Each custom parameter con
sists of a key and a value. The key must start with x:.
        callback.addCallbackVar("x:var1", "value1");
        callback.addCallbackVar("x:var2", "value2");
        // Configure the callback parameter for Map in the form.
        setCallBack(formFields, callback);
        // Configure OSSAccessKeyId.
        formFields.put("OSSAccessKeyId", accessKeyId);
        String policy = "{\"expiration\": \"2120-01-01T12:00:00.000Z\",\"conditions\": [[\"content-length-ran
ge\", 0, 104857600]]}";
        String encodePolicy = new String(Base64.encodeBase64(policy.getBytes()));
        // Configure the policy.
        formFields.put("policy", encodePolicy);
        // Generate a signature.
        String signaturecom = com.aliyun.oss.common.auth.ServiceSignature.create().computeSignature(ac
cessKeySecret, encodePolicy);
        // Configure the signature.
        formFields.put("Signature", signaturecom);
        String ret = formUpload(urlStr, formFields, localFilePath);
        System.out.println("Post Object [" + this.objectName + "] to bucket [" + bucketName + "]");
        System.out.println("post reponse:" + ret);
    }
    private static String formUpload(String urlStr, Map<String, String> formFields, String localFile)
            throws Exception {
        String res = "";
        HttpURLConnection conn = null;
        String boundary = "9431149156168";
        try {
            URL url = new URL(urlStr);
            conn = (HttpURLConnection) url.openConnection();
            conn.setConnectTimeout(5000);
            conn.setReadTimeout(30000);
            conn.setDoOutput(true);
            conn.setDoInput(true);
            conn.setRequestMethod("POST");
            conn.setRequestProperty("User-Agent",
                    "Mozilla/5.0 (Windows; U; Windows NT 6.1; zh-CN; rv:1.9.2.6)");
            // Set the MD5 value. The MD5 value is calculated based on the entire body.
            conn.setRequestProperty("Content-MD5", "<yourContentMD5>");
            conn.setRequestProperty("Content-Type"
```

```
conn.setRequestProperty("Content-Type",
        "multipart/form-data; boundary=" + boundary);
OutputStream out = new DataOutputStream(conn.getOutputStream());
// Recursively read all Map data in the form and write the data to the OutputStream.
if (formFields ! = null) {
    StringBuffer strBuf = new StringBuffer();
    Iterator<Entry<String, String>> iter = formFields.entrySet().iterator();
    int i = 0;
    while (iter.hasNext()) {
        Entry<String, String> entry = iter.next();
        String inputName = entry.getKey();
        String inputValue = entry.getValue();
        if (inputValue == null) {
            continue;
        }
        if (i == 0) {
            strBuf.append("--").append(boundary).append("\r\n");
            strBuf.append("Content-Disposition: form-data; name=\""
                    + inputName + "\"\r\n\r\n");
            strBuf.append(inputValue);
        } else {
            strBuf.append("\r\n").append("--").append(boundary).append("\r\n");
            strBuf.append("Content-Disposition: form-data; name=\""
                    + inputName + "\"\r\n\r\n");
            strBuf.append(inputValue);
        }
        i++;
    }
    out.write(strBuf.toString().getBytes());
}
// Read the file and write it to the OutputStream.
File file = new File(localFile);
String filename = file.getName();
String contentType = new MimetypesFileTypeMap().getContentType(file);
if (contentType == null || contentType.equals("")) {
    contentType = "application/octet-stream";
}
StringBuffer strBuf = new StringBuffer();
strBuf.append("\r\n").append("--").append(boundary)
        .append("\r\n");
strBuf.append("Content-Disposition: form-data; name=\"file\"; "
        + "filename=\"" + filename + "\"\r\n");
```

```
            strBuf.append("Content-Type: " + contentType + "\r\n\r\n");
            out.write(strBuf.toString().getBytes());
            DataInputStream in = new DataInputStream(new FileInputStream(file));
            int bytes = 0;
            byte[] bufferOut = new byte[1024];
            while ((bytes = in.read(bufferOut)) ! = -1) {
                out.write(bufferOut, 0, bytes);
            }
            in.close();
            byte[] endData = ("\r\n--" + boundary + "--\r\n").getBytes();
            out.write(endData);
            out.flush();
            out.close();
            // Read the returned data.
            strBuf = new StringBuffer();
            BufferedReader reader = new BufferedReader(new InputStreamReader(conn.getInputStream()));
            String line = null;
            while ((line = reader.readLine()) ! = null) {
                strBuf.append(line).append("\n");
            }
            res = strBuf.toString();
            reader.close();
            reader = null;
        } catch (Exception e) {
            System.err.println("Send post request exception: " + e);
            throw e;
        } finally {
            if (conn ! = null) {
                conn.disconnect();
                conn = null;
            }
        }
        return res;
    }
     private static void setCallBack(Map<String, String> formFields, Callback callback) {
        if (callback ! = null) {
            String jsonCb = OSSUtils.jsonizeCallback(callback);
            String base64Cb = BinaryUtil.toBase64String(jsonCb.getBytes());
            formFields.put("callback", base64Cb);
            if (callback.hasCallbackVar()) {
                Map<String, String> varMap = callback.getCallbackVar();
```

```
            for (Entry<String, String> entry : varMap.entrySet()) {
                formFields.put(entry.getKey(), entry.getValue());
            }
        }
    }
  }
  public static void main(String[] args) throws Exception {
    PostObjectSample ossPostObject = new PostObjectSample();
    ossPostObject.PostObject();
  }
}
```

View upload or download progress information

You can use progress bars to indicate the upload or download progress. The following code uses `OSSClient.putObject` as an example to describe how to view progress information.

```
static class PutObjectProgressListener implements ProgressListener {
  private long bytesWritten = 0;
  private long totalBytes = -1;
  private boolean succeed = false;
  @Override
  public void progressChanged(ProgressEvent progressEvent) {
    long bytes = progressEvent.getBytes();
    ProgressEventType eventType = progressEvent.getEventType();
    switch (eventType) {
    case TRANSFER_STARTED_EVENT:
      System.out.println("Start to upload.....");
      break;
    case REQUEST_CONTENT_LENGTH_EVENT:
      this.totalBytes = bytes;
      System.out.println(this.totalBytes + " bytes in total will be uploaded to OSS");
      break;
    case REQUEST_BYTE_TRANSFER_EVENT:
      this.bytesWritten += bytes;
      if (this.totalBytes ! = -1) {
        int percent = (int)(this.bytesWritten * 100.0 / this.totalBytes);
        System.out.println(bytes + " bytes have been written at this time, upload progress: " + percent
+ "%(" + this.bytesWritten + "/" + this.totalBytes + ")");
      } else {
        System.out.println(bytes + " bytes have been written at this time, upload ratio: unknown" + "("
+ this.bytesWritten + "/...)");
      }
```

```
            break;
        case TRANSFER_COMPLETED_EVENT:
            this.succeed = true;
            System.out.println("Succeed to upload, " + this.bytesWritten + " bytes have been transferred in to
tal");
            break;
        case TRANSFER_FAILED_EVENT:
            System.out.println("Failed to upload, " + this.bytesWritten + " bytes have been transferred");
            break;
        default:
            break;
        }
    }
    public boolean isSucceed() {
        return succeed;
    }
}
public static void main(String[] args) {
    String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
    String accessKeyId = "<accessKeyId>";
    String accessKeySecret = "<accessKeySecret>";
    String bucketName = "<bucketName>";
    String key = "object-get-progress-sample";
    OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
    try {
        // View the upload progress while you upload a file.
        ossClient.putObject(new PutObjectRequest(bucketName, key, new FileInputStream("<yourLocalFile>
")).
                <PutObjectRequest>withProgressListener(new PutObjectProgressListener()));
    } catch (Exception e) {
        e.printStackTrace();
    }
    ossClient.shutdown();
}
```

For the complete upload progress bar code, see GitHub.

Note

- You can view progress information with putObject, getObject, or uploadPart.
- However, you cannot view progress information with ossClient.uploadFile or ossClient.downloadFile.

2.4.2.1.7. Download objects

Download methods

The OSS Java SDK provides a variety of object download APIs. You can download an object from OSS through any of the following methods:

- Streaming download
- Download an object to a local file
- Resumable download
- Range download

Streaming download

When downloading a large object, users often prefer processing the data in the streaming mode (that is, processing one part at a time), but not processing all data at once.

Note For the complete streaming download code, see GitHub.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
String bucketName = "<Your bucket name>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
OSSObject ossObject = ossClient.getObject(bucketName, "yourKey");
// Read the object content.
System.out.println("Object content:");
BufferedReader reader = new BufferedReader(new InputStreamReader(ossObject.getObjectContent()))
;
while (true) {
    String line = reader.readLine();
    if (line == null) break;
    System.out.println("\n" + line);
}
reader.close();
// Close your client.
ossClient.shutdown();
```

Note

- The OSSObject instance contains the bucket of the object, object name, Object Meta, and an input stream.
- The input stream can be used to read and save the object content to another object or to the buffer. Object Meta contains the ETag, HTTP header, and User Meta.
- The stream obtained through the OSSClient.getObject API must be closed. Otherwise, resource leaks may occur.

```
OSSObject ossObject = ossClient.getObject(bucketName, key);
ossObject.getObjectContent().close();
```

- If you need to read 64 KB of data from OSS in the streaming mode, you can use the following method to read the data multiple times until 64 KB or the entire object is read:

```
byte[] buf = new byte[1024];
InputStream in = ossObject.getObjectContent();
for (int n = 0; n ! = -1; ) {
  n = in.read(buf, 0, buf.length);
}
in.close();
```

Do not use the following method:

```
byte[] buf = new byte[64 * 1024];
InputStream in = ossObject.getObjectContent();
in.read(buf, 0, buf.length);
in.close();
```

We recommend that you do not use this method because you may not be able to read all data at a time in the streaming mode. For more information, see InputStream.read.

Download an object to a local file

The following code provides an example of how to download the contents of the object to a specified local file. If the specified local file does not exist, a new one is created.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
String bucketName = "<Your bucket name>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Download the object to a local file.
ossClient.getObject(new GetObjectRequest(bucketName, "<yourKey>"), new File("<yourLocalFile>"));
// Close your client.
ossClient.shutdown();
```

Range download

If you need to download only a part of data from a large OSS object, you can use range download to download the data within a specified range. If the specified download range is 0-100, the data from byte 0 to byte 100 (included) is returned, that is, 101 bytes of data in total. If the specified range is invalid, the entire object is downloaded.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
String bucketName = "<Your bucket name>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
GetObjectRequest getObjectRequest = new GetObjectRequest(bucketName, "<yourKey>");
// Obtain data sized from 0 to 1,000 Bytes (including 0 and 1,000, a total of 1,001 Bytes).
getObjectRequest.setRange(0, 1000);
// Start range download.
OSSObject ossObject = ossClient.getObject(getObjectRequest);
// Read data.
byte[] buf = new byte[1024];
InputStream in = ossObject.getObjectContent();
for (int n = 0; n ! = -1; ) {
    n = in.read(buf, 0, buf.length);
}
// After the InputStream data is read, close the stream. Otherwise, connection leaks may occur.
in.close();
// Close your client.
ossClient.shutdown();
```

Note

- If the specified range is invalid (for example, the starting position or the ending position is a negative value or the range is greater than the object size), the entire object is downloaded.
- If you need to read 64 KB of data from OSS in the streaming mode, you can use the following method to read the data multiple times until 64 KB or the entire object is read:

```
byte[] buf = new byte[1024];
InputStream in = ossObject.getObjectContent();
for (int n = 0; n ! = -1; ) {
  n = in.read(buf, 0, buf.length);
}
in.close();
```

Do not use the following method:

```
byte[] buf = new byte[64 * 1024];
InputStream in = ossObject.getObjectContent();
in.read(buf, 0, buf.length);
in.close();
```

We recommend that you do not use this method because you may not be able to read all data at a time in the streaming mode. For more information, see InputStream.read.

Resumable download

You may fail to download a large object if the network is unstable or the program crashes. In this case, you have to download the object again, which is a waste of resources. If the network is unstable, you may need to retry multiple times. You can use `OSSClient.downloadFile` to achieve resumable download. The request parameter is DownloadFileRequest. This request contains the following parameters:

- bucket: the name of the bucket. It is a required parameter that is set through the constructor.
- key: the name of the object you want to download to OSS. It is a required parameter that is set through the constructor.
- downloadFile: a local file you want to download the object content to. It is an optional parameter that is set through the constructor or setDownloadFile. The default value is key.
- partSize: the part size from 1 Byte to 5 GB. Unit: bytes. It is an optional parameter that is set through setPartSize. The default value is 100 KB.
- taskNum: the number of parts for concurrent downloads. It is an optional parameter that is set through setTaskNum. The default value is 1.
- enableCheckpoint: indicates whether to enable resumable download. It is an optional parameter that is set through setEnableCheckpoint. The resumable download feature is disabled by default.
- checkpointFile: the file that stores the checkpoint information. When resumable download is enabled, you need to record the part download result in this local file. If the download fails, the

downloaded parts are not downloaded again. It is an optional parameter that can be set through setCheckpointFile. By default, this file is stored in the same directory as the file specified by downloadFile, that is, *downloadFile.ucp*.

The principle is to split the object you want to download into multiple parts and download them sequentially. When all parts are downloaded, the download of the entire object is completed. During the download, the download progress (recorded in the checkpoint object) and the downloaded parts are recorded. If a part fails to be downloaded, the next download continues from the point recorded in the checkpoint object. This requires that the same checkpoint object for the previous download be used. The checkpoint object is deleted after the resumable download is completed.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
String bucketName = "<Your bucket name>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Send a request to start 10 tasks simultaneously and start resumable download.
DownloadFileRequest downloadFileRequest = new DownloadFileRequest("bucketName", "key");
downloadFileRequest.setDownloadFile("downloadFile");
downloadFileRequest.setTaskNum(10);
downloadFileRequest.setEnableCheckpoint(true);
// Download the object to a local file.
DownloadFileResult downloadRes = ossClient.downloadFile(downloadFileRequest);
// When the download succeeds, Object Meta is returned.
downloadRes.getObjectMetadata();
// Close your client.
ossClient.shutdown();
```

Conditional download

You can specify one or more conditions for downloading an object. The object can be downloaded only when all specified conditions are met. Otherwise, an error is returned and the object cannot be downloaded. The following table describes the available download conditions.

Name	Description
If-Modified-Since	The object download condition. If the specified time is earlier than the actual object modification time, the object can be downloaded. Otherwise, an error is returned.

Name	Description
If-Unmodified-Since	The object download condition. If the specified time is equal to or later than the actual object modification time, the object can be downloaded. Otherwise, an error is returned.
If-Match	The object download condition. If the ETag value of the source object is equal to the ETag value specified in the request, the object can be downloaded. Otherwise, an error is returned.
If-None-Match	The object download condition. If the ETag value of the source object is not equal to the ETag value specified in the request, the object can be downloaded. Otherwise, an error is returned.

Note

- If the time specified by If-Modified-Since does not conform to the specification, the object and the 200 OK message are returned.
- You can use If-Modified-Since and If-Unmodified-Since as object download conditions at the same time. You can use If-Match and If-None-Match as object download conditions at the same time.
- If a request does not meet the condition specified in If-Unmodified-Since or If-Match, the 412 Precondition Failed error is returned.
- If a request does not meet the condition specified in If-Modified-Since or If-None-Match, the 304 Not Modified error is returned.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
String bucketName = "<Your bucket name>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
GetObjectRequest request = new GetObjectRequest(bucketName, "<yourKey>");
request.setModifiedSinceConstraint(new Date());
// Download the object to a local file.
ossClient.getObject(request, new File("<yourLocalFile>"));
// Close your client.
ossClient.shutdown();
```

Note

- You can use OSSClient.getObjectMetadata to obtain the ETag value;
- You can specify conditions for OSSClient.getObject and OSSClient.downloadFile.

Download Progress Bar

The OSS Java SDK supports the progress bar feature to display the upload and download progress. The following code takes 'OSSClient.getObject' as an example to describe how to use the progress bar feature.

Note For the complete progress bar code, see GitHub.

```
static class GetObjectProgressListener implements ProgressListener {
    private long bytesRead = 0;
    private long totalBytes = -1;
    private boolean succeed = false;
    @Override
    public void progressChanged(ProgressEvent progressEvent) {
      long bytes = progressEvent.getBytes();
      ProgressEventType eventType = progressEvent.getEventType();
      switch (eventType) {
      case TRANSFER_STARTED_EVENT:
        System.out.println("Start to download......");
        break;
      case RESPONSE_CONTENT_LENGTH_EVENT:
        this.totalBytes = bytes;
        System.out.println(this.totalBytes + " bytes in total will be downloaded to a local file");
        break;
      case RESPONSE_BYTE_TRANSFER_EVENT:
        this.bytesRead += bytes;
        if (this.totalBytes ! = -1) {
          int percent = (int)(this.bytesRead * 100.0 / this.totalBytes);
          System.out.println(bytes + " bytes have been read at this time, download progress:
              percent + "%(" + this.bytesRead + "/" + this.totalBytes + ")");
        } else {
          System.out.println(bytes + " bytes have been read at this time, download ratio: unknown" +
              "(" + this.bytesRead + "/...)");
        }
        break;
      case TRANSFER_COMPLETED_EVENT:
        this.succeed = true;
        System.out.println("Succeed to download, " + this.bytesRead + " bytes have been transferred in
```

```
total");
            break;
        case TRANSFER_FAILED_EVENT:
            System.out.println("Failed to download, " + this.bytesRead + " bytes have been transferred");
            break;
        default:
            break;
        }
    }
    public boolean isSucceed() {
        return succeed;
    }
  }
public static void main(String[] args) {
    String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
    String accessKeyId = "<accessKeyId>";
    String accessKeySecret = "<accessKeySecret>";
    String bucketName = "<bucketName>";
    String key = "object-get-progress-sample";
    OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
    try {
        // Download the object with the progress bar displayed.
        client.getObject(new GetObjectRequest(bucketName, key).
            <GetObjectRequest>withProgressListener(new GetObjectProgressListener()),
            new File("<yourLocalFile>"));
    } catch (Exception e) {
        e.printStackTrace();
    }
    ossClient.shutdown();
}
```

Note

- The PutObject, GetObject, and UploadPart APIs support the progress bar feature.
- The UploadFile and DownloadFile APIs do not support the progress bar feature.

2.4.2.1.8. Manage objects

In OSS, you can manage the objects in a bucket by using a series of APIs, such as SetObjectAcl, GetObjectAcl, ListObjects, DeleteObject, CopyObject, and DoesObjectExist. Object names are also called keys or object keys.

Check whether an object exists

The following code provides an example of how to use `OSSClient.doesObjectExist` to determine whether an object exists:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Check whether an object exists.
boolean found = ossClient.doesObjectExist("<bucketName>", "<key>")
// Close your client.
ossClient.shutdown();
```

Object ACL

The following table describes the permissions included in the ACL of an object.

ACL	Description
Default	The object inherits the ACL of the bucket. This is the default object ACL.
private	The object is a private resource. Only the owner or authorized user has the read and write permissions on the object. A signature is required for anonymous access requests.
public-read	Only the owner or authorized user of an object has the read and write permissions on the object. Other users (including anonymous users) have only read permissions on the object.
public-read-write	The object is a read/write resource for the public. All users of an object have the read and write permissions on the object.

The ACL privileges of objects take precedence over those of buckets. For example, OSS allows users to access a public-read-write object in a bucket even though the bucket is private. If no ACL has been set for an object, its bucket ACL applies.

Set the ACL for an object

You can use `OSSClient.setObjectAcl` to set the Object ACL.

ACL	Java SDK value
private	CannedAccessControlList.Private
public-read	CannedAccessControlList.PublicRead

ACL	Java SDK value
public-read-write	CannedAccessControlList.PublicReadWrite

The following code provides an example of how to set the ACL for an object:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Set the ACL for an object.
ossClient.setObjectAcl("<bucketName>", "<key>", CannedAccessControlList.PublicRead)
// Close your client.
ossClient.shutdown();
```

Obtain an object ACL

The following code provides an example of how to use `OSSClient.getObjectAcl` to obtain the object ACL:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Obtain the ACL of an object.
ObjectAcl objectAcl = ossClient.getObjectAcl("<bucketName>", "<key>");
System.out.println(objectAcl.getPermission().toString());
// Close your client.
ossClient.shutdown();
```

Obtain Object Meta

Object Meta describes the attributes of objects uploaded to OSS. These attributes are classified into two types: HTTP standard attributes (HTTP headers) and User Meta (user-defined Object Meta). You can set Object Meta when you upload or copy objects in various ways.

You can use `OSSClient.getSimplifiedObjectMeta` or `OSSClient.getObjectMetadata` to obtain Object Meta. You can obtain only object ETag, Size (object size), and LastModified (last modify time) if you use `getSimplifiedObjectMeta`. However, you can obtain all Object Meta if you use `getObjectMetadata`. getSimplified. ObjectMeta is more lightweight and faster.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requiremen
ts.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Obtain some Object Meta.
SimplifiedObjectMeta objectMeta = ossClient.getSimplifiedObjectMeta("<bucketName>", "<key>");
System.out.println(objectMeta.getSize());
System.out.println(objectMeta.getETag());
System.out.println(objectMeta.getLastModified());
// Obtain all Object Meta.
ObjectMetadata metadata = ossClient.getObjectMetadata("<bucketName>", "<key>");
System.out.println(metadata.getContentType());
System.out.println(metadata.getLastModified());
System.out.println(metadata.getExpirationTime());
// Close your client.
ossClient.shutdown();
```

List objects in a bucket

For the complete listObjects code, see GitHub.

You can use `OSSClient.listObjects` to list all objects in a bucket. listObjects supports three types of parameter formats:

- ObjectListing listObjects(String bucketName)
- ObjectListing listObjects(String bucketName, String prefix)
- ObjectListing listObjects(ListObjectsRequest listObjectsRequest)

The first two types are called simple list. You can use them to return a maximum of 100 objects. The parameter prefix specifies the prefix of the returned object. The last type provides multiple filtering features to implement flexible queries.

The following table describes parameters for ObjectListing.

Parameter	Description	Method
ObjectSummaries	The Object Meta to be returned.	List<OSSObjectSummary> getObjectSummaries()

Parameter	Description	Method
Prefix	The prefix contained in the names of returned objects.	String getPrefix()
Delimiter	The delimiter used to group objects by name.	String getDelimiter()
Marker	The starting position of the object list in the response to this request.	String getMarker()
MaxKeys	The maximum number of objects returned for this request.	int getMaxKeys()
NextMarker	The starting position of the object list in the response to the next request.	String getNextMarker()
IsTruncated	Specifies whether all results are returned.	boolean isTruncated()
CommonPrefixes	If the Delimiter parameter is specified in the request, the response contains the CommonPrefixes element. This element specifies a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter.	List<String> getCommonPrefixes()
EncodingType	The encoding type of the key in the response.	String getEncodingType()

- Simple list

  You can use the following code to list the objects in a bucket. You can list a maximum of 100 objects.

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// List objects.
ObjectListing objectListing = ossClient.listObjects("<bucketName>", "<KeyPrifex>");
List<OSSObjectSummary> sums = objectListing.getObjectSummaries();
for (OSSObjectSummary s : sums) {
   System.out.println("\t" + s.getKey());
}
// Close your client.
ossClient.shutdown();
```

You can use the following code to list the objects with the specified prefix in a bucket. You can list a maximum of 100 objects.

```
ObjectListing objectListing = ossClient.listObjects("<bucketName>", "<KeyPrifex>");
List<OSSObjectSummary> sums = objectListing.getObjectSummaries();
for (OSSObjectSummary s : sums) {
    System.out.println("\t" + s.getKey());
}
```

- List objects by specifying ListObjectsRequest

  You can set parameters of ListObjectsReques to achieve various flexible queries. The following table describes the parameters you can set for ListObjectsRequest.

Parameter	Description	Method
Prefix	The prefix that must be contained in the names (key) of the returned objects.	setPrefix(String prefix)
Delimiter	The delimiter used to group objects by name. CommonPrefixes specify a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter.	setDelimiter(String delimiter)
Marker	The starting position of the object list. Objects are sorted in the alphabetical order and those objects following this marker are listed.	setMarker(String marker)
MaxKeys	The maximum number of objects returned for one request. If this parameter is not specified, the default value 100 is used. The maximum number cannot exceed 1,000.	setMaxKeys(Integer maxKeys)
Encoding Type	The encoding type for object names in the response body. Currently, URL encoding is supported.	setEncodingType(String encodingType)

- Set the maximum number of returned objects

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requir
ements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
final int maxKeys = 200;
// List objects.
ObjectListing objectListing = ossClient.listObjects(new ListObjectsRequest("<bucketName>").withM
axKeys(maxKeys));
List<OSSObjectSummary> sums = objectListing.getObjectSummaries();
for (OSSObjectSummary s : sums) {
   System.out.println("\t" + s.getKey());
}
// Close your client.
ossClient.shutdown();
```

- List objects with a specified prefix

  You can list a maximum of 100 objects.

```
final String keyPrefix = "<keyPrefix>"
ObjectListing objectListing = ossClient.listObjects(new ListObjectsRequest("<bucketName>").withPr
efix(keyPrefix));
List<OSSObjectSummary> sums = objectListing.getObjectSummaries();
for (OSSObjectSummary s : sums) {
   System.out.println("\t" + s.getKey());
}
```

- List objects after a specified object

  You can list a maximum of 100 objects (excluding the specified object).

```
final String keyMarker = "<keyMarker>"
ObjectListing objectListing = ossClient.listObjects(new ListObjectsRequest("<bucketName>").withM
arker(keyMarker));
List<OSSObjectSummary> sums = objectListing.getObjectSummaries();
for (OSSObjectSummary s : sums) {
   System.out.println("\t" + s.getKey());
}
```

- List all objects by page

  You can list a maximum of maxKeys objects on each page.

```
final int maxKeys = 200;
String nextMarker = null;
do {
    objectListing = ossClient.listObjects(new ListObjectsRequest("<bucketName>").withMarker(next
Marker).withMaxKeys(maxKeys));
    List<OSSObjectSummary> sums = objectListing.getObjectSummaries();
    for (OSSObjectSummary s : sums) {
        System.out.println("\t" + s.getKey());
    }
    nextMarker = objectListing.getNextMarker();
} while (objectListing.isTruncated());
```

- List all the objects after a specified object by page

  You can set maxKeys to specify the maximum objects (after a specified object) that can be listed on each page.

```
final int maxKeys = 200;
String nextMarker = "<nextMarker>";
do {
    objectListing = ossClient.listObjects(new ListObjectsRequest("<bucketName>").withMarker(next
Marker).withMaxKeys(maxKeys));
    List<OSSObjectSummary> sums = objectListing.getObjectSummaries();
    for (OSSObjectSummary s : sums) {
        System.out.println("\t" + s.getKey());
    }
    nextMarker = objectListing.getNextMarker();
} while (objectListing.isTruncated());
```

- List all the objects with a specified prefix by page

  The following code provides an example of how to set maxKeys and a prefix to list the maximum number of desired objects that can be listed on each page:

```
final int maxKeys = 200;
final String keyPrefix = "<keyPrefix>";
String nextMarker = "<nextMarker>";
do {
    objectListing = ossClient.listObjects(new ListObjectsRequest("<bucketName>").
            withPrefix(keyPrefix).withMarker(nextMarker).withMaxKeys(maxKeys));
    List<OSSObjectSummary> sums = objectListing.getObjectSummaries();
    for (OSSObjectSummary s : sums) {
        System.out.println("\t" + s.getKey());
    }
    nextMarker = objectListing.getNextMarker();
} while (objectListing.isTruncated());
```

- Specify the encoding type for object names in the response

  If the object name contains special characters such as single quotation marks ('), double quotation marks ("), ampersands (&), and angle brackets (< >), and Chinese characters, encode the characters before transmission. Currently, OSS supports the url -based encoding.

```
final int maxKeys = 200;
final String keyPrefix = "<keyPrefix>";
String nextMarker = "<nextMarker>";
ObjectListing objectListing;
do {
    ListObjectsRequest listObjectsRequest = new ListObjectsRequest(bucketName);
    listObjectsRequest.setPrefix(keyPrefix);
    listObjectsRequest.setMaxKeys(maxKeys);
    listObjectsRequest.setMarker(nextMarker);
    // Specify the encoding type.
    listObjectsRequest.setEncodingType("url");
    objectListing = ossClient.listObjects(listObjectsRequest);
    // Object decoding.
    for (OSSObjectSummary objectSummary: objectListing.getObjectSummaries()) {
        System.out.println("Key:" + URLDecoder.decode(objectSummary.getKey(), "UTF-8"));
    }
    // CommonPrefixe decoding.
    for (String commonPrefixes: objectListing.getCommonPrefixes()) {
        System.out.println("CommonPrefixes:" + URLDecoder.decode(commonPrefixes, "UTF-8"));
    }
    // NextMarker decoding.
    if (objectListing.getNextMarker() ! = null) {
        nextMarker = URLDecoder.decode(objectListing.getNextMarker(), "UTF-8");
    }
} while (objectListing.isTruncated());
```

- Simulate a folder

  OSS does not use the folder concept. OSS stores all elements as objects. Creating a folder means creating an empty object. This object can be uploaded and downloaded. The console displays any object ending with a forward slash (/) as a folder.

  Users can use a combination of Delimiters and Prefixes to simulate folder functions as follows: The combination of Delimiter and Prefix is as follows:

  - If Prefix is set to a folder name in the request, the object names starting with this prefix are listed, including all recursive objects and subfolders in this folder. The names are listed in the Contents element.
  - If Prefix is set to a folder name and Delimiter is set to a forward slash (/) in the request, the names of the objects and subfolders in the folder are listed in the CommonPrefixes element. Recursive objects and recursive subfolders are not listed.

  > **Note**
  >
  > - For the complete code of creating objects, see GitHub.

Assume that a bucket contains four objects oss.jpg, fun/test.jpg, fun/movie/001.avi, and fun/movie/007.avi, and the forward slash (/) is used as the folder delimiter. The following examples show how to simulate a folder.

- List all objects in the bucket

  The following code provides an example of how to list all objects in the bucket:

```
// Create ListObjectsRequest.
ListObjectsRequest listObjectsRequest = new ListObjectsRequest(bucketName);
// List objects.
ObjectListing listing = ossClient.listObjects(listObjectsRequest);
// Traverse all objects.
System.out.println("Objects:");
for (OSSObjectSummary objectSummary : listing.getObjectSummaries()) {
   System.out.println(objectSummary.getKey());
}
// Traverse all CommonPrefixs elements.
System.out.println("CommonPrefixs:");
for (String commonPrefix : listing.getCommonPrefixes()) {
   System.out.println(commonPrefix);
}
```

  Output:

```
Objects:
fun/movie/001.avi
fun/movie/007.avi
fun/test.jpg
oss.jpg
CommonPrefixs:
```

- List all recursive objects in a folder

  Set Prefix to list all recursive objects in a folder (fun/):

```
// Create ListObjectsRequest.
ListObjectsRequest listObjectsRequest = new ListObjectsRequest(bucketName);
listObjectsRequest.setPrefix("fun/");
// List all recursive objects in the fun folder.
ObjectListing listing = ossClient.listObjects(listObjectsRequest);
// Traverse all objects.
System.out.println("Objects:");
for (OSSObjectSummary objectSummary : listing.getObjectSummaries()) {
   System.out.println(objectSummary.getKey());
}
// Traverse all CommonPrefixs elements.
System.out.println("\nCommonPrefixs:");
for (String commonPrefix : listing.getCommonPrefixes()) {
   System.out.println(commonPrefix);
}
```

  Output:

```
Objects:
fun/movie/001.avi
fun/movie/007.avi
fun/test.jpg
CommonPrefixs:
```

- List objects and subfolders in a folder

  Set Prefix and Delimiter to list the objects and subfolders in a folder (fun/):

```
// Create ListObjectsRequest.
ListObjectsRequest listObjectsRequest = new ListObjectsRequest(bucketName);
// Use the forward slash (/) as the folder delimiter.
listObjectsRequest.setDelimiter("/");
// List the objects and subfolders in the fun folder.
listObjectsRequest.setPrefix("fun/");
ObjectListing listing = ossClient.listObjects(listObjectsRequest);
// Traverse all objects.
System.out.println("Objects:");
for (OSSObjectSummary objectSummary : listing.getObjectSummaries()) {
   System.out.println(objectSummary.getKey());
}
// Traverse all CommonPrefixs elements.
System.out.println("\nCommonPrefixs:");
for (String commonPrefix : listing.getCommonPrefixes()) {
   System.out.println(commonPrefix);
}
```

Output:

```
Objects:
fun/test.jpg
CommonPrefixs:
fun/movie/
```

> **Note**
>
> - In the response, the ObjectSummaries element lists the objects in the fun folder.
> - The CommonPrefixs element lists the subfolders in the fun folder. The fun/movie/001.avi and fun/movie/007.avi objects are not listed because they are in the movie subfolder in the fun folder.

Delete objects

- Delete an object

  The following code provides an example of how to use `OSSClient.deleteObject` to delete an object:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirem
ents.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Delete an object.
ossClient.deleteObject("<bucketName>", "<key>");
// Close your client.
ossClient.shutdown();
```

- Delete multiple objects

  The following code provides an example of how to use `OSSClient.deleteObjects` to delete multiple objects simultaneously:

  ```
  public DeleteObjectsResult deleteObjects(DeleteObjectsRequest deleteObjectsRequest)
  ```

  You can delete a maximum of 1,000 objects for one request. Two return modes are supported: Verbose and Quiet.

  - Verbose mode: return the results of successfully deleted objects, that is, DeleteObjectsResult.getDeletedObjects. Default mode.
  - Quiet mode: return the results of objects with errors during deletion, that is DeleteObjectsResult.getDeletedObjects.

  The following table describes the parameters in DeleteObjectsRequest.

Parameter	Description	Method
Keys	The objects you wan to delete.	setKeys(List<String>)
Quiet	The return mode. Valid values include true (Quiet) and false (Verbose). The Verbose mode is used by default.	setQuiet(boolean)
EncodingType	The encoding type of the key in the response. Currently, URL encoding is supported.	setEncodingType(String)

  The following table describes the parameters for DeleteObjectsResult.

Parameter	Description	Method
deletedObjects	The deletion result. In Verbose mode, successfully deleted objects are listed. In Quiet mode, objects that failed to be deleted are listed.	List<String> getDeletedObjects()

Parameter	Description	Method
EncodingType	The encoding type of the key in the response. If this parameter is left unspecified, Key is not encoded.	getEncodingType()

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Delete objects.
List<String> keys = new ArrayList<String>();
keys.add("key0");
keys.add("key1");
keys.add("key2");
DeleteObjectsResult deleteObjectsResult = ossClient.deleteObjects(new DeleteObjectsRequest("<bucketName>").withKeys(keys));
List<String> deletedObjects = deleteObjectsResult.getDeletedObjects();
// Close your client.
ossClient.shutdown();
```

Note For the complete code of simultaneous object deletion, see GitHub.

Copy objects

You can copy an object from one bucket to another in the same region (such as China (Hangzhou), China (Shenzhen), and China (Qingdao)) You can use `OSSClient.copyObject` .

- CopyObjectResult copyObject(String sourceBucketName, String sourceKey, String destinationBucketName, String destinationKey)
- CopyObjectResult copyObject(CopyObjectRequest copyObjectRequest)

The first method specifies the source bucket/key and the target bucket/key. The content and Object Meta of the target object is the same as those of the source object. This is called the simple copy. The second method allows you to specify the reason data of the target object and the constraints of the COPY operation. In the COPY operation, if the source object URL and target object URL are the same, the meta information of the source object is replaced directly.

The following table lists configurable parameters of CopyObjectRequest.

Parameter	Description	Method

Parameter	Description	Method
sourceBucketName	The name of the bucket of the source object.	setSourceBucketName(String sourceBucketName)
sourceKey	The key of the source object.	setSourceKey(String sourceKey)
destinationBucketName	The name of the bucket of the target object.	setDestinationBucketName(String destinationBucketName)
destinationKey	The key of the target object.	setDestinationKey(String destinationKey)
newObjectMetadata	The Object Meta of the target object.	setNewObjectMetadata(ObjectMetadata newObjectMetadata)
matchingETagConstraints	The object copy condition. If the ETag value of the source object is equal to the ETag value specified in the request, OSS copies the object. Otherwise, OSS returns an error.	setMatchingETagConstraints(List<String> matchingETagConstraints)
nonmatchingEtagConstraints	The object copy condition. If the ETag value of the source object is not equal to the ETag value specified in the request, OSS copies the object; otherwise, OSS returns an error.	setNonmatchingETagConstraints(List<String> nonmatchingEtagConstraints)
unmodifiedSinceConstraint	The object copy condition. If the specified time is equal to or later than the actual object modification time, OSS copies the object; otherwise, OSS returns an error.	setUnmodifiedSinceConstraint(Date unmodifiedSinceConstraint)
modifiedSinceConstraint	The object copy condition. If the source object has been modified since the time specified in the request, OSS copies the object; otherwise, OSS returns an error.	setModifiedSinceConstraint(Date modifiedSinceConstraint)

The following table describes the parameters you can configure for CopyObjectRequest.

Parameter	Description	Method
etag	The unique tag of an object.	String getETag()
lastModified	The last modification time of an object.	Date getLastModified()

Note

- You must have permissions to operate on the source object. Otherwise the operation may fail.
- This operation cannot copy data across regions. For example, an object in a Hangzhou bucket may not be copied to a Qingdao bucket.
- This operation supports a maximum object size of 1 GB.

- Simple copy

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Copy an object.
CopyObjectResult result = ossClient.copyObject("<srcBucketName>", "<srcKey>", "<destBucketName>", "<destKey>");
System.out.println("ETag: " + result.getETag() + " LastModified: " + result.getLastModified());
// Close your client.
ossClient.shutdown();
```

- CopyObjectRequest-based copy

  You can also copy an object by specifying CopyObjectRequest:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirem
ents.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// To view the AccessKey, log on to https://ak-console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Create CopyObjectRequest.
CopyObjectRequest copyObjectRequest = new CopyObjectRequest(srcBucketName, srcKey, destBucke
tName, destKey);
// Set new Object Meta.
ObjectMetadata meta = new ObjectMetadata();
meta.setContentType("text/plain");
copyObjectRequest.setNewObjectMetadata(meta);
// Copy the object.
CopyObjectResult result = ossClient.copyObject(copyObjectRequest);
System.out.println("ETag: " + result.getETag() + " LastModified: " + result.getLastModified());
// Close your client.
ossClient.shutdown();
```

Copy a large object

CopyObject is used to copy objects smaller than 1 GB. To copy an object larger than 1 GB, use UploadPartCopy. UploadPartCopy involves three steps:

- `OSSClient.initiateMultipartUpload` : Initialize the multipart copy task.
- `OSSClient.uploadPartCopy` : Start the multipart copy. All the parts except for the last one must be greater than 100 KB in size.
- `OSSClient.completeMultipartUpload` : Complete the multipart copy task.

> **Note** For the complete multipart copy code, see GitHub.

```
String sourceBucketName = "<sourceBucketName>";
String sourceKey = "<sourceKey>";
String targetBucketName = "<targetBucketName>";
String targetKey = "<targetKey>";
// Obtain the size of the copied object.
ObjectMetadata objectMetadata = ossClient.getObjectMetadata(sourceBucketName, sourceKey);
long contentLength = objectMetadata.getContentLength();
// Part size: 10 MB
long partSize = 1024 * 1024 * 10;
// Calculate the number of parts.
```

```
int partCount = (int) (contentLength / partSize);
if (contentLength % partSize ! = 0) {
   partCount++;
}
System.out.println("total part count:" + partCount);
// Initialize an UploadPartCopy task.
InitiateMultipartUploadRequest initiateMultipartUploadRequest = new InitiateMultipartUploadRequest(t
argetBucketName, targetKey);
InitiateMultipartUploadResult initiateMultipartUploadResult = ossClient.initiateMultipartUpload(initiate
MultipartUploadRequest);
String uploadId = initiateMultipartUploadResult.getUploadId();
// Start the UploadPartCopy task.
List<PartETag> partETags = new ArrayList<PartETag>();
for (int i = 0; i < partCount; i++) {
    // Calculate the size of each part.
   long skipBytes = partSize * i;
   long size = partSize < contentLength - skipBytes ? partSize : contentLength - skipBytes;
   // Create UploadPartCopyRequest.
   UploadPartCopyRequest uploadPartCopyRequest =
      new UploadPartCopyRequest(sourceBucketName, sourceKey, targetBucketName, targetKey);
   uploadPartCopyRequest.setUploadId(uploadId);
   uploadPartCopyRequest.setPartSize(size);
   uploadPartCopyRequest.setBeginIndex(skipBytes);
   uploadPartCopyRequest.setPartNumber(i + 1);
   UploadPartResult uploadPartResult = ossClient.uploadPart(uploadPartRequest);
   // Save the returned PartETags to List.
   partETags.add(uploadPartCopyResult.getPartETag());
}
// Submit the UploadPartCopy task.
CompleteMultipartUploadRequest completeMultipartUploadRequest = new CompleteMultipartUploadReq
uest(
            targetBucketName, targetKey, uploadId, partETags);
ossClient.completeMultipartUpload(completeMultipartUploadRequest);
```

Note

- During the Upload Part Copy operation, you can specify the target Object Meta through InitiateMultipartUploadRequest.
- The Upload Part Copy operation also supports constraints which can be specified through UploadPartCopyRequest.

2.4.2.1.9. Authorized access

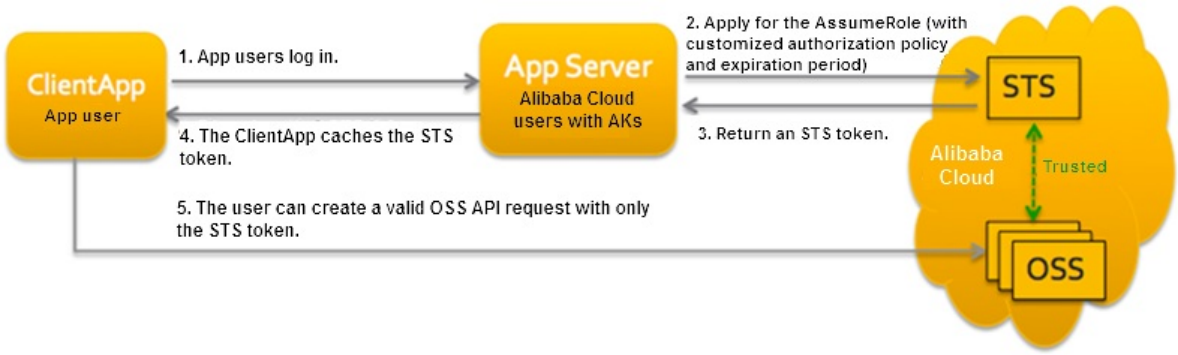
Use STS for temporary access authorization

- Overview

  OSS allows you to use Alibaba Cloud STS for temporary access authorization. Alibaba Cloud STS is a web service that provides a temporary access token to a cloud computing user. Through STS, you can grant a third-party application or federated user (whose user ID is managed by yourself) an access credential with a custom validity period and permissions. The third-party application or federated user can use the access credential to directly call the Alibaba Cloud product APIs or use the Alibaba Cloud product SDKs to access the cloud product APIs.

  - You do not need to expose your long-term key (AccessKey) to a third-party application. You need only to generate an access token and send it to the third-party application. You can customize the access permissions and validity period of this token.
  - The access token automatically becomes invalid upon expiration.

  An application is used as an example. The following figure shows the interaction process.



  The solution is described in detail as follows:

  i. Log on as an application user. You can manage your application user ID. You can customize the ID management system or use an external Web account or OpenID. For each valid application user, you can use the AppServer to precisely define the principle of least privilege (POLP).

  ii. The AppServer requests a security token from STS. Before calling STS, the AppServer needs to determine the POLP (described in policy syntax) of the application user and the expiration time of the authorization. Then, the AppServer calls the AssumeRole API of STS to obtain the security token.

  iii. STS returns a valid access credential to the AppServer, including a security token, a temporary access key (AccessKey ID and AccessKey Secret), and the expiration time.

  iv. The AppServer returns the access credential to the ClientApp. The ClientApp caches this credential. When the credential becomes invalid, the ClientApp must request a new valid access credential from the AppServer. For example, if the access credential is valid for one hour, the ClientApp can request the AppServer to update the access credential every 30 minutes.

  v. The ClientApp uses the locally cached access credential to request Alibaba Cloud service APIs. Cloud services detect the STS access credential, verify the credential based on STS, and correctly respond to user requests.

The key is to call the AssumeRole API of STS to obtain a valid access credential. You can also directly use the STS SDK to call this API.

- Use an STS credential to create a request with a signature

  After you obtain a temporary STS credential for your OssClient, the OssClient is generated based on the security token and temporary Access Key (AccessKey ID and AccessKey Secret). The following code provides an example of how to upload an object:

```
String accessKeyId = "<accessKeyId>";
String accessKeySecret = "<accessKeySecret>";
String securityToken = "<securityToken>"
// Take China (Hangzhou) as an example.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";

OSSClient client = new OSSClient(endpoint, accessKeyId, accessKeySecret, securityToken);
```

Add a signature to a URL for authorized temporary access

- Generate a signature for a URL

  You can generate a signature and add it to a URL for temporary access. During URL generation, you can specify the URL expiration time to limit the access duration.

  - Generate a signature and add it to a URL

    The following code provides an example of how to generate a URL with a signature:

```
String bucketName = "your-bucket-name";
String key = "your-object-key";

// Set the URL validity period to one hour.
Date expiration = new Date(new Date().getTime() + 3600 * 1000);

// Generate the URL with a signature.
URL url = client.generatePresignedUrl(bucketName, key, expiration);
```

    The generated URL supports access through GET by default, which grants users direct access to related content through a browser.

  - Generate a URL with a signature for other HTTP methods

    If you want to allow users to perform other temporary operations (such as the object upload and deletion), you may need to generate a URL with a signature for another method. The following code provides an example of how to generate a URL with a signature for another method:

```
// Generate a URL for the PUT method.
URL url = client.generatePresignedUrl(bucketName, key, expiration, HttpMethod.PUT);
```

    By setting HttpMethod.PUT, you can use the generated URL to upload objects.

- Add user-defined parameters (UserMetadata)

  If you want to generate a URL with a signature to upload objects with the header information such as UserMetadata and Content-Type specified, use the following code:

```
// Create a request.
GeneratePresignedUrlRequest generatePresignedUrlRequest = new GeneratePresignedUrlRequest
(bucketName, key);

// Set HttpMethod to PUT.
generatePresignedUrlRequest.setMethod(HttpMethod.PUT);

// Add UserMetadata.
generatePresignedUrlRequest.addUserMetadata("author", "baymax");

// Add Content-Type.
request.setContentType("application/octet-stream");

// Generate a signed URL.
URL url = client.generatePresignedUrl(generatePresignedUrlRequest);
```

  Note that only a URL with a signature is generated during the preceding process. You need to add Object Meta to the access request header. The following code provides an example of how to add Object Meta to the request header.

- Use a URL with a signature to send a request

  Currently, the Java SDK allows you to add a signature to a URL to send PutObject and GetObject requests.

- Add a signature to a URL to send a GetObject request

```
// Generate a signature string on the server for a URL.
OSSClient Server = new OSSClient(endpoint, accessId, accessKey);
Date expiration = DateUtil.parseRfc822Date("Wed, 18 Mar 2015 14:20:00 GMT");
GeneratePresignedUrlRequest request = new GeneratePresignedUrlRequest(bucketName, key, Http
Method.GET);
// Set the expiration time.
request.setExpiration(expiration);
// Generate the URL with the signature (HTTP GET request).
URL signedUrl = Server .generatePresignedUrl(request);
System.out.println("signed url for getObject: " + signedUrl);

// Use the URL with the signature string to send the request on the client.
OSSClient client = new OSSClient(endpoint, accessKeyId, accessKeySecret);
Map<String, String> customHeaders = new HashMap<String, String>();
// Add the GetObject request header.
customHeaders.put("Range", "bytes=100-1000");
OSSObject object = client.getObject(signedUrl,customHeaders);
```

- Add a signature to a URL to send a PutObject request

```
// Generate a signature string on the server for a URL.
OSSClient Server = new OSSClient(endpoint, accessKeyId, accessKeySecret);
Date expiration = DateUtil.parseRfc822Date("Wed, 18 Mar 2015 14:20:00 GMT");
GeneratePresignedUrlRequest request = new GeneratePresignedUrlRequest(bucketName, key, Http
Method.PUT);
// Set the expiration time.
request.setExpiration(expiration);
// Set Content-Type.
request.setContentType("application/octet-stream");
// Add the user-defined Object Meta.
request.addUserMetadata("author", "aliy");
// Generate the URL with the signature (HTTP PUT request).
URL signedUrl = Server.generatePresignedUrl(request);
System.out.println("signed url for putObject: " + signedUrl);

// Use the URL with the signature string to send the request on the client.
OSSClient client = new OSSClient(endpoint, accessKeyId, accessKeySecret);
File f = new File(filePath);
FileInputStream fin = new FileInputStream(f);
// Add the PutObject request header.
Map<String, String> customHeaders = new HashMap<String, String>();
customHeaders.put("Content-Type", "application/octet-stream");
// Add the user-defined Object Meta.
customHeaders.put("x-oss-meta-author", "aliy");
PutObjectResult result = client.putObject(signedUrl, fin, f.length(), customHeaders);
```

2.4.2.1.10. Manage lifecycle rules

OSS allows you to set lifecycle rules to automatically delete expired objects, thereby saving storage space. You can set multiple lifecycle rules for the same bucket. Each rule includes:

- Rule ID: The ID identifies the rule and must be unique.
- Policy: The rule applies only to objects with a specified prefix.
- Expiration: It can be specified in any of the following ways:
  i. Set by Number of Days: It specifies the number of days from the last modification time of objects.
  ii. Set by Date: It specifies the date prior to which objects are created. If objects are created prior to the date, these objects are deleted.
  iii. Prefix: All objects with this prefix are deleted on a specific date, regardless of the last modification time of objects. We recommend that you do not set this parameter.
- Status: It specifies whether this lifecycle rule is enabled.

The preceding lifecycle rules apply to all the objects in a specified bucket or the objects with the specified prefix. You can also set lifecycle rules for parts that are uploaded with uploadPart. The lifecycle of parts is similar to that of objects. Two types of expiration time are supported. The time of Init Multipart Upload applies to the effective time.

Set lifecycle rules

Use the following code to configure lifecycle rules:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// It is highly risky to log on with the AccessKey of an Apsara Stack tenant account because the account has permissions on all APIs in OSS. We recommend that you log on as a RAM user to access APIs or perform routine operations and maintenance. To create a RAM account, log on to https://ram.console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
String bucketName = "<Your bucket name>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
SetBucketLifecycleRequest request = new SetBucketLifecycleRequest(bucketName);
// Set the rule ID and object name prefix.
String ruleId0 = "rule0";
String matchPrefix0 = "A0/";
String ruleId1 = "rule1";
String matchPrefix1 = "A1/";
String ruleId2 = "rule2";
String matchPrefix2 = "A2/";
String ruleId3 = "rule3";
String matchPrefix3 = "A3/";
// Set the expiration duration to 3 days after last modified date.
request.AddLifecycleRule(new LifecycleRule(ruleId0, matchPrefix0, RuleStatus.Enabled, 3));
// Set the expiration date to delete objects that are created before the date.
LifecycleRule rule = new LifecycleRule(ruleId1, matchPrefix1, RuleStatus.Enabled);
rule.setCreatedBeforeDate(DateUtil.parseISO8601Date("2022-10-12T00:00:00.000Z"));
request.AddLifecycleRule(rule);
// Set the expiration duration to 3 days for parts in an object.
rule = new LifecycleRule(ruleId2, matchPrefix2, RuleStatus.Enabled);
LifecycleRule.AbortMultipartUpload abortMultipartUpload = new LifecycleRule.AbortMultipartUpload();
abortMultipartUpload.setExpirationDays(3);
rule.setAbortMultipartUpload(abortMultipartUpload);
request.AddLifecycleRule(rule);
// Set expiration date to delete parts that are created before the date.
```

```
rule = new LifecycleRule(ruleId3, matchPrefix3, RuleStatus.Enabled);
abortMultipartUpload = new LifecycleRule.AbortMultipartUpload();
abortMultipartUpload.setCreatedBeforeDate(DateUtil.parseISO8601Date("2022-10-12T00:00:00.000Z"));
rule.setAbortMultipartUpload(abortMultipartUpload);
request.AddLifecycleRule(rule);
ossClient.setBucketLifecycle(request);
// Close your client.
ossClient.shutdown();
```

View lifecycle rules

The following code provides an example of how to view lifecycle rules:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// It is highly risky to log on with the AccessKey of an Apsara Stack tenant account because the account has permissions on all APIs in OSS. We recommend that you log on as a RAM user to access APIs or perform routine operations and maintenance. To create a RAM account, log on to https://ram.console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
String bucketName = "<Your bucket name>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
List<LifecycleRule> rules = ossClient.getBucketLifecycle(bucketName);
for (LifecycleRule rule : rules) {
   System.out.println(rule.getId());
   System.out.println(rule.getPrefix());
   System.out.println(rule.getExpirationDays());
   System.out.println(rule.getCreatedBeforeDate());
   if(rule.hasAbortMultipartUpload()) {
      System.out.println(rule.getAbortMultipartUpload().getExpirationDays());
      System.out.println(rule.getAbortMultipartUpload().getCreatedBeforeDate());
   }
}
// Close your client.
ossClient.shutdown();
```

Clear lifecycle rules

Use the following code to clear lifecycle rules:

```
// This example uses endpoint China (Hangzhou). Specify the actual endpoint based on your requirements.
String endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
// It is highly risky to log on with the AccessKey of an Apsara Stack tenant account because the account has permissions on all APIs in OSS. We recommend that you log on as a RAM user to access APIs or perform routine operations and maintenance. To create a RAM account, log on to https://ram.console.aliyun.com.
String accessKeyId = "<Your AccessKey ID>";
String accessKeySecret = "<Your AccessKey Secret>";
String bucketName = "<Your bucket name>";
// Create an OssClient instance.
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
ossClient.deleteBucketLifecycle(bucketName);
// Close your client.
ossClient.shutdown();
```

2.4.2.1.11. CORS

CORS allows Web applications to access resources that belong to another region. OSS provides APIs for developers to conveniently control CORS permissions.

Set CORS rules

You can use setBucketCors to set a CORS rule for a specified bucket. If a rule already exists, it is replaced by the new one. You can use the CORSRule class to set specific rules. Example:

```
SetBucketCORSRequest request = new SetBucketCORSRequest();
request.setBucketName(bucketName);
// Specify a container that stores CORS rules. Each bucket allows 10 rules at most.
ArrayList<CORSRule> putCorsRules = new ArrayList<CORSRule>();
CORSRule corRule = new CORSRule();
ArrayList<String> allowedOrigin = new ArrayList<String>();
// Specify the allowed source of cross-origin requests.
allowedOrigin.add( "http://www.b.com");
ArrayList<String> allowedMethod = new ArrayList<String>();
// Specify the allowed cross-origin request methods (GET, PUT, DELETE, POST, and HEAD).
allowedMethod.add("GET");
ArrayList<String> allowedHeader = new ArrayList<String>();
// Specify whether the headers specified by Access-Control-Request-Headers in the OPTIONS prefetch c
ommand are allowed.
allowedHeader.add("x-oss-test");
ArrayList<String> exposedHeader = new ArrayList<String>();
// Specify the response header that allows user access from applications.
exposedHeader.add("x-oss-test1");
corRule.setAllowedMethods(allowedMethod);
corRule.setAllowedOrigins(allowedOrigin);
corRule.setAllowedHeaders(allowedHeader);
corRule.setExposeHeaders(exposedHeader);
// Specify the cache time for the response of a browser prefetch (OPTIONS) request for a specific resou
rce, in seconds.
corRule.setMaxAgeSeconds(10);
// A maximum of 10 rules are allowed.
putCorsRules.add(corRule);
request.setCorsRules(putCorsRules);
oss.setBucketCORS(request);
```

> **Note**
>
> - You can set a maximum of 10 rules for a bucket.
> - Only one wildcard (*) is supported by AllowedOrigins and AllowedMethods. * indicates that requets from all regions or operations are allowed.
> - However, AllowedHeaders and ExposeHeaders do not support wildcards (*).

Obtain CORS rules

You can use GetBucketCors to obtain CORS rules of a bucket. Example:

```
ArrayList<CORSRule> corsRules;
// Obtain the list of CORS rules.
corsRules = (ArrayList<CORSRule>) oss.getBucketCORSRules(bucketName);
for (CORSRule rule : corsRules) {
    for (String allowedOrigin1 : rule.getAllowedOrigins()) {
        // Obtain allowed cross-origin request sources.
        System.out.println(allowedOrigin1);
    }
    for (String allowedMethod1: rule.getAllowedMethods()) {
        // Obtain allowed cross-origin request methods.
        System.out.println(allowedMethod1);
    }
    if (rule.getAllowedHeaders().size() > 0){
        for (String allowedHeader1 : rule.getAllowedHeaders()) {
            //Obtain the list of allowed headers.
            System.out.println(allowedHeader1);
        }
    }
    if (rule.getExposeHeaders().size() > 0) {
        for (String exposeHeader : rule.getExposeHeaders()) {
        // Obtain allowed headers.
        System.out.println(exposeHeader);
        }
    }
    if ( null ! = rule.getMaxAgeSeconds()) {
        System.out.println(rule.getMaxAgeSeconds());
    }
}
```

Delete CORS rules

You can disable CORS for a specified bucket and delete all CORS rules of the bucket.

```
// Delete all CORS rules of the bucket.
oss.deleteBucketCORSRules(bucketName);
```

2.4.2.1.12. Set access logging

Overview

OSS allows you to set bucket access logging. After configurations, access to a bucket is recorded in logs that are stored in a user-specified bucket in OSS. The log object name format is as follows:

```
<TargetPrefix><SourceBucket>-YYYY-mm-DD-HH-MM-SS-UniqueString
```

You need to specify `TargetPrefix`. An access logging rule consists of the following two parts:

- target_bucket: the bucket where logs are stored
- target_prefix: the prefix of the stored log objects

Enable bucket access logging

The following code provides an example of how to use `OSSClient.setBucketLogging` to enable bucket access logging:

```
SetBucketLoggingRequest request = new SetBucketLoggingRequest("sourceBucket");
request.setTargetBucket("targetBucket");
request.setTargetPrefix("targetPrefix");
ossClient.setBucketLogging(request);
```

View bucket access logging settings

The following code provides an example of how to use `OSSClient.getBucketLogging` to view access logging settings:

```
BucketLoggingResult result = ossClient.getBucketLogging("sourceBucket");
System.out.println(result.getTargetBucket());
System.out.println(result.getTargetPrefix());
```

Disable bucket access logging

The following code provides an example of how to use `OSSClient.setBucketLogging` to disable bucket access logging:

```
SetBucketLoggingRequest request = new SetBucketLoggingRequest("sourceBucket");
request.setTargetBucket(null);
request.setTargetPrefix(null);
ossClient.setBucketLogging(request);
```

2.4.2.1.13. Static website hosting

If an error occurs when the OSS allows you to direct your domain name to an OSS service URL. In this way, when you access your website, you actually access an OSS bucket. You need to respectively set the names of objects (in the bucket) corresponding to the homepage (index) and error page (error) of the website.

Set hosting pages

The following code provides an example of how to use `OSSClient.setBucketWebsite` to set hosting pages:

```
SetBucketWebsiteRequest request = new SetBucketWebsiteRequest("bucketName");
request.setIndexDocument("index.html");
request.setErrorDocument("error.html");
ossClient.setBucketWebsite(request);
```

View hosting pages

The following code provides an example of how to use `OSSClient.getBucketWebsite` to view hosting pages:

```
BucketWebsiteResult result = ossClient.getBucketWebsite("bucketName");
System.out.println(result.getIndexDocument());
System.out.println(result.getErrorDocument());
```

Delete hosting pages

The following code provides an example of how to use `OSSClient.deleteBucketWebsite` to delete hosting pages:

```
ossClient.deleteBucketWebsite("bucketName");
```

2.4.2.1.14. Hotlinking

To prevent user data in OSS from being leeched, OSS supports hotlinking based on the referer field in the HTTP header.

Set a referer whitelist

You can use the following code to set a referer whitelist:

```
OSSClient client = new OSSClient(endpoint, accessId, accessKey);
List<String> refererList = new ArrayList<String>();
// Add a referer item.
refererList.add("http://www.aliyun.com");
refererList.add("http://www. *.com");
refererList.add("http://www. *.aliyuncs.com");
// Allow the referer field to be empty and set a bucket referer list.
BucketReferer br = new BucketReferer(true, refererList);
client.setBucketReferer(bucketName, br);
```

> **Note** You can use wildcard characters (*) and (?) for the refer parameter.

Obtain the referer whitelist

```
// Obtain the bucket referer list.
br = client.getBucketReferer(bucketName);
refererList = br.getRefererList();
for (String referer : refererList) {
   System.out.println(referer);
}
```

```
Example of output results:
http://www.aliyun.com
http://www. *.com"
http://www.?.aliyuncs.com
```

Clear the referer whitelist

You cannot clear the referer whitelist directly. You can only reset it to overwrite the previous rules.

```
OSSClient client = new OSSClient(endpoint, accessId, accessKey);
// Allow an empty referer field by default and clear the referer whitelist.
BucketReferer br = new BucketReferer();
client.setBucketReferer(bucketName, br);
```

2.4.2.1.15. IMG

Image processing (IMG) is a secure, cost-effective, and highly reliable image processing service provided by OSS. IMG is capable of processing large amounts of images. After source images are uploaded to OSS, you can call the Representational State Transfer (RESTful) API to process images anytime, anywhere, and on any Internet device. You can create your own image processing service based on OSS IMG.

Basic features

OSS provides the following IMG features:

- Obtain image information.
- Convert image formats.
- Resize, crop, and rotate images.
- Apply image effects.
- Add watermarks: allows you to add images, text, or image-text watermarks to another image.
- Customize imaging processing styles. Log on to the OSS console, click a bucket name to go to the Bucket Information tab. Choose **Image Processing** > **Create Style** to customize an image processing style.
- Image processing access rules: calls multiple IMG features.

How to use IMG

IMG uses the standard `HTTP GET` request. You can set processing parameters in QueryString of the URL.

- Anonymous access

  If the access permission for an image object is public-read, as described in the following table, you can access the image anonymously.

Bucket permission	Object permission
Public-read or public-read-write	Default
Any permission	Public-read or public-read-write

  You can access IMG anonymously using a third-level domain name in the following format:

```
http://bucket.<endpoint>/object?x-oss-process=image/action,parame_value
```

Parameter	Description
bucket	The name of the bucket.
endpoint	The endpoint used to access the region to which the bucket belongs.
object	The name of the image object.
image	The reserved identifier for IMG.
action	Operations on the image, such as resizing, cropping, and rotating.
param	The parameter corresponding to the operations performed on the image.

  - Basic operations

    For example, scale an image to a width of 100 px. Adjust the height based on the ratio.

```
http://image-demo.oss-cn-hangzhou.aliyuncs.com/example.jpg?x-oss-process=image/resize,w_100
```

- Custom image styles

  You can use third-level domain names to access processed images. The URL format is as follows:

  ```
  http://<yourBucketName>.<yourEndpoint>/<yourObjectName>?x-oss-process=style/<yourStyleName>
  ```

  - style: specifies the reserved identifier of a custom image style.
  - yourStyleName: specifies the name of a custom image style. It is the name of the rule that is specified in the OSS console.

  Example:

  ```
  http://image-demo.oss-cn-hangzhou.aliyuncs.com/example.jpg?x-oss-process=style/oss-pic-style-w-100
  ```

- Cascade operations

  Cascade operations allow you to perform multiple operations on an image in sequence. The format is as follows:

  ```
  http://<yourBucketName>.<yourEndpoint>/<yourObjectName>?x-oss-process=image/<yourAction1>,<yourParamValue1>/<yourAction2>,<yourParamValue2>/...
  ```

  Example:

  ```
  http://image-demo.oss-cn-hangzhou.aliyuncs.com/example.jpg?x-oss-process=image/resize,w_100/rotate,90
  ```

- Access through HTTPS

  IMG supports access through HTTPS. Example:

  ```
  https://image-demo.oss-cn-hangzhou.aliyuncs.com/example.jpg?x-oss-process=image/resize,w_100
  ```

- Authorized access

  If the access permission included in the ACL for an image object is Private, as described in the following table, you must be authorized to access IMG.

Bucket permission	Object permission
Private	Default
Any permission	Private

  The following code provides an example of how to add a signature to a URL to access IMG:

```
String endpoint = "<endpoint, such as http://oss-cn-hangzhou.aliyuncs.com>";
String accessKeyId = "<accessKeyId>";
String accessKeySecret = "<accessKeySecret>";
String bucketName = "<bucketName>";
private static String key = "example.jpg";
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Set the IMG style.
String style = "image/resize,m_fixed,w_100,h_100/rotate,90";
// Set the validity period to 10 minutes.
Date expiration = new Date(new Date().getTime() + 1000 * 60 * 10 );
GeneratePresignedUrlRequest req = new GeneratePresignedUrlRequest(bucketName, key, HttpMet
hod.GET);
req.setExpiration(expiration);
req.setProcess(style);
URL signedUrl = ossClient.generatePresignedUrl(req);
System.out.println(signedUrl);
```

Note

- You can set Create Style, HTTPS, and Cascade Processing for authorized access.
- Use `Date expiration = DateUtil.parseRfc822Date("Wed, 21 Dec 2022 14:20:00 GMT");` to specify the expiration time.

- Access with SDKs

  You can directly use SDKs to access and process image objects with any ACLs.

  Note

  - For the complete IMG code, see GitHub.
  - You can use the SDK to operate image objects by setting Create Style, HTTPS, and Cascade Processing.

  - Basic operations

    Basic IMG operations include obtaining image information, converting image formats, resizing, cropping, rotating, applying effects, and adding watermarks.

    ```
    String endpoint = "<endpoint, such as http://oss-cn-hangzhou.aliyuncs.com>";
    String accessKeyId = "<accessKeyId>";
    String accessKeySecret = "<accessKeySecret>";
    String bucketName = "<bucketName>";
    String key = "example.jpg";
    OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
    // Resize the image.
    String style = "image/resize,m_fixed,w_100,h_100";
    ```

```
GetObjectRequest request = new GetObjectRequest(bucketName, key);
request.setProcess(style);
ossClient.getObject(request, new File("example-resize.jpg"));
// Crop the image.
style = "image/crop,w_100,h_100,x_100,y_100,r_1";
request = new GetObjectRequest(bucketName, key);
request.setProcess(style);
ossClient.getObject(request, new File("example-crop.jpg"));
// Rotate the image.
style = "image/rotate,90";
request = new GetObjectRequest(bucketName, key);
request.setProcess(style);
ossClient.getObject(request, new File("example-rotate.jpg"));
// Sharpen the image.
style = "image/sharpen,100";
request = new GetObjectRequest(bucketName, key);
request.setProcess(style);
ossClient.getObject(request, new File("example-sharpen.jpg"));
// Add watermarks.
style = "image/watermark,text_SGVsbG8g5Zu-54mH5pyN5YqhIQ";
request = new GetObjectRequest(bucketName, key);
request.setProcess(style);
ossClient.getObject(request, new File("example-watermark.jpg"));
// Convert the image format.
style = "image/format,png";
request = new GetObjectRequest(bucketName, key);
request.setProcess(style);
ossClient.getObject(request, new File("example-format.png"));
// Obtain image information.
style = "image/info";
request = new GetObjectRequest(bucketName, key);
request.setProcess(style);
ossClient.getObject(request, new File("example-info.txt"));
ossClient.shutdown();
```

- Custom image styles

```
String endpoint = "<endpoint, such as http://oss-cn-hangzhou.aliyuncs.com>";
String accessKeyId = "<accessKeyId>";
String accessKeySecret = "<accessKeySecret>";
String bucketName = "<bucketName>";
String key = "example.jpg";
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Customize a style.
String style = "style/oss-pic-style-w-100";
GetObjectRequest request = new GetObjectRequest(bucketName, key);
request.setProcess(style);
ossClient.getObject(request, new File("example-new.jpg"));
ossClient.shutdown();
```

- Cascade operations

```
String endpoint = "<endpoint, such as http://oss-cn-hangzhou.aliyuncs.com>";
String accessKeyId = "<accessKeyId>";
String accessKeySecret = "<accessKeySecret>";
String bucketName = "<bucketName>";
private static String key = "example.jpg";
OSSClient ossClient = new OSSClient(endpoint, accessKeyId, accessKeySecret);
// Perform cascade operations.
String style = "image/resize,m_fixed,w_100,h_100/rotate,90";
GetObjectRequest request = new GetObjectRequest(bucketName, key);
request.setProcess(style);
ossClient.getObject(request, new File("example-new.jpg"));
ossClient.shutdown();
```

2.4.2.1.16. Exception handling

If an exception occurs when you call the OssClient API, the related operation fails. Otherwise, the related operation succeeds. If an exception occurs, the data returned by the API is invalid. OSS Java SDK exceptions are classified into two types: OSSException and ClientException. Both are inherited from RuntimeException.

Exception handling example

```
try {
    // Do some operations with the instance here, such as put object...
    client.putObject(...);
} catch (OSSException oe) {
    System.out.println("Caught an OSSException, which means your request made it to OSS, "
            + "but was rejected with an error response for some reason.") ;
    System.out.println("Error Message: " + oe.getErrorCode());
    System.out.println("Error Code:       " + oe.getErrorCode());
    System.out.println("Request ID:      " + oe.getRequestId());
    System.out.println("Host ID:           " + oe.getHostId());
} catch (ClientException e) {
    System.out.println("Caught an ClientException, which means the client encountered "
            + "a serious internal problem while trying to communicate with OSS, "
            + "such as not being able to access the network.") ;
    System.out.println("Error Message: " + ce.getMessage());
} finally {
    if (client ! = null) {
        client.shutdown();
    }
}
```

ClientException

A ClientException occurs when a client attempts to send a request or transmit data to OSS. For example, a ClientException is thrown when a client sends a request but the network is inaccessible or when the upload of an object fails due to an I/O exception.

OSSException

OSSException indicates a server error caused by the parsing of a server error message. The error code and error message are returned, so that you can locate the problem and handle it properly.

OSSException typically contains the following error information:

- Code: the error code that OSS returns to the user.
- Message: the detailed error message provided by OSS.
- RequestId: the UUID of a request. If the problem persists, you can seek help from OSS development engineers and provide them with the request ID.
- HostId: the ID of a host to identify the accessed OSS cluster, which is the same as the host ID specified in the request.

Common OSS error codes

Error code	Description	HTTP status code
AccessDenied	The error message returned when the access is denied.	403

Error code	Description	HTTP status code
BucketAlreadyExists	The error message returned when the bucket already exists.	409
BucketNotEmpty	The error message returned when the bucket is not empty.	409
EntityTooLarge	The error message returned when the entity is too large.	400
EntityTooSmall	The error message returned when the entity is too small.	400
FileGroupTooLarge	The error message returned when the object group is too large.	400
FilePartNotExist	The error message returned when the object part does not exist.	400
FilePartStale	The error message returned when the object part has expired.	400
InvalidArgument	The error message returned when the parameter format is invalid.	400
InvalidAccessKeyId	The error message returned when the AccessKey ID does not exist.	403
InvalidBucketName	The error message returned when the bucket name is invalid.	400
InvalidDigest	The error message returned when the digest is invalid.	400
InvalidObjectName	The error message returned when the object name is invalid.	400
InvalidPart	The error message returned when the part is invalid.	400
InvalidPartOrder	The error message returned when the part sequence is invalid.	400
InvalidTargetBucketForLogging	The error message returned when the logging operation involves an invalid target bucket.	400
InternalError	The error message returned when an internal OSS error occurs.	500
MalformedXML	The error message returned when the XML format is invalid.	400
MethodNotAllowed	The error message returned when the method is not supported.	405

Error code	Description	HTTP status code
MissingArgument	The error message returned when a parameter is missing.	411
MissingContentLength	The error message returned when the content length is missing.	411
NoSuchBucket	The error message returned when no such bucket exists.	404
NoSuchKey	The error message returned when no such key exists.	404
NoSuchUpload	The error message returned when no such multipart upload ID exists.	404
NotImplemented	The error message returned when the method cannot be implemented.	501
PreconditionFailed	The error message returned when a precondition error occurs.	412
RequestTimeTooSkewed	The error message returned when the duration between the request sending time and the server responding time exceeds 15 minutes.	403
RequestTimeout	The error message returned when the request has timed out.	400
SignatureDoesNotMatch	The error message returned when a signature error occurs.	403
InvalidEncryptionAlgorithmError	The error message returned when the specified encryption algorithm (entropy) is invalid.	400

2.4.2.1.17. FAQs

JAR package conflicts

An error similar to the following is returned while you are using the OSS Java SDK:

```
Exception in thread "main" java.lang.NoClassDefFoundError: org/apache/http/ssl/TrustStrategy
    at com.aliyun.oss.OSSClient.<init>(OSSClient.java:268)
    at com.aliyun.oss.OSSClient.<init>(OSSClient.java:193)
    at com.aliyun.oss.demo.HelloOSS.main(HelloOSS.java:77)
Caused by: java.lang.ClassNotFoundException: org.apache.http.ssl.TrustStrategy
    at java.net.URLClassLoader$1.run(URLClassLoader.java:366)
    at java.net.URLClassLoader$1.run(URLClassLoader.java:355)
    at java.security.AccessController.doPrivileged(Native Method)
    at java.net.URLClassLoader.findClass(URLClassLoader.java:354)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:425)
    at sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:308)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:358)
    ... 3 more
```

Or

```
Exception in thread "main" java.lang.NoSuchFieldError: INSTANCE
 at org.apache.http.impl.io.DefaultHttpRequestWriterFactory.<init>(DefaultHttpRequestWriterFactory.java:52)
 at org.apache.http.impl.io.DefaultHttpRequestWriterFactory.<init>(DefaultHttpRequestWriterFactory.java:56)
 at org.apache.http.impl.io.DefaultHttpRequestWriterFactory.<clinit>(DefaultHttpRequestWriterFactory.java:46)
 at org.apache.http.impl.conn.ManagedHttpClientConnectionFactory.<init>(ManagedHttpClientConnectionFactory.java:82)
 at org.apache.http.impl.conn.ManagedHttpClientConnectionFactory.<init>(ManagedHttpClientConnectionFactory.java:95)
 at org.apache.http.impl.conn.ManagedHttpClientConnectionFactory.<init>(ManagedHttpClientConnectionFactory.java:104)
 at org.apache.http.impl.conn.ManagedHttpClientConnectionFactory.<clinit>(ManagedHttpClientConnectionFactory.java:62)
 at org.apache.http.impl.conn.PoolingHttpClientConnectionManager$InternalConnectionFactory.<init>(PoolingHttpClientConnectionManager.java:572)
 at org.apache.http.impl.conn.PoolingHttpClientConnectionManager.<init>(PoolingHttpClientConnectionManager.java:174)
 at org.apache.http.impl.conn.PoolingHttpClientConnectionManager.<init>(PoolingHttpClientConnectionManager.java:158)
 at org.apache.http.impl.conn.PoolingHttpClientConnectionManager.<init>(PoolingHttpClientConnectionManager.java:149)
 at org.apache.http.impl.conn.PoolingHttpClientConnectionManager.<init>(PoolingHttpClientConnectionManager.java:125)
 at com.aliyun.oss.common.comm.DefaultServiceClient.createHttpClientConnectionManager(DefaultServiceClient.java:237)
 at com.aliyun.oss.common.comm.DefaultServiceClient.<init>(DefaultServiceClient.java:78)
 at com.aliyun.oss.OSSClient.<init>(OSSClient.java:268)
 at com.aliyun.oss.OSSClient.<init>(OSSClient.java:193)
 at OSSManagerImpl.upload(OSSManagerImpl.java:42)
 at OSSManagerImpl.main(OSSManagerImpl.java:63)
```

There may be JAR package conflicts in your project. The cause is that the OSS Java SDK uses Apache httpclient 4.4.1, whereas your project uses Apache httpclient or commons-httpclient that conflicts with Apache httpclient 4.4.1. Run mvn dependency:tree in your project directory to view the package and version that your project uses. For example, the preceding error occurs in the project because Apache httpclient 4.3 is used.

```
[INFO] --- maven-dependency-plugin:2.2:tree (default-cli) @ maven-demo ---
[INFO] com.aliyun.oss:maven-demo:jar:0.1.1-SNAPSHOT
[INFO] +- junit:junit:jar:4.10:test
[INFO] |  \- org.hamcrest:hamcrest-core:jar:1.1:test
[INFO] +- org.apache.httpcomponents:httpclient:jar:4.3:compile
[INFO] |  +- org.apache.httpcomponents:httpcore:jar:4.3:compile
[INFO] |  +- commons-logging:commons-logging:jar:1.1.3:compile
[INFO] |  \- commons-codec:commons-codec:jar:1.6:compile
[INFO] \- com.aliyun.oss:aliyun-sdk-oss:jar:2.2.1:compile
[INFO]    +- org.jdom:jdom:jar:1.1:compile
[INFO]    \- net.sf.json-lib:json-lib:jar:jdk15:2.4:compile
[INFO]       +- commons-beanutils:commons-beanutils:jar:1.8.0:compile
[INFO]       +- commons-collections:commons-collections:jar:3.2.1:compile
[INFO]       +- commons-lang:commons-lang:jar:2.5:compile
[INFO]       \- net.sf.ezmorph:ezmorph:jar:1.0.6:compile
```

There are two solutions to jar conflicts.

- Use a unified version. If your project uses a version in conflict with Apache httpclient 4.4.1, you must use the 4.4.1 version. Remove dependency on other versions of Apache httpclient in POM. xml. If your project uses commons-httpclient, conflicts may also occur. Remove commons-httpclient.
- Resolve dependency conflicts. If your project is dependent on multiple third-party packages and the third-party packages are dependent on different versions of Apache httpclient, your project may contain dependency conflicts. Use exclusion to remove the conflicts. For more information, see maven guides.

The OSS Java SDK is dependent on the following versions of packages. The solution to conflicts is similar to that for httpclient, and therefore it is not repeated here.

```
[INFO] com.aliyun.oss:maven-demo:jar:0.1.1-SNAPSHOT
[INFO] +- junit:junit:jar:4.10:test
[INFO] |  \- org.hamcrest:hamcrest-core:jar:1.1:test
[INFO] \- com.aliyun.oss:aliyun-sdk-oss:jar:2.2.1:compile
[INFO]    +- org.apache.httpcomponents:httpclient:jar:4.4.1:compile
[INFO]    |  +- org.apache.httpcomponents:httpcore:jar:4.4.1:compile
[INFO]    |  +- commons-logging:commons-logging:jar:1.2:compile
[INFO]    |  \- commons-codec:commons-codec:jar:1.9:compile
[INFO]    +- org.jdom:jdom:jar:1.1:compile
[INFO]    \- net.sf.json-lib:json-lib:jar:jdk15:2.4:compile
[INFO]       +- commons-beanutils:commons-beanutils:jar:1.8.0:compile
[INFO]       +- commons-collections:commons-collections:jar:3.2.1:compile
[INFO]       +- commons-lang:commons-lang:jar:2.5:compile
[INFO]       \- net.sf.ezmorph:ezmorph:jar:1.0.6:compile
```

Missing files

If the following errors occur when you use OSS Java SDK:

```
Exception in thread "main" java.lang.NoClassDefFoundError: org/apache/http/auth/Credentials
    at com.aliyun.oss.OSSClient.<init>(OSSClient.java:268)
    at com.aliyun.oss.OSSClient.<init>(OSSClient.java:193)
    at com.aliyun.oss.demo.HelloOSS.main(HelloOSS.java:76)
Caused by: java.lang.ClassNotFoundException: org.apache.http.auth.Credentials
    at java.net.URLClassLoader$1.run(URLClassLoader.java:366)
    at java.net.URLClassLoader$1.run(URLClassLoader.java:355)
    at java.security.AccessController.doPrivileged(Native Method)
    at java.net.URLClassLoader.findClass(URLClassLoader.java:354)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:425)
    at sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:308)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:358)
    ... 3 more
```

Or

```
Exception in thread "main" java.lang.NoClassDefFoundError: org/apache/http/protocol/HttpContext
    at com.aliyun.oss.OSSClient.<init>(OSSClient.java:268)
    at com.aliyun.oss.OSSClient.<init>(OSSClient.java:193)
    at com.aliyun.oss.demo.HelloOSS.main(HelloOSS.java:76)
Caused by: java.lang.ClassNotFoundException: org.apache.http.protocol.HttpContext
    at java.net.URLClassLoader$1.run(URLClassLoader.java:366)
    at java.net.URLClassLoader$1.run(URLClassLoader.java:355)
    at java.security.AccessController.doPrivileged(Native Method)
    at java.net.URLClassLoader.findClass(URLClassLoader.java:354)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:425)
    at sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:308)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:358)
    ... 3 more
```

Or

```
Exception in thread "main" java.lang.NoClassDefFoundError: org/jdom/input/SAXBuilder
    at com.aliyun.oss.internal.ResponseParsers.getXmlRootElement(ResponseParsers.java:645)
    at ... ...
    at com.aliyun.oss.OSSClient.doesBucketExist(OSSClient.java:471)
    at com.aliyun.oss.OSSClient.doesBucketExist(OSSClient.java:465)
    at com.aliyun.oss.demo.HelloOSS.main(HelloOSS.java:82)
Caused by: java.lang.ClassNotFoundException: org.jdom.input.SAXBuilder
    at java.net.URLClassLoader$1.run(URLClassLoader.java:366)
    at java.net.URLClassLoader$1.run(URLClassLoader.java:355)
    at java.security.AccessController.doPrivileged(Native Method)
    at java.net.URLClassLoader.findClass(URLClassLoader.java:354)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:425)
    at sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:308)
    at java.lang.ClassLoader.loadClass(ClassLoader.java:358)
    ... 11 more
```

Your project may lack the necessary files for OSS Java SDK compilation and execution. Dependencies of OSS Java SDK are as follows:

- aliyun-sdk-oss-2.2.1.jar
- hamcrest-core-1.1.jar
- jdom-1.1.jar
- commons-codec-1.9.jar
- httpclient-4.4.1.jar
- commons-logging-1.2.jar
- httpcore-4.4.1.jar
- log4j-1.2.15.jar

Specifically, the log4j-1.2.15.jar package is optional. This package can be added when you need the logging feature. All other packages are required.

Solution: Add packages on which the OSS Java SDK is dependent to your project as follows:

- If you use Eclipse, refer to the Java-SDK user manual and choose **Installation > Method 2: Import the required packages into the Eclipse project.**
- If you use Ant, put the packages on which the OSS Java SDK is dependent into the lib directory of the project.
- If you use Javac or Java directly, use -classpath/-cp to specify the path of packages on which the OSS Java SDK is dependent, or put these packages into the classpath directory.

Connection timeout

The following exception is thrown when you run the OSS Java SDK:

```
com.aliyun.oss.ClientException: SocketException
    at com.aliyun.oss.common.utils.ExceptionFactory.createNetworkException(ExceptionFactory.java:71)
    at com.aliyun.oss.common.comm.DefaultServiceClient.sendRequestCore(DefaultServiceClient.java:116
)
    at com.aliyun.oss.common.comm.ServiceClient.sendRequestImpl(ServiceClient.java:121)
    at com.aliyun.oss.common.comm.ServiceClient.sendRequest(ServiceClient.java:67)
    at com.aliyun.oss.internal.OSSOperation.send(OSSOperation.java:92)
    at com.aliyun.oss.internal.OSSOperation.doOperation(OSSOperation.java:140)
    at com.aliyun.oss.internal.OSSOperation.doOperation(OSSOperation.java:111)
    at com.aliyun.oss.internal.OSSBucketOperation.getBucketInfo(OSSBucketOperation.java:1152)
    at com.aliyun.oss.OSSClient.getBucketInfo(OSSClient.java:1220)
    at com.aliyun.oss.OSSClient.getBucketInfo(OSSClient.java:1214)
    at com.aliyun.oss.demo.HelloOSS.main(HelloOSS.java:94)
Caused by: org.apache.http.conn.HttpHostConnectException: Connect to oss-test.oss-cn-hangzhou-inte
rnal.aliyuncs.com:80 [oss-test.oss-cn-hangzhou-internal.aliyuncs.com/10.84.135.99] failed: Connection ti
med out: connect
    at org.apache.http.impl.conn.DefaultHttpClientConnectionOperator.connect(DefaultHttpClientConnecti
onOperator.java:151)
    at org.apache.http.impl.conn.PoolingHttpClientConnectionManager.connect(PoolingHttpClientConnecti
onManager.java:353)
    at org.apache.http.impl.execchain.MainClientExec.establishRoute(MainClientExec.java:380)
    at org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:236)
    at org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:184)
    at org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
    at org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.java:184)
    at org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:82)
    at com.aliyun.oss.common.comm.DefaultServiceClient.sendRequestCore(DefaultServiceClient.java:113
)
    ... 9 more
```

The cause is an endpoint error or network connection failure. If the error cannot be located directly, use the OSSProbe tool to locate the possible causes of the error.

org.apache.http.NoHttpResponseException: The target server failed to respond

The following exception is thrown when you run the OSS Java SDK:

The cause is that no connection validity check was performed before the connection was reused. The preceding error occurs if an expired connection is reused. This is a bug in Apache httpclient 4.4. For more information, see HTTPCLIENT-1609. The bug is fixed in V4.4.1 and later. The preceding issue exists because Apache httpclient 4.4 is used in Java SDK V2.1.2 and later. Apache httpclient 4.4.1 is used in Java SDK V2.1.2 and later, and therefore the issue is fixed. If this issue occurs, upgrade the OSS Java SDK to V2.1.2 and later.

An error occurs when the OSS Java SDK is called

If an errors occurs when you call the OSS Java SDK, call `jstack -l <pid>` to view the stack. The error is displayed as follows:

```
"main" prio=6 tid=0x000000000291e000 nid=0xc40 waiting on condition [0x0000000002dae000]
java.lang.Thread.State: WAITING (parking)
   at sun.misc.Unsafe.park(Native Method)
   - parking to wait for  <0x00000007d85697f8> (a java.util.concurrent.locks.AbstractQueuedSynchronizer
$ConditionObject)
   at java.util.concurrent.locks.LockSupport.park(LockSupport.java:186)
   at java.util.concurrent.locks.AbstractQueuedSynchronizer$ConditionObject.await(AbstractQueuedSyn
chronizer.java:2043)
   at org.apache.http.pool.PoolEntryFuture.await(PoolEntryFuture.java:138)
   at org.apache.http.pool.AbstractConnPool.getPoolEntryBlocking(AbstractConnPool.java:306)
   at org.apache.http.pool.AbstractConnPool.access$000(AbstractConnPool.java:64)
   at org.apache.http.pool.AbstractConnPool$2.getPoolEntry(AbstractConnPool.java:192)
   at org.apache.http.pool.AbstractConnPool$2.getPoolEntry(AbstractConnPool.java:185)
   at org.apache.http.pool.PoolEntryFuture.get(PoolEntryFuture.java:107)
   at org.apache.http.impl.conn.PoolingHttpClientConnectionManager.leaseConnection(PoolingHttpClient
ConnectionManager.java:276)
   at org.apache.http.impl.conn.PoolingHttpClientConnectionManager$1.get(PoolingHttpClientConnectio
nManager.java:263)
   at org.apache.http.impl.execchain.MainClientExec.execute(MainClientExec.java:190)
   at org.apache.http.impl.execchain.ProtocolExec.execute(ProtocolExec.java:184)
   at org.apache.http.impl.execchain.RedirectExec.execute(RedirectExec.java:110)
   at org.apache.http.impl.client.InternalHttpClient.doExecute(InternalHttpClient.java:184)
   at org.apache.http.impl.client.CloseableHttpClient.execute(CloseableHttpClient.java:82)
   at com.aliyun.oss.common.comm.DefaultServiceClient.sendRequestCore(DefaultServiceClient.java:113
)
   at com.aliyun.oss.common.comm.ServiceClient.sendRequestImpl(ServiceClient.java:123)
   at com.aliyun.oss.common.comm.ServiceClient.sendRequest(ServiceClient.java:68)
   at com.aliyun.oss.internal.OSSOperation.send(OSSOperation.java:94)
   at com.aliyun.oss.internal.OSSOperation.doOperation(OSSOperation.java:146)
   at com.aliyun.oss.internal.OSSOperation.doOperation(OSSOperation.java:113)
   at com.aliyun.oss.internal.OSSObjectOperation.getObject(OSSObjectOperation.java:229)
   at com.aliyun.oss.OSSClient.getObject(OSSClient.java:629)
   at com.aliyun.oss.OSSClient.getObject(OSSClient.java:617)
   at samples.HelloOSS.main(HelloOSS.java:49)
```

The cause is the connection leakage in the connection pool. It may be because the `OSSClient.getObject` is not closed after use. Check your program and ensure that no connection leak occurs. The following code provides an example of how to close OssObject:

```
// Read the object
OSSObject ossObject = ossClient.getObject(bucketName, key);
// Use ObjectContent and ObjectMetadata
// ...
// Make sure to close the connection after use.
ossObject.getObjectContent().close();
```

ConnectionClosedException: Premature end of Content-Length delimited message body ...

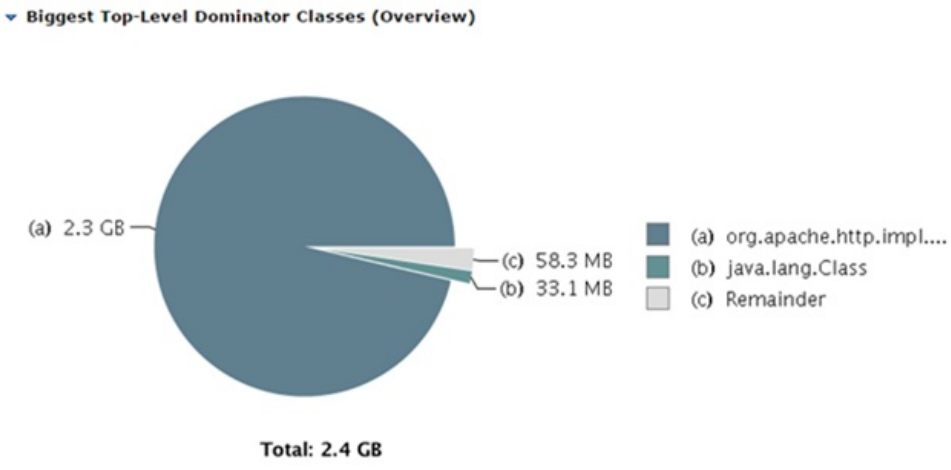
If an error similar to the following is reported during the use of `OSSClient.getObject` :

```
Exception in thread "main" org.apache.http.ConnectionClosedException: Premature end of Content-Leng
th delimited message body (expected: 11990526; received: 202880
    at org.apache.http.impl.io.ContentLengthInputStream.read(ContentLengthInputStream.java:180)
    at org.apache.http.impl.io.ContentLengthInputStream.read(ContentLengthInputStream.java:200)
    at org.apache.http.impl.io.ContentLengthInputStream.close(ContentLengthInputStream.java:103)
    at org.apache.http.impl.execchain.ResponseEntityProxy.streamClosed(ResponseEntityProxy.java:128)
    at org.apache.http.conn.EofSensorInputStream.checkClose(EofSensorInputStream.java:228)
    at org.apache.http.conn.EofSensorInputStream.close(EofSensorInputStream.java:174)
    at java.io.FilterInputStream.close(FilterInputStream.java:181)
    at java.io.FilterInputStream.close(FilterInputStream.java:181)
    at com.aliyun.oss.event.ProgressInputStream.close(ProgressInputStream.java:147)
    at java.io.FilterInputStream.close(FilterInputStream.java:181)
    at samples.HelloOSS.main(HelloOSS.java:39)
```

The cause is that the interval between the two data reading attempts exceeded one minute. The OSS closes the connection if no data is sent or received for more than one minute. This error occurs if your application functions as follows: Read part of the data, process the data, read the data, and then process the data. The data processing time is not fixed.

Memory leaks

When the OSS Java SDK project is called and runs for a while (depending on the business volume, the runtime may range from hours to days), the memory is exhausted. Use the memory analysis tool to analyze the memory usage. We recommend that you use Eclipse Memory Analyzer(MAT). The analysis result is similar to that shown in the following figure, where PoolingHttpClientConnectionManager occupies 96% of the memory.



Biggest Top-Level Dominator Classes

Label	Number of Objects	Used Heap Size	Retained Heap Size	Retained Heap, %
org.apache.http.impl.conn.PoolingHttpClientConnectionManager	112,701	3,606,432	2,517,081,408	96.33%
java.lang.Class	6,562	60,792	34,679,768	1.33%
∑ Total: 2 entries	119,263	3,667,224	2,551,761,176	

Cause: Multiple OssClient instances are created in the project, but OSSClient.shutdown is not called to close each client, leading to object leaks. Ensure that OSSClient.shutdown is called after an OssClient instance is used.

InterruptedException occurs when OSSClient.shutdown is called

The following exception is thrown when OSSClient.shutdown is called:

```
java.lang.InterruptedException: sleep interrupted
    at java.lang.Thread.sleep(Native Method)
    at com.aliyun.oss.common.comm.IdleConnectionReaper.run(IdleConnectionReaper:76)
```

Cause: There is a background thread from OSSClient: IdleConnectionReaper. Close idle connections regularly. If the shutdown method is called when the IdleConnectionReaper thread is asleep, the above exception will be thrown. If an error occurs when the OSS Java SDK V2.3.0 has fixed this issue. Use the following code to ignore this exception:

```
try {
serviceClient.shutdown();
} catch(Exception e) {
}
```

2.4.2.2. Python-SDK

2.4.2.2.1. Installation

Related resources

- GitHub project
- PyPi homepage

Environment dependency

This version of Python SDK is applicable to Python 2.6, 2.7, 3.3, 3.4, and 3.5. Follow the instructions on the Python official website to install an appropriate version of Python.

After Python is installed:

- Verify the Python version in Linux Shell:

  ```
  $ python -V
  Python 2.7.10
  ```

  If the preceding information is displayed, you have successfully installed Python 2.7.10.

- In Windows CMD, verify the Python version.

  ```
  C:\> python -V
  Python 2.7.10
  ```

  If the preceding information is displayed, you have successfully installed Python 2.7.10. If the "Not an internal or external command" message appears, choose Environment Variables > Path to check the configuration and add the Python installation path.

Install the SDK

- Install SDK by Pip

  ```
  pip install oss2
  ```

- Install the SDK through source code

  Download the SDK package of an appropriate version from github, decompress the package, and check whether the setup.py file exists in the directory.

  ```
  python setup.py install
  ```

- Verification

  Enter python on the command line and press Enter to check the SDK version in the Python environment.

  ```
  >>> import oss2
  >>> oss2.__version__
  '2.0.0'
  ```

  If the preceding information is displayed, you have successfully installed the Python SDK of the specific version. (Version 2.0.0 is used as an example.)

Uninstall the SDK

We recommend that you run pip to uninstall the SDK.

```
pip uninstall oss2
```

Sample program

The sample code for the Python SDK is in the examples directory. For more information, see GitHub. The following table describes the sample files in the sample program.

Sample file	Content
object_basic.py	Shows basic object operations, including how to upload, download, list, and delete objects.
object_extra.py	Shows advanced object operations, including how to set the language, configure the user-defined Object Meta, copy objects, and upload and append objects.
upload.py	Shows advanced use of Object Upload like resumable upload and multipart upload.
download.py	Shows object download use, such as downloading objects, downloading by range and resumable download.
object_check.py	Shows how to use data verification during uploads/downloads, including MD5 and CRC.
object_progress.py	Shows how to use the progress bar feature, including the upload progress bar and the download progress bar.
object_callback.py	Shows how to perform upload callback.
object_post.py	Shows how to use PostObject. The PostObject implementation is not dependent on the Python SDK.
sts.py	Shows how to use STS, including obtaining the temporary user key for playing a role and using the temporary user key to access OSS.
live_channel.py	Shows how to use LiveChannel.
image.py	Shows how to use the image service.
bucket.py	Shows how to manage buckets, including creating, deleting, and listing buckets.

Historical versions

This version of the Python SDK is incompatible with the earlier version 0.4.2, and it does not contain the command line tool osscmd.

2.4.2.2.2. Quick start

Overview

Ensure that you are familiar with OSS basic concepts, such as bucket, object, endpoint, AccessKey ID, and AccessKey Secret.

This section describes how to use the OSS Python SDK to access OSS, such as view the bucket list, upload and download objects, and view the object list. These programs are written in a script object by default, and can be executed through Python. Examples in the following sections may depend on previous ones. You can also paste these examples into the Python interactive environment for testing.

> **Note** Do not use running buckets to test the examples in this document.

View a bucket list

```
# -*- coding: utf-8 -*-

import oss2

auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
service = oss2. Service(auth, 'Your endpoint')

print([b.name for b in oss2. BucketIterator(service)])
```

Classes in the preceding code include:

- The oss2.Auth object contains the user's authentication information, that is, AccessKey ID and AccessKey Secret.
- The oss2.Service object is used for service-relevant operations. Currently, it is used to list buckets.
- The oss2.BucketIterator object is an iterator capable of traversing your bucket information.

Create a bucket

The following code provides an example of how to create a private bucket in China (Hangzhou):

```
bucket = oss2. Bucket(auth, 'http://oss-cn-hangzhou.aliyuncs.com', 'Your bucket name')
bucket.create_bucket(oss2.models.BUCKET_ACL_PRIVATE)
```

The oss2.Bucket object is used to upload, download, and delete objects and set the bucket.

Upload objects

The following code provides an example of how to upload a local file named local.txt to an OSS object named remote.txt:

```
bucket.put_object_from_file('remote.txt', 'local.txt')
```

Download objects

The following code provides an example of how to download an object from OSS to a local file:

```
bucket.get_object_to_file('remote.txt', 'local-backup.txt')
```

List objects

The following code provides an example of how to list 10 objects in a bucket:

```
from itertools import islice


for b in islice(oss2. ObjectIterator(bucket), 10):
    print(b.key)
```

The oss2.ObjectIterator object is an iterator that can be used like other iterators.

Delete objects

```
bucket.delete_object('remote.txt')
```

2.4.2.2.3. Initialization

Most operations of the OSS Python SDK are performed through oss2. Service and oss2. Bucket. The following code describes how to initialize these two classes.

Set the connection timeout value

You can specify the optional parameter connect_timeout to set the connection timeout value in seconds. The following code provides an example of how to initialize an oss2. Service object and set the connection timeout value to 30 seconds (similar to that for initializing oss2.Bucket):

```
# -*- coding: utf-8 -*-
import oss2
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
service = oss2. Service(auth, 'http://oss-cn-hangzhou.aliyuncs.com', connect_timeout=30)
```

2.4.2.2.4. Manage buckets

A bucket is a namespace in OSS and a management entity for advanced features such as billing, access control, and access logging.

View all buckets

Use oss2. BucketIterator to traverse all the buckets.

```
# -*- coding: utf-8 -*-

import oss2

auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
service = oss2. Service(auth, 'Your endpoint')

print([b.name for b in oss2. BucketIterator(service)])
```

Where, oss2. Service is used to access OSS-relevant classes. Currently, it is only used to list a user's buckets.

Create a bucket

To create a bucket in a specified region, specify an endpoint and a bucket name.

```
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
bucket.create_bucket()
```

For example, when you set the endpoint to `http://oss-cn-beijing.aliyuncs.com`, you can create a bucket in China (Beijing). For more information about endpoints, regions, and their mapping relationships as well as the bucket naming rules, see the introduction to basic OSS concepts.

You can specify the bucket ACL when creating a bucket. For example, you can use the following code to create a public-read bucket:

```
bucket.create_bucket(oss2. BUCKET_ACL_PUBLIC_READ)
```

Delete a bucket

The following code provides an example of how to delete an empty bucket:

```
try:
    bucket.delete_bucket()
except oss2.exceptions.BucketNotEmpty:
    print('bucket is not empty.')
except oss2.exceptions.NoSuchBucket:
    print('bucket does not exist')
```

If the bucket you want to delete is not empty (For example, it contains objects or data parts being uploaded.), you cannot delete the bucket and the SDK throws the BucketNotEmpty exception. If the bucket you want to delete does not exist, the SDK throws the NoSuchBucket exception.

Note

- Once a bucket is deleted, other users can apply for that bucket name.
- If a bucket is not empty, you can list and delete objects in the bucket (terminate multipart upload if there is any) to clear the bucket, and then delete the bucket.

View the ACL of a bucket

```
print(bucket.get_bucket_acl().acl)
```

Set the ACL for a bucket

The following code provides an example of how to set the ACL for a bucket to private:

```
bucket.put_bucket_acl(oss2. BUCKET_ACL_PRIVATE)
```

2.4.2.2.5. Upload objects

OSS provides multiple upload modes. The maximum size of data you can upload varies with different upload modes. In simple upload (PutObject) and append upload (AppendObject) modes, the maximum size of an object you can upload is 5 GB. In multipart upload mode, the maximum size of each part you can upload can reach 5 GB, and the maximum size of the combined object can reach 48.8 TB. The simple upload mode is described first. This section details the setting of data. The setting of data is similar in other upload modes, and therefore is not repeated.

Simple upload

You can use `Bucket.put_object` to upload a small object.

Upload a string

The following code provides an example of how to upload a string from the buffer:

```
# -*- coding: utf-8 -*-
import oss2
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
bucket.put_object('remote.txt', 'content of object')
```

You can specify bytes for the object you want to upload.

```
bucket.put_object('remote.txt', b'content of object')
```

Or you can specify Unicode for the object you want to upload.

```
bucket.put_object('remote.txt', u'content of object')
```

In fact, the second parameter (the name of which is data) of oss2.Bucket.put_object supports two types of strings:

- bytes: The string is directly uploaded.
- unicode: The string is uploaded after automatically converted into UTF-8 bytes.

Upload a local file

```
with open('local.txt', 'rb') as fileobj:
    bucket.put_object('remote.txt', fileobj)
```

Comparing with the code for uploading a string, you can find that the data parameter can be set to either a string or a file object.

> Note The file object must be opened in the binary mode because the number of bytes in the object must be available before the upload.

The Python SDK also provides the following method to easily upload a local file:

```
bucket.put_object_from_file('remote.txt', 'local.txt')
```

Upload a network stream

```
import requests
input = requests.get('http://www.aliyun.com')
bucket.put_object('aliyun.txt', input)
```

The requests.get request returns an iterable object. In this case, the Python SDK uploads the object through chunked encoding.

Return values

```
result = bucket.put_object('remote.txt', 'content of object')
print('http status: {0}'.format(result.status))
print('request_id: {0}'.format(result.request_id))
print('ETag: {0}'.format(result.etag))
print('date: {0}'.format(result.headers['date']))
```

Responses returned by each OSS server share the following attributes:

- status: the HTTP return code
- request_id: the request ID
- headers: the HTTP response header

ETag is a unique attribute returned by put_object.

> Note The request ID uniquely identifies a request. We recommend that you include it in program logs.

Summary

As you can see from the preceding examples, the Python SDK supports multiple types of input sources for upload modes, thanks to a third-party request library. In summary, the following types of input data (which can be specified by the data parameter) are supported:

- String of the bytes type
- String of the Unicode type: The string is uploaded after automatically converted into UTF-8 bytes.
- File object: The file object must be opened in the binary mode, such as the rb mode.
- Iterable object: The iterable object is uploaded through chunked encoding.

> **Note** If the seek and tell methods are applicable to a file object, the object is uploaded from the current position until the entire object is uploaded.

Resumable download

If the local file to be uploaded is large or network conditions are poor, the upload may be interrupted. In this case, if you re-upload the already uploaded data, it not only wastes time but also consumes network resources. The Python The Python SDK provides an easy-to-use `oss2.resumable_upload` API to resume the upload of a local file:

```
oss2.resumable_download(bucket, 'remote.txt', 'local.txt')
```

The principle is that when the file length is larger than or equal to the value specified by multipart_threshold (optional), multipart upload is enabled. In this case, a .py-oss-upload directory is created in the home directory. The current progress is stored in an object in the created directory. You can also use the optional store parameter to specify the directory that stores the progress.

The following code provides a fully custom example:

```
oss2.resumable_download(bucket, 'remote.txt', 'local.txt',
    store=oss2. ResumableStore(root='/tmp'),
    multipart_threshold=100*1024,
    part_size=100*1024,
    num_threads=4)
```

The parameters are described as follows:

- ResumableStore: stores progress information in the */tmp/.py-oss-upload* directory.
- multipart_threshold: the multipart upload method that can be used if the object length is not smaller than 100 KB.
- part_size: the size (100 KB) of each part. If the object is too large, the size of each part may be larger than 100 KB.
- num_threads: the number (4) of concurrent uploads.

Note

- Set oss2.defaults.connection_pool_size to a value greater than or equal to the number of threads.
- The Python version must be 2.1.0 and later.

Multipart upload

When multipart upload is used, you can perform more refined control over the upload task. Multipart upload is applicable for the scenarios where the file size is unknown and the concurrent upload and custom resumable upload are enabled. One multipart upload task can be performed in three steps:

- Initialize a task (Bucket.init_multipart_upload): Obtain an upload ID.
- Upload parts (Bucket.upload_part): You can upload multiple parts concurrently.
- Complete multipart upload (Bucket.complete_multipart_upload): Combine the uploaded parts to generate an OSS object.

The following code provides an example:

```
import os
from oss2 import SizedFileAdapter, determine_part_size
from oss2.models import PartInfo
key = 'remote.txt'
filename = 'local.txt'
total_size = os.path.getsize(filename)
part_size = determine_part_size(total_size, preferred_size=100 * 1024)
# Initialize parts.
upload_id = bucket.init_multipart_upload(key).upload_id
parts = []
# Upload parts sequentially.
with open(filename, 'rb') as fileobj:
    part_number = 1
    offset = 0
    while offset < total_size:
        num_to_upload = min(part_size, total_size - offset)
        result = bucket.upload_part(key, upload_id, part_number,
                                    SizedFileAdapter(fileobj, num_to_upload))
        parts.append(PartInfo(part_number, result.etag))
        offset += num_to_upload
        part_number += 1
# Complete multipart upload.
bucket.complete_multipart_upload(key, upload_id, parts)
# Verify the upload.
with open(filename, 'rb') as fileobj:
    assert bucket.get_object(key).read() == fileobj.read()
```

In the example:

- determine_part_size is a helper function that you can use to determine the part size.
- SizedFileAdapter(fileobj, size) can be used to generate a new file object with the same start offset as the original file, but only data of the specified size can be read.

> **Note** The object names (key) in the three steps must be the same. The same upload ID must be used in the steps of uploading parts and completing multipart upload.

Append upload

You can use Bucket.append_object to enable append upload.

```
result = bucket.append_object('append.txt', 0, 'content of first append')
bucket.append_object('append.txt', result.next_position, 'content of second append')
```

The offset (specified by the position parameter) of the first upload is set to 0. If the object already exists and

- If it is not appendable, OSS throws an ObjectNotAppendable exception.
- If it is appendable but the input offset does not match the current object size, OSS throws a PositionNotEqualToLength exception.

If it is not the first upload, you can use Bucket.head_object or the next_position attribute returned in the last append operation to obtain the offset parameter value.

Set the HTTP header

During upload, you can use headers to set the HTTP header supported by OSS, such as Content-Type.

```
bucket.put_object('a.json', '{"age": 1}', headers={'Content-Type': 'application/json; charset=utf-8'})
```

Set user-defined Object Meta

The following code provides an example of how to specify an HTTP header prefixed with x-oss-meta- to set the user-defined Object Meta of an object:

```
bucket.put_object('story.txt', 'a novel', headers={'x-oss-meta-author': 'O. Henry'})
```

Progress bar

The progress bar can be enabled using the optional parameter progress_callback of each upload API. The following code uses Bucket.put_object to enable the progress bar of a simple command line (open a Python source file):

```
# -*- coding: utf-8 -*-
from __future__ import print_function
import os, sys
import oss2
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
def percentage(consumed_bytes, total_bytes):
    if total_bytes:
        rate = int(100 * (float(consumed_bytes) / float(total_bytes)))
        print('\r{0}% '.format(rate), end='')
        sys.stdout.flush()
bucket.put_object('story.txt', 'a'*1024*1024, progress_callback=percentage)
```

Note

- If you cannot determine the size of the data you want to upload, the second parameter (total_bytes) of progress_callback is set to None.
- For the complete progress bar code, see GitHub.

2.4.2.2.6. Download objects

Overview

The Python SDK provides two basic download APIs:

- `Bucket.get_object` : Its response is a file-like object as well as an iterable object.
- `Bucket.get_object_to_file` : downloads an object to a local file.

The Python SDK also provides an easy-to-use API:

- `oss2.resumable_download` : helps with resumable download and concurrent downloads.

Streaming download

The following code provides an example of how to read all data of an OSS object simultaneously and display the data:

```
# -*- coding: utf-8 -*-
import oss2
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
remote_stream = bucket.get_object('remote.txt')
print(remote_stream.read())
```

You can use some library functions because the response is a file object. For example, you can download the object to a local file.

```
import shutil
remote_stream = bucket.get_object('remote.txt')
with open('local-backup.txt', 'wb') as local_fileobj:
    shutil.copyfileobj(remote_stream, local_fileobj)
```

The response is also an iterable object. Therefore, you can copy the content of the object to another object in the streaming mode.

```
remote_stream = bucket.get_object('remote.txt')
bucket.put_object('remote-backup.txt', remote_stream)
```

Download an object to a local file

The following code provides an example of how to download the remote.txt object from OSS to the local-backup.txt file in the current directory:

```
bucket.get_object_to_file('remote.txt', 'local-backup.txt')
```

Range download

You can set byte_range (optional) to specify the download range. byte_range is a tuple, which specifies the start and end bytes for the range download. The following code provides an example of how to download the data of first 100 bytes:

```
remote_stream = bucket.get_object('remote.txt', byte_range=(0, 99))
```

Note byte_range specifies the closed interval of the byte offset, which starts from 0. For example, (0, 99) indicates that the download range is from byte 0 to byte 99, covering 100 bytes in total.

Progress bar

Download APIs provide progress_callback (optional) to use progress bars and display progress information. The following code provides an example of how to enable progress bar display (by creating a Python source object):

```
# -*- coding: utf-8 -*-
from __future__ import print_function
import os, sys
import oss2
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
def percentage(consumed_bytes, total_bytes):
    if total_bytes:
        rate = int(100 * (float(consumed_bytes) / float(total_bytes)))
        print('\r{0}% '.format(rate), end='')
        sys.stdout.flush()
bucket.get_object_to_file('remote.txt', 'local-backup.txt', progress_callback=percentage)
```

Note

- If the HTTP response header does not contain the Content-Length header, total_bytes (the second parameter of progress_callback) is set to None.
- For the complete code of progress bars, see GitHub.

Resumable download

When the local object you want to download is large, or the network conditions are poor, the download may be interrupted. If you retry the download, it will waste time and bandwidths. To resolve this problem, the Python SDK provides an easy-to-use `oss2.resumable_download` for resumable download.

The following code provides an example of how to download the remote.txt object from OSS to the current local directory and rename it local.txt:

```
oss2.resumable_download(bucket, 'remote.txt', 'local.txt')
```

The resumable download process is as follows:

1. Create a local temporary file, the name of which consists of the original object name and a random suffix.
2. Read the OSS object based on the range you specified in the `Range` header in the HTTP request and write the read content to the corresponding position of the temporary file.
3. After the download is completed, rename the temporary file as the target file.

During the preceding process, the checkpoint information, that is, the range of downloaded data, is stored in the local disk. If the download is interrupted and is resumed later, the system reads the checkpoint information and downloads only the missing parts.

The following code provides an example of how to set resumable download:

```
oss2.resumable_download(bucket, 'remote.txt', 'local.txt',
 store=oss2. ResumableDownloadStore(root='/tmp'),
 multiget_threshold=20*1024*1024,
 part_size=10*1024*1024,
 num_threads=3)
```

The parameters are described as follows:

- ResumableDownloadStore stores the checkpoint information in the */tmp/.py-oss-download* directory.
- multiget_threshold specifies the minimum object size of 20 MB that applies to range download.
- part_size : We recommend that the data to be downloaded is 10 MB each time. If the object is too large, the actual size of data downloaded each time is greater than the specified value.
- num_threads: specifies the number of concurrent download threads of 3.

Note the following details when you use this function:

- Prevent multiple programs (threads) from concurrently calling this function for the same source object and target object. This is because one piece of checkpoint information overwrites another on the disk, or one temporary file name conflicts with another.
- Do not use the part whose size is too small. In other words, the part_size value must be greater than or equal to oss2.defaults.multiget_part_size.
- If the target file with the same name already exists, the file is replaced.

> **Note**
>
> - Set oss2.defaults.connection_pool_size to a value that is greater than or equal to the number of threads.
> - The Python version must be 2.1.0 and later.

2.4.2.2.7. Manage objects

You can use the Python SDK to list, delete, and copy objects, view object information, and modify Object Meta.

List objects

The Python SDK provides a series of iterators for you to list objects and perform multipart upload.

Simple list

The following code provides an example of how to list 10 objects in a bucket:

```
# -*- coding: utf-8 -*-
import oss2
from itertools import islice
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
for b in islice(oss2. ObjectIterator(bucket), 10):
    print(b.key)
```

List by prefix

The following code provides an example of how to list objects prefixed with img- only:

```
for obj in oss2. ObjectIterator(bucket, prefix='img-'):
    print(obj.key)
```

Simulate a folder

Buckets in OSS are flat-structured because OSS has no folders or directories. You can simulate a folder by adding a forward slash (/) to an object name. When listing objects, set the delimiter parameter (directory delimiter) to forward slash (/). OSS determines whether there is a folder by checking whether an object is a CommonPrefix.

The following code provides an example of how to list all content in the root directory:

```
for obj in oss2. ObjectIterator(bucket, delimiter='/'):
    if obj.is_prefix():  # directory
        print('directory: ' + obj.key)
    else:              # object
        Print ('file: '+ obj. Key)
```

Note Folder listing simulation is inefficient. We recommend that you do not use it.

Determine whether a specified object exists

You can use `object_exists` to determine whether an object exists. If the response is true, the object exists. If the object is false, the object does not exist.

```
exist = bucket.object_exists('remote.txt')
if exist:
    print('object exist')
else:
    print('object not eixst')
```

Delete objects

The following code provides an example of how to delete an object:

```
bucket.delete_object('remote.txt')
```

You can delete multiple objects (up to 1,000 objects). The following code provides an example of how to delete three objects and display the names of successfully-deleted objects:

```
result = bucket.batch_delete_objects(['a.txt', 'b.txt', 'c.txt'])
print('\n'.join(result.deleted_keys))
```

Copy objects

The following code provides an example of how to copy the content of the source.txt object in a bucket named src-bucket to the target.txt object in the current bucket:

```
bucket.copy_object('src-bucket', 'source.txt', 'target.txt')
```

Copy a large object

When an object to be copied is large, we recommend that you do not use multipart copy to avoid timeout. Similar to multipart upload, multipart copy is completed in three steps:

1. Initialize a task (Bucket.init_multipart_upload): Obtain an upload ID.
2. Copy parts (Bucket.upload_part_copy): Each part of the source object is copied as a part of the target object.
3. Complete multipart copy (Bucket.complete_multipart_copy): Multipart copy is completed and the target object is generated.

Example:

```
from oss2.models import PartInfo
from oss2 import determine_part_size
src_key = 'remote.txt'
dst_key = 'remote-dst.txt'
bucket.put_object(src_key, 'a' * (1024 * 1024 + 100))
total_size = bucket.head_object(src_key).content_length
part_size = determine_part_size(total_size, preferred_size=100 * 1024)
# Initialize parts.
upload_id = bucket.init_multipart_upload(dst_key).upload_id
parts = []
# Copy parts one by one.
part_number = 1
offset = 0
while offset < total_size:
    num_to_upload = min(part_size, total_size - offset)
    byte_range = (offset, offset + num_to_upload - 1)
    result = bucket.upload_part_copy(bucket.bucket_name, src_key, byte_range,
                                     dst_key, upload_id, part_number)
    parts.append(PartInfo(part_number, result.etag))
    offset += num_to_upload
    part_number += 1
# Complete multipart upload.
bucket.complete_multipart_upload(dst_key, upload_id, parts)
```

Modify Object Meta

The following code provides an example of how to modify User Meta:

```
bucket.update_object_meta('story.txt', {'x-oss-meta-author': 'O. Henry'})
bucket.update_object_meta('story.txt', {'x-oss-meta-price': '100 dollar'})
```

The previous value of the User Meta (the HTTP header prefixed with "x-oss-meta-") is overwritten each time the User Meta is called. In the preceding example, User Meta "x-oss-meta-author" is deleted during the second invocation.

Other information such as Content-Type can also be changed:

```
bucket.update_object_meta('story.txt', {'Content-Type': 'text/plain'})
```

Note that the Content-Type parameter and original User Meta are modified during this invocation.

View the ACL of an object

```
print(bucket.get_object_acl('story.txt').acl)
```

Note There are four permissions included in object ACLs: default, private, public-read, and public-read-write.

Set the ACL of an object

The following code provides an example of how to set a public-read ACL for an object:

```
bucket.put_object_acl('story.txt', oss2. OBJECT_ACL_PUBLIC_READ)
```

Note

There are four permissions included in object ACLs: default, private, public-read, and public-read-write. They correspond to the following parameters:

- oss2.OBJECT_ACL_DEFAULT
- oss2.OBJECT_ACL_PRIVATE
- oss2.OBJECT_ACL_PUBLIC_READ
- oss2.OBJECT_ACL_PUBLIC_READ_WRITE

2.4.2.2.8. Authorized access

Download by using a private link

You can generate a private link (also known as a URL with a signature) for access to a private bucket.

```
# -*- coding: utf-8 -*-
import oss2
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
print(bucket.sign_url('GET', 'object-in-bucket.txt', 60))
```

A private link is displayed if you use the preceding code. You can share the link with other users to download the object directly through a browser or using tools such as wget. The link is only valid within 60 seconds after generation.

Use STS for temporary access authorization

You can use STS for temporary access permissions.

To use STS, perform the following steps:

1. Create a RAM user in Apsara Stack Management Console.
2. Create an STS role in Apsara Stack Management Console and grant the RAM user the permission to play this role.
3. Use the AccessKey ID and AccessKey Secret of the RAM user to apply for a temporary token from STS.

4. Use the authentication information in the temporary token to create an `StsAuth` class instance.
5. Use the `StsAuth` class instance to initialize the `Bucket` class instance.

The following code provides an example of how to obtain a temporary token. First install the official Python STS client:

```
$ pip install aliyun-python-sdk-sts
```

Then, obtain temporary authorization through STS. You need to set end_point, bucket_name, access_key_id, access_key_secret, and role_arn in the preceding code to valid values based on the actual conditions. We assume that the role has the permission to upload files.

In the preceding parameters, role_arn is the role ID.

```
# -*- coding: utf-8 -*-
from aliyunsdkcore import client
from aliyunsdksts.request.v20150401 import AssumeRoleRequest
import json
import oss2
endpoint = 'oss-cn-hangzhou.aliyuncs.com'
bucket_name = '<The name of the bucket you want to access>'
access_key_id = '<The AccessKeyId of the RAM user>'
access_key_secret = '<The AccessKeySecret of the RAM user>'
role_arn = '<The role ID>'
clt = client.AcsClient(access_key_id, access_key_secret, 'cn-hangzhou')
req = AssumeRoleRequest.AssumeRoleRequest()
# For simplicity, parameters such as Duration and Policy are not set. For more information, see relevant
documents about RAM and STS.
req.set_accept_format('json') # Set the return value format to JSON.
req.set_RoleArn(role_arn)
req.set_RoleSessionName('session-name')
body = clt.do_action(req)
# No error check is performed for simplicity.
token = json.loads(body)
# Initialize the StsAuth instance.
auth = oss2. StsAuth(token['Credentials']['AccessKeyId'],
                token['Credentials']['AccessKeySecret'],
                token['Credentials']['SecurityToken'])
# Initialize the bucket instance.
bucket = oss2. Bucket(auth, endpoint, bucket_name)
# Upload a string.
bucket.put_object('object-name.txt', b'hello world')
```

Note

- If the temporary token expires, you need to obtain a new token and set the auth member variable in oss2.Bucket to a new StsAuth.
- The Python version must be 2.0.6 and later.
- For the complete STS use code, see GitHub.

2.4.2.2.9. Static website hosting

You can use the Python SDK to set your buckets to the static website hosting mode. After the setting, the OSS can be accessed as a static website, and the page can automatically jump to the index page or error page.

Set static website hosting

The following code provides an example of how to enable static website hosting, and set the index page to index.html and the error page (the 404 page) to error.html:

```
# -*- coding: utf-8 -*-


import oss2
from oss2.models import BucketWebsite


auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')


bucket.put_bucket_website(BucketWebsite('index.html', 'error.html'))
```

Obtain the static website hosting configuration

```
try:
    website = bucket.get_bucket_website()
    print('Index file is {0}, error file is {1}'.format(website.index_file, website.error_file))
except oss2.exceptions.NoSuchWebsite as e:
    print('Website is not configured, request_id={0}'.format(e.request_id))
```

Note that if static website hosting is disabled, the system throws a NoSuchWebsite exception when get_bucket_website is used.

Disable static website hosting

```
bucket.delete_bucket_website()
```

2.4.2.2.10. Manage lifecycle rules

Lifecycle rules

You can set lifecycle rules for your buckets to manage objects in the buckets. Currently, you can define rules to delete specific objects. Each rule is composed of the following parts:

- Rule ID: The ID identifies the rule and must be unique.
- Policy: The rule applies only to objects with a specified prefix.
- Expiration: It can be specified in either of the following ways:
  - Set by Number of Days: It specifies the number of days from the last modification time of objects.
  - Set by Date: It specifies the date prior to which objects are created. If objects are created prior to the date, these objects are deleted.
- Status: It specifies whether this lifecycle rule is enabled.

> **Note** User data may be deleted based on the lifecycle rules. Therefore, you must carefully read related documentation, and apply the lifecycle rules to running buckets only after the rules have been verified in testing buckets.

Set lifecycle rules

The following code provides an example of how to use `bucket.put_bucket_lifecycle` to set lifecycle rules:

```
# -*- coding: utf-8 -*-
import oss2
from oss2.models import LifecycleExpiration, LifecycleRule, BucketLifecycle,AbortMultipartUpload
import datetime
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
# Set the expiration duration to 3 days after last modified date.
rule1 = LifecycleRule('rule1', 'tests/',
                status=LifecycleRule.ENABLED,
                expiration=LifecycleExpiration(days=3))
# Set the expiration date to delete objects that are created before the date.
rule2 = LifecycleRule('rule2', 'logging-',
                status=LifecycleRule.DISABLED,
expiration=LifecycleExpiration(created_before_date=datetime.date(2018, 12, 12)))
# Set the expiration duration to 3 days for parts in an object.
rule3 = LifecycleRule('rule3', 'tests1/',
                status=LifecycleRule.ENABLED,
        abort_multipart_upload=AbortMultipartUpload(days=3))
# Set the expiration date to delete parts that are created before the date.
rule4 = LifecycleRule('rule4', 'logging1-',
                status=LifecycleRule.DISABLED,
                abort_multipart_upload = AbortMultipartUpload(created_before_date=datetime.date(2018, 1
2, 12)))
lifecycle = BucketLifecycle([rule1, rule2,rule3,rule4])
bucket.put_bucket_lifecycle(lifecycle)
```

Obtain lifecycle rules

The following code provides an example of how to use `bucket.get_bucket_lifecycle` to view lifecycle rules:

```
# -*- coding: utf-8 -*-
import oss2
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
lifecycle = bucket.get_bucket_lifecycle()
for rule in lifecycle.rules:
    if rule.abort_multipart_upload is None:
        print('id={0}, prefix={1}, status={2}, days={3}, created_before_date={4}'
              .format(rule.id, rule.prefix, rule.status,
                      rule.expiration.days,
                      rule.expiration.created_before_date))
    else:
        print('id={0}, prefix={1}, status={2}, days={3}, created_before_date={4}'
              .format(rule.id, rule.prefix, rule.status,
                      rule.abort_multipart_upload.days,
                      rule.abort_multipart_upload.created_before_date))
```

Delete lifecycle rules

The following code provides an example of how to use `bucket.delete_bucket_lifecycle` to clear lifecycle rules:

```
# -*- coding: utf-8 -*-
import oss2
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
bucket.delete_bucket_lifecycle()
# An exception is thrown if you try to obtain the lifecycle rules again.
try:
    lifecycle = bucket.get_bucket_lifecycle()
except oss2.exceptions.NoSuchLifecycle:
    print('lifecycle is not configured')
```

2.4.2.2.11. CORS

CORS allows Web applications to access resources that belong to another region. OSS provides APIs for developers to conveniently control CORS permissions.

Set CORS rules

The following code provides an example of how to set a CORS rule:

```
# -*- coding: utf-8 -*-
import oss2
from oss2.models import BucketCors, CorsRule
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
rule = CorsRule(allowed_origins=['*'],
                allowed_methods=['GET', 'HEAD'],
                allowed_headers=['*'],
                max_age_seconds=1000)
bucket.put_bucket_cors(BucketCors([rule]))
```

Obtain CORS rules

```
try:
   cors = bucket.get_bucket_cors()
except oss2.exceptions.NoSuchCors:
   print('cors is not set')
else:
   for rule in cors.rules:
      print('AllowedOrigins={0}'.format(rule.allowed_origins))
      print('AllowedMethods={0}'.format(rule.allowed_methods))
      print('AllowedHeaders={0}'.format(rule.allowed_headers))
      print('ExposeHeaders={0}'.format(rule.expose_headers))
      print('MaxAgeSeconds={0}'.format(rule.max_age_seconds))
```

Delete CORS rules

```
bucket.delete_bucket_cors()
```

2.4.2.2.12. Set access logging

Overview

You can set bucket access logging to store bucket access logs in a specified bucket for future analysis. Access logs exist as objects in a specified bucket. One text object is generated every hour. The object name format is as follows:

```
<TargetPrefix><SourceBucket>-YYYY-mm-DD-HH-MM-SS-UniqueString
```

You need to specify TargetPrefix.

The access logging configuration consists of the following parts:

- TargetBucket: the name of the target bucket. Log objects generated are stored in this bucket.

- TargetPrefix: the prefix of the log object name. It can be left unspecified.

Enable access logging

The following code provides an example of how to enable the logging feature, store logs in the current bucket, and prefix log objects with logging/:

```
# -*- coding: utf-8 -*-
import oss2
from oss2.models import BucketLogging
auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')
bucket.put_bucket_logging(BucketLogging(bucket.bucket_name, 'logging/'))
```

View access logging settings

```
logging = bucket.get_bucket_logging()
print('TargetBucket={0}, TargetPrefix={1}'.format(logging.target_bucket, logging.target_prefix))
```

Disable access logging

```
bucket.delete_bucket_logging()
```

2.4.2.2.13. Hotlinking

OSS is a Pay-As-You-Go service. To prevent user data in OSS from being leeched, OSS supports hotlinking based on the referer field in the HTTP header.

Configure hotlinking

```
# -*- coding: utf-8 -*-

import oss2
from oss2.models import BucketReferer

auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')

bucket.put_bucket_referer(BucketReferer(True, ['http://alibaba.com', 'http://*.aliyuncs.com']))
```

After the preceding code is successfully run, you can configure hotlinking as follows:

- The first parameter allow_empty_referer value True indicates that an empty refer is allowed. You can also set the value to False as required.
- The referer whitelist is . A wildcard (*) is supported, such as *http://*.aliyuncs.com*.

Obtain the hotlinking settings

```
config = bucket.get_bucket_referer()
print('allow empty referer={0}, referers={1}'.format(config.allow_empty_referer, config.referers))
```

Disable hotlinking

To disable hotlinking, you need to set the allow_empty_referer parameter to True and clear the referer whitelist.

```
bucket.put_bucket_referer(BucketReferer(True, []))
```

2.4.2.2.14. Handle errors

Overview

If an error occurs during the runtime of a program, the Python SDK throws an exception accordingly. There are three types of exceptions: ClientError, RequestError and ServerError. They are all subclasses of OssError, and are all defined in the oss2.exceptions submodule.

OssError has the following important member variables:

- status: int type. It is an HTTP status code for ServerError or a fixed value for the other two types of exceptions.
- request_id: str type. It is the request ID returned by the OSS server for ServerError or a null string for the other two types of exceptions.
- code and message: str type. They correspond to the text in the Code and Message XML tags in an OSS error response.

ClientError

ClientError is caused by input error on the client side. For example, ClientError is thrown when an empty object name list is received during Bucket.batch_delete_objects. The status value of ClientError objects is fixed to oss2.exceptions.OSS_CLIENT_ERROR_STATUS.

RequestError

When the underlying HTTP library throws an exception, the Python SDK converts it to RequestError. The status value of such exceptions is fixed to oss2.exceptions.OSS_REQUEST_ERROR_STATUS.

ServerError

When the OSS server returns an HTTP error code of 4xx or 5xx, the Python SDK converts the response of the OSS server to ServerError. To easily use the Python SDK, the following subclasses are derived from status and code:

Exception class	Corresponding HTTP status code	OSS error code	Remarks

Exception class	Corresponding HTTP status code	OSS error code	Remarks
NotModified	304	Null	The error message returned when no change occurs.
AccessDenied	403	AccessDenied	The error message returned when the access is denied.
NoSuchBucket	404	NoSuchBucket	The error message returned when no such bucket exists.
NoSuchKey	404	NoSuchKey	The error message returned when no such object name exists.
NoSuchUpload	404	NoSuchUpload	The error message returned when no such multipart upload exists.
NoSuchWebsite	404	NoSuchWebsiteConfiguration	The error message returned when no such static website hosting is configured.
NoSuchLifecycle	404	NoSuchLifecycle	The error message returned when no such lifecycle management is set.
NoSuchCors	404	NoSuchCORSConfiguration	The error message returned when no such CORS rule is set.
BucketNotEmpty	409	BucketNotEmpty	The error message returned when the bucket is not empty.
PositionNotEqualToLength	409	PositionNotEqualToLength	The error message returned when the appending position does not match the file length.
ObjectNotAppendable	409	ObjectNotAppendable	The error message returned when the object is not appendable.

All exceptions of the 404 status code are subclasses of NotFound. All exceptions of the 409 status code are subclasses of Conflict.

Note Not all OSS error codes have corresponding exceptions. Currently, only typical exceptions are defined.

Examples

The following code provides an example of how to handle the exception when the object name does not exist during the object download, and display the HTTP status code and the request ID:

```
# -*- coding: utf-8 -*-

import oss2

auth = oss2. Auth('Your AccessKey ID', 'Your AccessKey Secret')
bucket = oss2. Bucket(auth, 'Your endpoint', 'Your bucket name')

try:
    stream = bucket.get_object('random-key.txt')
except oss2.exceptions.NoSuchKey as e:
    print('status={0}, request_id={1}'.format(e.status, e.request_id))
```

2.4.2.2.15. Chinese character and time

Chinese character

The following table describes the terms that are involved in this topic.

Name	Description
str	The default string type used in Python. Python 2.x uses the bytes type and Python 3.x uses the Unicode type.
Bytes	Byte streams. The length is calculated based on the number of bytes. For example, the length of b'中文' is calculated based on the encoding mode. If UTF-8 is used, its length is 6.
Unicode	Unicode streams. The length is calculated based on the number of Chinese characters. For example, the length of u'中文' is 2.

Input and output restrictions

The following table describes the restrictions on input parameter types for the Python SDK.

Input parameter	Suggested type	Remarks
OSS object name	str	If the data type is bytes, UTF-8 is required for encoding.
Local file name	String and Unicode	If the data type is bytes, UTF-8 is required for encoding.
Input data stream	Bytes	Example: data in Bucket.put_object.

The "Local file name" indicates the local file name parameter in Bucket.get_object_to_file (example).

The following table describes the output restrictions.

Output	Type
The result obtained by parsing the XML document	str
Downloaded content	Bytes

The result obtained by parsing the XML document indicates the strings in the results obtained from APIs such as Bucket.list_objects and Bucket.get_bucket_lifecycle.

Ensure that the source Python file is encoded with UTF-8 because data of the bytes type is encoded with UTF-8 in OSS Python SDK by default.

Help functions

The OSS Python SDK provides three types of functions for data type conversion.

Function	Description
to_bytes	Converts Unicode data into bytes data encoded with UTF-8. Data of other types is returned without conversion.
to_unicode	Converts bytes data encoded with UTF-8 into Unicode data. Data of other types is returned without conversion.
to_string	In the Python 2 series, Unicode is converted to string. For data of other types, the original data type is returned. In the Python 3 series, bytes is converted to string. For data of other types, the original data type is returned.

Time

Python SDK converts the timestamp string (datetime.datetime) obtained from the server to Unix time. In other words, the timestamp string is converted to seconds since January 1, 1970 UTC. For example, the value of last_modified returned from bucket.get_object is the Unix Time of integer type. For example, the last_modified time in the response for Bucket.get_object is the Unix Time of the integer type.

You can use `datetime.datetime.fromtimestamp()` to convert time and obtain timestamp strings.

2.4.2.2.16. IMG

OSS Image Processing (IMG) is a secure, cost-friendly, and highly reliable image processing service that processes large amounts of data. You can upload original images to OSS. Through simple `RESTful` APIs, you can use any Internet devices to process images anytime anywhere. IMG provides image processing APIs. To upload images, use the OSS upload API. You can create your own image processing service based on OSS IMG.

Basic features

OSS provides the following IMG features:

- Obtain image information
- Convert image formats
- Resize, crop, and rotate images
- Apply image effects
- Add image, text, and text-and-image watermarks to images
- Customize imaging processing styles. Log on to the OSS console, click a bucket name to go to the Bucket Information tab page. Choose **Image Processing** > **Create Style** to customize an image processing style.
- Call multiple IMG features through cascading processing

IMG use

IMG enables you to use the `HTTP GET` request for access. All IMG parameters are included in the QueryString of `URL` .

- Anonymous access

  If the access permission of an image object is `publc-read` , as shown in the following table, anonymous users can access the image object.

Bucket permission	Object permission
public-read or public-read-write	default
Any permission	public-read or public-read-write

  You can access IMG anonymously using a third-level domain name in the following format:

```
http://bucket.<endpoint>/object?x-oss-process=image/action,parame_value
```

  - bucket: the name of the user's bucket
  - endpoint: the domain name for accessing the region to which the user's bucket belongs
  - object: the image object uploaded to OSS by the user
  - image: the identifier reserved by IMG
  - action: the operation performed by the user on the image, such as resizing, cropping, or rotating
  - parame: the parameter corresponding to the operation performed by the user on the image

  Example:

```
http://image-demo.oss-cn-hangzhou.aliyuncs.com/example.jpg?x-oss-process=image/resize,w_100
```

  For a custom style, you can access IMG anonymously using a third-level domain name in the following format:

```
http://bucket.<endpoint>/object?x-oss-process=x-oss-process=style/name
```

  - style: the identifier reserved by the system for the user's custom style

- name: the name of a custom style that is defined in Rule Name in the OSS console

Example:

```
http://image-demo.oss-cn-hangzhou.aliyuncs.com/example.jpg?x-oss-process=style/oss-pic-style-w-100
```

Through cascading processing, you can perform multiple operations in sequence on an image using a URL in the following format:

```
http://bucket.<endpoint>/object?x-oss-process=image/action,parame_value/action,parame_value/...
```

Example:

```
http://image-demo.oss-cn-hangzhou.aliyuncs.com/example.jpg?x-oss-process=image/resize,w_100/rotate,90
```

IMG also supports HTTPS access. The following code provides an example:

```
https://image-demo.oss-cn-hangzhou.aliyuncs.com/example.jpg?x-oss-process=image/resize,w_100
```

- Authorized access

If the access permission for an image object is private, as shown in the following table, you must be authorized to access IMG.

Bucket permission	Object permission
private	default
Any permission	private

The following code provides an example of how to add a signature to a URL to access IMG:

```
# -*- coding: utf-8 -*-
import oss2
endpoint = '<endpoint, such as http://oss-cn-hangzhou.aliyuncs.com>'
access_key_id = '<access_key_id>'
access_key_secret = '<access_key_secret>'
bucket_name = '<bucket_name>'
key = 'example.jpg'
# Create a bucket. All object-related APIs can be called based on the bucket.
bucket = oss2. Bucket(oss2. Auth(access_key_id, access_key_secret), endpoint, bucket_name)
# Upload a sample image.
bucket.put_object_from_file(key, 'example.jpg')
# Generate a signature for a URL. Set the validity period to 10 minutes.
style = 'image/resize,m_fixed,w_100,h_100/rotate,90'
url = bucket.sign_url('GET', key, 10 * 60, params={'x-oss-process': style})
print(url)
```

> Note
>
> - You can set Create Style, HTTPS, and Cascading Processing for authorized access.
> - The expiration time of sign_url is in seconds.

- Access with the SDK

  You can directly use the `SDK` to access and process image objects with any ACLs.

  > Note
  >
  > - For the complete IMG code, see GitHub.
  > - You can use the SDK to operate image objects by setting Create Style, HTTPS, and Cascading Processing.

  - Basic operations

    Basic IMG operations include obtaining image information, converting image formats, resizing, cropping, rotating, applying effects, and adding watermarks.

```
# -*- coding: utf-8 -*-
import os
import oss2
endpoint = '<endpoint, such as http://oss-cn-hangzhou.aliyuncs.com>'
access_key_id = '<access_key_id>'
access_key_secret = '<access_key_secret>'
bucket_name = '<bucket_name>'
key = 'example.jpg'
new_pic = 'example-new.jpg'
# Create a bucket. All object-related APIs can be called based on the bucket.
bucket = oss2. Bucket(oss2. Auth(access_key_id, access_key_secret), endpoint, bucket_name)
# Upload a sample image.
bucket.put_object_from_file(key, 'example.jpg')
# Resize the image.
style = 'image/resize,m_fixed,w_100,h_100'
bucket.get_object_to_file(key, new_pic, process=style)
# Crop the image.
style = 'image/crop,w_100,h_100,x_100,y_100,r_1'
bucket.get_object_to_file(key, new_pic, process=style)
# Rotate the image.
style = 'image/rotate,90'
bucket.get_object_to_file(key, new_pic, process=style)
# Sharpen the image.
style = 'image/sharpen,100'
bucket.get_object_to_file(key, new_pic, process=style)
# Add a text watermark.
style = 'image/watermark,text_SGVsbG8g5Zu-54mH5pyN5YqhIQ'
bucket.get_object_to_file(key, new_pic, process=style)
# Convert the image format.
style = 'image/format,png'
bucket.get_object_to_file(key, new_pic, process=style)
# Delete the sample image.
bucket.delete_object(key)
# Delete the local file.
os.remove(new_pic)
```

Note `get_object` also supports the IMG feature.

- Custom styles

```
# -*- coding: utf-8 -*-
import os
import oss2
endpoint = '<endpoint, such as http://oss-cn-hangzhou.aliyuncs.com>'
access_key_id = '<access_key_id>'
access_key_secret = '<access_key_secret>'
bucket_name = '<bucket_name>'
key = 'example.jpg'
new_pic = 'example-new.jpg'
# Create a bucket. All object-related APIs can be called based on the bucket.
bucket = oss2. Bucket(oss2. Auth(access_key_id, access_key_secret), endpoint, bucket_name)
# Upload a sample image.
bucket.put_object_from_file(key, 'example.jpg')
# Customize a style.
style = 'style/oss-pic-style-w-100'
# Process the image.
bucket.get_object_to_file(key, new_pic, process=style)
# Delete the sample image.
bucket.delete_object(key)
# Delete the local file.
os.remove(new_pic)
```

> **Note** `get_object` also supports the IMG feature.

- Cascading processing

```
# -*- coding: utf-8 -*-
import os
import oss2
endpoint = '<endpoint, such as http://oss-cn-hangzhou.aliyuncs.com>'
access_key_id = '<access_key_id>'
access_key_secret = '<access_key_secret>'
bucket_name = '<bucket_name>'
key = 'example.jpg'
new_pic = 'example-new.jpg'
# Create a bucket. All object-related APIs can be called based on the bucket.
bucket = oss2. Bucket(oss2. Auth(access_key_id, access_key_secret), endpoint, bucket_name)
# Upload a sample image.
bucket.put_object_from_file(key, 'example.jpg')
# Perform cascading processing.
style = 'image/resize,m_fixed,w_100,h_100/rotate,90'
# Process the image.
bucket.get_object_to_file(key, new_pic, process=style)
# Delete the sample image.
bucket.delete_object(key)
# Delete the local file.
os.remove(new_pic)
```

Note `get_object` also supports the IMG feature.

2.4.2.3. PHP-SDK

2.4.2.3.1. Installation

SDK

- GitHub: https://github.com/aliyun/aliyun-oss-php-sdk
- Version iterations: https://github.com/aliyun/aliyun-oss-php-sdk/releases

Environment requirements

- PHP 5.3+ (Run the `php -v` command to view the current PHP version.)
- cURL extension (Run the `php -m` command to check whether cURL extension has been installed).

Note

- In Ubuntu, you can use the apt-get package manager to install the PHP cURL extension `sudo apt-get install php-curl` .
- In CentOS, you can use the yum package manager to install the PHP cURL extension `sudo yum install php-curl` .
- The PHP SDK does not support PHP 7 currently.

Installation

Composer

If you use Composer to manage project dependencies, run the following command in the root directory of your project:

```
composer require aliyuncs/oss-sdk-php
```

Alternatively, in `composer.json` , declare the dependency on Alibaba Cloud OSS SDK for PHP:

```
"require": {
   "aliyuncs/oss-sdk-php": "~2.0"
}
```

Run `composer install` to install the dependency. After the dependency is installed, check whether your directory structure is similar to the following structure:

```
├── app.php
├── composer.json
├── composer.lock
└── vendor
```

The `app.php` is a user application. The *vendor/*directory contains the dependent library. You need to introduce the dependency in `app.php` :

```
require_once __DIR__ . '/vendor/autoload.php';
```

Note

- If your project references `autoload.php` , you do not need to introduce `autoload.php` again after adding the SDK dependency.
- If a network error occurs when you use Composer, run the following command to use the image source of Composer China: `composer config -g repositories.packagist composer http://packagist.phpcomposer.com.`

Phar

When installing the SDK through Phar, select the required version on the Release page, download the Phar package, and introduce the following file into your code.

```
require_once '/path/to/oss-sdk-php.phar';
```

Source code

When installing the SDK through source code, select the required version on the Release page, download the ZIP package, find the `autoload.php` file in the root directory of the decompressed package, and introduce the file into your code:

```
require_once '/path/to/oss-sdk/autoload.php';
```

Sample program

To run the sample program, perform the following steps:

- Decompress the downloaded SDK package.
- Modify the Config.php file in the samples directory:
  - Set OSS_ACCESS_ID to the AccessKey ID that you obtain from OSS.
  - Set OSS_ACCESS_KEYto the AccessKey Secret that you obtain from OSS.
  - Set OSS_ENDPOINT to the endpoint that you select for accessing OSS, for example, `http://oss-cn-hangzhou.aliyuncs.com.`
  - Set OSS_TEST_BUCKET to the bucket to be used to run samples. The sample program creates objects in this bucket. Do not use a bucket in the production environment to avoid contaminating user data.
- Run `php RunAll.php` in the samples directory. You can also run a single sample file.

The following table describes the sample files in the sample program.

Sample file	Content
Object.php	Shows object operations, including how to upload, download, copy, delete, and list objects as well as set Object Meta.
MultipartUpload.php	Shows how to upload large objects and perform multipart upload.
Signature.php	Shows how to perform authorized access with a signed URL.
Callback.php	Shows how to perform upload callback.
Image.php	Shows how to use image processing.
LiveChannel.php	Shows how to use LiveChannel.
Bucket.php	Shows how to manage buckets, including creating, deleting, and listing buckets as well as setting bucket ACLs.

Sample file	Content
BucketLifecycle.php	Shows how to set, read, and delete the lifecycle configuration of a bucket.
BucketLogging.php	Shows how to set, read, and delete the logging configuration of a bucket.
BucketReferer.php	Shows how to set, read, and delete the hotlinking configuration of a bucket.
BucketWebsite.php	Shows how to set, read, and delete the static website hosting configuration of a bucket.
BucketCors.php	Shows how to set, read, and delete the CORS configuration of a bucket.

Earlier version

Compared with 1. *. *, this version is a major version upgrade. The APIs are no longer compatible. We recommend that you use the SDK of the latest version.

2.4.2.3.2. Initialization

The OSS\OssClient is a client class of the SDK, which provides a series of APIs for you to manage buckets and objects.

Set an AccessKey

To access Apsara Stack OSS, you need a pair of valid access keys (AccessKey ID and AccessKey Secret) for signature authentication.

After obtaining the AccessKey ID and AccessKey Secret, follow the steps for initialization.

Create an OssClient instance

Create an OssClient instance based on the OSS endpoint.

```
<? php
use OSS\OssClient;
use OSS\Core\OssException;
$accessKeyId = "<Your AccessKey ID obtained from OSS>";
$accessKeySecret = "<Your AccessKey Secret obtained from OSS>";
$endpoint = "<endpoint that you select for accessing OSS, such as http://oss-cn-hangzhou.aliyuncs.com
>";
try {
    $ossClient = new OssClient($accessKeyId, $accessKeySecret, $endpoint);
} catch (OssException $e) {
    print $e->getMessage();
}
```

Set network parameters

We can use ClientConfiguration to set some network parameters:

```
<? php
$ossClient->setTimeout(3600 /* seconds */);
$ossClient->setConnectTimeout(10 /* seconds */);
```

In the code,

- `setTimeout` specifies the request timeout value in seconds, which is 5,184,000 seconds by default. We recommend that you do not use an excessively small value, because it takes a long time to upload a large file.
- `setConnectTimeout` specifies the connection timeout value in seconds. The default value is 10 seconds.

2.4.2.3.3. Quick start

Ensure that you are familiar with OSS basic concepts, such as bucket, object, endpoint, AccessKey ID, and AccessKey Secret. This topic describes how to quickly use the OSS PHP SDK to complete routine operations, such as create buckets, upload objects, and download objects.

Typical classes

Class name	Description
OSS\OssClient	The OSS client class. You can call APIs through an OssClient instance.
OSS\Core\OssException	The OSS exception class. You need only to pay attention to OSS exceptions when using OSS.

Basic operations

Create a bucket

The following code provides an example of how to create a bucket:

```
<? php
$accessKeyId = "<Your AccessKey ID obtained from OSS>";
$accessKeySecret = "<Your AccessKey Secret obtained from OSS>";
$endpoint = "<endpoint that you select for accessing OSS, such as http://oss-cn-hangzhou.aliyuncs.com
>";
$bucket= " <Your bucket name that follows the naming rule>";
try {
    $ossClient = new OssClient($accessKeyId, $accessKeySecret, $endpoint);
    $ossClient->createBucket($bucket);
} catch (OssException $e) {
    print $e->getMessage();
}
```

Upload objects

Objects are the most basic data units in OSS and can be simply considered as files. The following code provides an example of how to upload an object:

```
<? php
$accessKeyId = "<Your AccessKey ID obtained from OSS>";
$accessKeySecret = "<Your AccessKey Secret obtained from OSS>";
$endpoint = "<endpoint that you select for accessing OSS, such as http://oss-cn-hangzhou.aliyuncs.com
>";
$bucket= " <Your bucket name that follows the naming rule>";
$object = " <Your object name that follows the naming rule>";
$content = "Hi, OSS.";
try {
    $ossClient = new OssClient($accessKeyId, $accessKeySecret, $endpoint);
    $ossClient->putObject($bucket, $object, $content);
} catch (OssException $e) {
    print $e->getMessage();
}
```

Download objects

You can read an object that has been downloaded. The following code provides an example of how to obtain an object:

```
<? php
$accessKeyId = "<Your AccessKey ID obtained from OSS>";
$accessKeySecret = "<Your AccessKey Secret obtained from OSS>";
$endpoint = "<endpoint that you select for accessing OSS, such as http://oss-cn-hangzhou.aliyuncs.com
>";
$bucket= " <Your bucket name that follows the naming rule>";
$object = " <Your object name that follows the naming rule>";
try {
    $ossClient = new OssClient($accessKeyId, $accessKeySecret, $endpoint);
    $content = $ossClient->getObject($bucket, $object);
    print("object content: " . $content);
} catch (OssException $e) {
    print $e->getMessage();
}
```

List objects

After objects are uploaded, you may want to view the objects contained in the bucket. The following code provides an example of how to list objects in the bucket:

```
<? php
$accessKeyId = "<Your AccessKey ID obtained from OSS>";
$accessKeySecret = "<Your AccessKey Secret obtained from OSS>";
$endpoint = "<endpoint that you select for accessing OSS, such as http://oss-cn-hangzhou.aliyuncs.com
>";
$bucket= " <Your bucket name that follows the naming rule>";
try {
    $ossClient = new OssClient($accessKeyId, $accessKeySecret, $endpoint);
    $listObjectInfo = $ossClient->listObjects($bucket);
    $objectList = $listObjectInfo->getObjectList();
    if (! empty($objectList)) {
        foreach ($objectList as $objectInfo) {
        print($objectInfo->getKey() . "\t" . $objectInfo->getSize() . "\t" . $objectInfo->getLastModified() . "\
n");
        }
    }
} catch (OssException $e) {
    print $e->getMessage();
}
```

> Note
>
> - You can use the preceding code to list 100 objects by default.

Delete an object

The following code provides an example of how to delete a specified object in a specified bucket:

```
<? php
$accessKeyId = "<Your AccessKey ID obtained from OSS>";
$accessKeySecret = "<Your AccessKey Secret obtained from OSS>";
$endpoint = "<endpoint that you select for accessing OSS, such as http://oss-cn-hangzhou.aliyuncs.com
>";
$bucket= " <Your bucket name that follows the naming rule>";
$object = " <Your object name that follows the naming rule>";
try {
   $ossClient = new OssClient($accessKeyId, $accessKeySecret, $endpoint);
   $ossClient->deleteObject($bucket, $object);
} catch (OssException $e) {
   print $e->getMessage();
}
```

Handle responses

The OssClient provides the following two types of data returned from APIs:

- Put and Delete: Operations succeed if null is returned through APIs without OSSException.
- Get and List: Operations succeed if the requested data is returned through APIs without OSSException.

Example:

```
<? php
$bucketListInfo = $ossClient->listBuckets();
$bucketList = $bucketListInfo->getBucketList();
foreach($bucketList as $bucket) {
   print($bucket->getLocation() . "\t" . $bucket->getName() . "\t" . $bucket->getCreatedate() . "\n");
}
```

In the preceding code, `$bucketListInfo` belongs to OSS\Model\BucketListInfo.

2.4.2.3.4. Manage buckets

A bucket is a storage space in OSS and a management entity for advanced features such as billing, access control, and access logging.

> Note For the complete code, see GitHub.

Create a bucket

The following code provides an example of how to use `OssClient::createBucket` to create a bucket:

```
<? php
/**
 * Create a bucket.
 * The ACL specifies the access permission on the bucket, which may be private, public-read, or public-re
ad-write.
 * The private permission indicates that only the bucket owner or the authorized user has the permissio
n to read and write the bucket.
 * The three permissions respectively correspond to "OSSClient::OSS_ACL_TYPE_PRIVATE",
 *            OssClient::OSS_ACL_TYPE_PUBLIC_READ,
 *            OssClient::OSS_ACL_TYPE_PUBLIC_READ_WRITE
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Name of the bucket to be created
 * @return null
 */
function createBucket($ossClient, $bucket)
{
    try {
        $ossClient->createBucket($bucket, OssClient::OSS_ACL_TYPE_PRIVATE);
    } catch (OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

> **Note**
>
> - The bucket name must be globally unique.

Determine whether a bucket exists

The following code provides an example of how to use `OssClient::doesBucketExist` to determine whether a bucket exists:

```
/**
 * Determine whether a bucket exists.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 */
function doesBucketExist($ossClient, $bucket)
{
    try {
        $res = $ossClient->doesBucketExist($bucket);
    } catch (OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    if ($res === true) {
        print(__FUNCTION__ . ": OK" . "\n");
    } else {
        print(__FUNCTION__ . ": FAILED" . "\n");
    }
}
```

List all of your buckets

The following code provides an example of how to use `OssClient::listBuckets` to list all of your buckets:

```
<? php
/**
 * List all of your buckets.
 *
 * @param OssClient $ossClient OssClient instance
 * @return null
 */
function listBuckets($ossClient)
{
    $bucketList = null;
    try{
        $bucketListInfo = $ossClient->listBuckets();
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    $bucketList = $bucketListInfo->getBucketList();
    foreach($bucketList as $bucket) {
        print($bucket->getLocation() . "\t" . $bucket->getName() . "\t" . $bucket->getCreatedate() . "\n");
    }
}
```

Delete a bucket

The following code provides an example of how to use `OssClient::deleteBucket` to delete a bucket:

```
<? php
/**
 * Delete a bucket.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Name of the bucket to be deleted
 * @return null
 */
function deleteBucket($ossClient, $bucket)
{
    try{
        $ossClient->deleteBucket($bucket);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note

- You cannot delete a non-empty bucket (which contains objects or parts from multipart upload).
- To delete a non-empty bucket, you must first delete all objects and parts from it.

Set the ACL for a bucket

You can not only configure the bucket ACL when creating a bucket, but also modify the bucket ACL based on your business requirements. Only the creator of the bucket has permission to perform this operation.

Currently, three access permissions included in the ACL are available for a bucket:

ACL	Corresponding value in the PHP SDK
private	OssClient::OSS_ACL_TYPE_PRIVATE
public-read	OssClient::OSS_ACL_TYPE_PUBLIC_READ
public-read-write	OssClient::OSS_ACL_TYPE_PUBLIC_READ_WRITE

The following code provides an example of how to use `OssClient::putBucketAcl` to set the bucket ACL:

```
<? php
/**
 * Configure the ACL of a bucket.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function putBucketAcl($ossClient, $bucket)
{
    $acl = OssClient::OSS_ACL_TYPE_PRIVATE;
    try {
        $ossClient->putBucketAcl($bucket, $acl);
    } catch (OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Obtain the ACL of a bucket

The following code provides an example of how to use `OssClient::getBucketAcl` to obtain the bucket ACL:

```
<? php
/**
 * Obtain the ACL of a bucket.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function getBucketAcl($ossClient, $bucket)
{
    try {
        $res = $ossClient->getBucketAcl($bucket);
    } catch (OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
    print('acl: ' . $res);
}
```

2.4.2.3.5. Upload objects

In OSS, objects are the basic data units for user operations. The OSS PHP SDK provides a variety of object upload APIs. You can upload an object through any of the following methods:

- Upload a string
- Object upload
- Append upload
- Multipart upload

The size of objects for string upload, object upload, and append upload operations must not exceed 5 GB. If the object size is large, use the multipart upload method. The total size of parts for multipart upload cannot exceed 48.8 TB.

Upload a string

The following code provides an example of how to upload a specified string to an object:

```
<? php
/**
 * Upload a string as the object content.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function putObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    $content = file_get_contents(__FILE__);
    try{
        $ossClient->putObject($bucket, $object, $content);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Upload a local file

The following code provides an example of how to upload a specified local file to an object:

```
<? php
/**
 * Upload the content of a specified local file.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function uploadFile($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    $filePath = __FILE__;
    try{
        $ossClient->uploadFile($bucket, $object, $filePath);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note When you upload an object by using the preceding method, ensure that the object size does not exceed 5 GB. If the object exceeds 5 GB, use multipart upload.

Append upload

Through simple upload, multipart upload, and resumable upload, normal objects are created with fixed content. They are read-only and cannot be modified. If you want to change the object content, you must upload an object of the same name to overwrite the existing one. This is a major difference between OSS and typical file systems. This feature is inconvenient in many scenarios, such as video surveillance and live video broadcast, because video data is constantly produced in real time.

OSS allows you to use Append Object to append content directly to the end of an object. This method applies to appendable objects. The objects uploaded with other methods are normal objects. The appended data is instantly readable.

Append a string

The following code provides an example of how to append a specified string to an object:

```
<? php
/**
 * Append a string.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function putObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/append-test-object-name.txt";
    $content_array = array('Hello OSS', 'Hi OSS', 'OSS OK');
    try{
        $position = $this->ossClient->appendObject($this->bucket, $object, $content_array[0], 0);
        $position = $this->ossClient->appendObject($this->bucket, $object, $content_array[1], $position);
        $position = $this->ossClient->appendObject($this->bucket, $object, $content_array[2], $position);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Append an object

The following code provides an example of how to append a local file to an OSS object:

```
/**
* Append an object.
*
* @param OssClient $ossClient OssClient instance
* @param string $bucket Bucket name
* @return null
*/
function putObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/append-test-object-name.txt";
    try{
        $position = $this->ossClient->appendFile($this->bucket, $object, __FILE__, 0);
        $position = $this->ossClient->appendFile($this->bucket, $object, __FILE__, $position);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

> **Note**
>
> - There is no limit to the number of append uploads. The maximum object size is 5 GB. Use multipart upload to upload larger objects.
> - You cannot use copyObject for appendable objects.

Multipart upload

Aside from the PutObject API, OSS also provides multipart upload to upload objects. You can use multipart upload in many scenarios, including but not limited to:

- Resumable upload is required.
- The object you want to upload is larger than 100 MB.
- The OSS server is frequently disconnected due to poor network conditions.
- The size of the object to be uploaded is unknown.

> **Note** For the complete multipart upload code, see GitHub.

Upload a local file in multipart upload mode

The following code provides an example of how to use an encapsulated easy-to-use API to upload an object through multipart upload:

```
<? php
/**
 * Upload an object through multipart upload.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function multiuploadFile($ossClient, $bucket)
{
    $object = "test/multipart-test.txt";
    $file = __FILE__;
    try{
        $ossClient->multiuploadFile($bucket, $object, $file);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Upload a local directory in multipart upload mode

The following code provides an example of how to use an encapsulated easy-to-use API to upload a directory through multipart upload:

```
<? php
/**
 * Upload objects by directory.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 *
 */
function uploadDir($ossClient, $bucket) {
    $localDirectory = ".";
    $prefix = "samples/codes";
    try {
        $ossClient->uploadDir($bucket, $prefix, $localDirectory);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    printf(__FUNCTION__ . ": completeMultipartUpload OK\n");
}
```

Multipart upload through original APIs

The typical multipart upload process is as follows:

- Initialize a MultipartUpload task (InitiateMultipartUpload).
- Upload the parts sequentially or concurrently (UploadPart).
- Complete the multipart upload (CompleteMultipartUpload) or abort the multipart upload (AbortMultipartUpload).

The following code provides an example of how to complete a MultipartUpload task sequentially through original APIs. The following code provides an example of how to perform resumable upload or other advanced operations:

```
<? php
/**
 * Use basic APIs to perform multipart upload sequentially.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @throws OssException
 */
function putObjectByRawApis($ossClient, $bucket)
{
    $object = "test/multipart-test.txt";
```

```
/**
 * Step 1: Initialize a MultipartUpload task. In other words, initialize multiple parts to be uploaded and obtain an upload ID.
 */
try{
    $uploadId = $ossClient->initiateMultipartUpload($bucket, $object);
} catch(OssException $e) {
    print(__FUNCTION__ . ": initiateMultipartUpload OK" . "\n");
    printf($e->getMessage() . "\n");
    return;
}
print(__FUNCTION__ . ": initiateMultipartUpload OK" . "\n");
/*
 * Step 2: Upload parts.
 */
$partSize = 10 * 1024 * 1024;
$uploadFile = __FILE__;
$uploadFileSize = filesize($uploadFile);
$pieces = $ossClient->generateMultiuploadParts($uploadFileSize, $partSize);
$responseUploadPart = array();
$uploadPosition = 0;
$isCheckMd5 = true;
foreach ($pieces as $i => $piece) {
    $fromPos = $uploadPosition + (integer)$piece[$ossClient::OSS_SEEK_TO];
    $toPos = (integer)$piece[$ossClient::OSS_LENGTH] + $fromPos - 1;
    $upOptions = array(
        $ossClient::OSS_FILE_UPLOAD => $uploadFile,
        $ossClient::OSS_PART_NUM => ($i + 1),
        $ossClient::OSS_SEEK_TO => $fromPos,
        $ossClient::OSS_LENGTH => $toPos - $fromPos + 1,
        $ossClient::OSS_CHECK_MD5 => $isCheckMd5,
    );
    if ($isCheckMd5) {
        $contentMd5 = OssUtil::getMd5SumForFile($uploadFile, $fromPos, $toPos);
        $upOptions[$ossClient::OSS_CONTENT_MD5] = $contentMd5;
    }
    //2. Upload each part to OSS.
    try {
        $responseUploadPart[] = $ossClient->uploadPart($bucket, $object, $uploadId, $upOptions);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": initiateMultipartUpload, uploadPart - part#{$i} FAILED\n");
```

```
            printf($e->getMessage() . "\n");
            return;
        }
        printf(__FUNCTION__ . ": initiateMultipartUpload, uploadPart - part#{$i} OK\n");
    }
    $uploadParts = array();
    foreach ($responseUploadPart as $i => $eTag) {
        $uploadParts[] = array(
            'PartNumber' => ($i + 1),
            'ETag' => $eTag,
        );
    }
    /**
     * step 3. Complete the upload.
     */
    try {
        $ossClient->completeMultipartUpload($bucket, $object, $uploadId, $uploadParts);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": completeMultipartUpload OK\n");
        printf($e->getMessage() . "\n");
        return;
    }
    printf(__FUNCTION__ . ": completeMultipartUpload OK\n");
}
```

Note

- The preceding process consists of three steps: 1. Initialize a task; 2. Upload parts; 3. Complete the upload.
- When you use the UploadPart method to upload each part (in step 2), note that:
- Each part, except the last one, must be larger than or equal to 100 KB. However, the UploadPart API does not immediately verify the size of the uploaded part (because it cannot immediately determine which part is the last one). It verifies the size of the uploaded part only when multipart upload is completed.
- OSS returns the MD5 value of the data part received by the server through the UploadPart API of the OssClient instance.
- The part number ranges from 1 to 10,000. If a part number is beyond this range, OSS returns the InvalidArgument error code.
- When each part is uploaded, the stream is directed to the starting position of the uploaded part.
- After each part is uploaded, OSS returns a PartETag object in the response, which is a combination of the ETag value and part number of the uploaded part. You need to keep the PartETag because it will be used to complete the multipart upload (in step 3). For more information about operations, see the preceding code.
- After you initialize the MultipartUpload task or upload some parts, you can use the abortMultipartUpload API to abort the MultipartUpload task. When the MultipartUpload task is aborted, you cannot use the same upload ID to perform any operations and the uploaded parts are also deleted.

View uploaded parts

You can list all the parts that have been successfully uploaded with a specified upload ID.

The following code provides an example of how to view all uploaded parts of a MultipartUpload task:

```
/**
 * View uploaded parts.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @param string $uploadId Upload ID
 * @return null
 */
function putObject($ossClient, $bucket, $uploadId)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    try{
        $listPartsInfo = $ossClient->listParts($bucket, $object, $upload_id);
        foreach ($listPartsInfo->getListPart() as $partInfo) {
            print($partInfo->getPartNumber() . "\t" . $partInfo->getSize() . "\t" . $partInfo->getETag() . "\t" .
$partInfo->getLastModified() . "\n");
        }
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

View ongoing MultipartUpload tasks

The following code provides an example of how to list ongoing MultipartUpload tasks:

```
<? php
/**
 * Obtain a list of currently unfinished MultipartUpload tasks.
 *
 * @param $ossClient OssClient
 * @param $bucket string
 */
function listMultipartUploads($ossClient, $bucket) {
    $options = array(
            'delimiter' => '/',
            'max-uploads' => 100,
            'key-marker' => '',
            'prefix' => '',
            'upload-id-marker' => ''
        );
    try {
        $listMultipartUploadInfo = $ossClient->listMultipartUploads($bucket, $options);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": listMultipartUploads FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    printf(__FUNCTION__ . ": listMultipartUploads OK\n");
    $listUploadInfo = $listMultipartUploadInfo->getUploads();
    var_dump($listUploadInfo);
}
```

The following table describes the parameters of $options in the preceding code.

Key	Description
delimiter	The delimiter used to group objects by name. CommonPrefixes specify a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter.
key-marker	The starting position of the returned results. This parameter is used together with the upload-id-marker parameter.
max-uploads	Specifies the maximum number of multipart upload tasks returned for one request. If this parameter is not specified, the default value 1,000 is used. The max-uploads value cannot exceed 1,000.
prefix	The prefix that must be contained in the keys of the returned objects. Note that if you use a prefix to make a query, the returned key values still contain the prefix.

Key	Description
upload-id-marker	Used together with the key-marker parameter to specify the starting position of the returned results.

Set Object Meta

Object Meta describes the attributes of objects uploaded to OSS. These attributes are classified into two types: HTTP standard attributes (HTTP headers) and User Meta (user-defined Object Meta). Object Meta can be set in various upload modes (string upload, object upload, append upload, and multipart upload) or during object copy operations. The name of Object Meta is case-insensitive.

Set HTTP headers

OSS allows you to customize HTTP headers. For information about HTTP headers, see RFC2616. The following table describes some commonly-used HTTP headers.

Name	Description	Default value
Content-MD5	The object data verification. After this value is specified, OSS enables MD5 verification for the object content and compares the MD5 value that you have provided with the MD5 value of the object. OSS throws an error if any inconsistency is found.	None
Content-Type	The object MIME. It defines the object type and Webpage encoding mode and determines the form and encoding mode used by the browser to read the object. If not specified, the object MIME is generated based on the key or object name extension. If no extension is available, the default value applies.	application/octet-stream
Content-Disposition	The instructions for how the MIME user agent displays an attached object, whether it opens or downloads the attached object, and the object name.	None
Content-Length	The length of the uploaded object. Excess length is truncated. If the data falls short of the length, the actual data length applies.	The duration of the stream or object

Name	Description	Default value
Expires	The expiration time of the buffer. The time format is GMT.	None
Cache-Control	The Webpage caching behavior specified when the object is downloaded.	None

The following code provides an example of how to set the HTTP headers of an object during upload:

```
/**
 * Set Object Meta of an object during the upload.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function putObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    $content = file_get_contents(__FILE__);
    $options = array(
        OssClient::OSS_HEADERS => array(
            'Expires' => '2012-10-01 08:00:00',
            'Content-Disposition' => 'attachment; filename="xxxxxx"',
    ));
    try{
        $ossClient->putObject($bucket, $object, $content, $options);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note

- You can set the Content-Type parameter of an object to modify the object type.
- You can set Content-Disposition of an object to control the object download behavior.

User-defined Object Meta

OSS allows you to customize Object Meta to describe objects.

The following code provides an example of how to set the user-defined Object Meta of an object during the upload:

```
<? php
/**
 * Set the user-defined Object Meta of an object during the upload.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function putObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    $content = file_get_contents(__FILE__);
    $options = array(OssClient::OSS_HEADERS => array(
        'x-oss-meta-self-define-title' => 'user define meta info',
    ));
    try{
        $ossClient->putObject($bucket, $object, $content, $options);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note

- You can use `OssClient::getObjectMeta` to obtain Obejct Meta.
- The name of the user-defined meta is case-insensitive. For example, if user-defined Obejct Meta is set to x-oss-meta-name, you need only to read the parameter named x-oss-meta-name.
- An object may contain multiple pieces of Object Meta, the total size of which cannot exceed 8 KB.

Use MD5 verification during uploads

OSS supports MD5 verification to ensure the consistency between the data sent by the PHP SDK and the data received on the OSS server. MD5 verification is disabled by default during object uploads (string upload, object upload, append upload, and multipart upload). If you need to enable MD5 verification, you can set options for object uploads.

The following code provides an example of how to enable MD5 verification during the upload:

```
<? php
/**
 * Enable MD5 verification during the upload.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function putObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    $options = array(OssClient::OSS_CHECK_MD5 => true);
    try{
        $ossClient->uploadFile($bucket, $object, __FILE__, $options);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note Performance may deteriorate if MD5 verification is used.

2.4.2.3.6. Download objects

The OSS PHP SDK provides a variety of object download APIs. You can download an object from OSS through any of the following methods:

- Download an object to a local file
- Download an object to the buffer
- Range download
- Conditional download

Note For the complete object download code, see GitHub.

Download an object to a local file

The following code provides an example of how to download an OSS object to a local file:

```
<? php
/**
 * get_object_to_local_file
 *
 * Obtain the object
 * Download the object to a specified file
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function getObjectToLocalFile($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/download-test-object-name.txt";
    $localfile = "download-test-object-name.txt";
    $options = array(
        OssClient::OSS_FILE_DOWNLOAD => $localfile,
    );
    try{
        $ossClient->getObject($bucket, $object, $options);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK, please check localfile: 'upload-test-object-name.txt'" . "\n");
}
```

Download an object to the buffer

The following code provides an example of how to download an object to the buffer:

```
<? php
/**
 * Obtain the content of an object.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function getObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    try{
        $content = $ossClient->getObject($bucket, $object);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Range download

If you need to download only a part of data from a large OSS object, you can use range download to download the data within a specified range. If the specified download range is 0-100, the data from byte 0 to byte 100 (included) is returned, that is, 101 bytes of data in total. If the specified range is invalid, the entire object is downloaded.

The following code provides an example of how to download the content of [1, 100] of an object to the buffer:

```
<? php
/**
 * Obtain the content of an object.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function getObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    try{
        $options = array(OssClient::OSS_RANGE => '0-100');
        $content = $ossClient->getObject($bucket, $object, $options);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note

- You can use range download to download an entire object.
- The download range is a closed interval `[start, end]`, with both ends inclusive.

Conditional download

You can specify one or more conditions for downloading an object. The object can be downloaded only when all specified conditions are met. Otherwise, an error is returned and the object cannot be downloaded. The following table describes the available download conditions.

Name	Description	Corresponding value in the PHP SDK
If-Modified-Since	The object download condition. If the specified time is earlier than the actual object modification time, the object can be downloaded. Otherwise, an error is returned.	OssClient::OSS_IF_MODIFIED_SINCE
If-Unmodified-Since	The object download condition. If the specified time is equal to or later than the actual object modification time, the object can be downloaded. Otherwise, an error is returned.	OssClient::OSS_IF_UNMODIFIED_SINCE

Name	Description	Corresponding value in the PHP SDK
If-Match	The object download condition. If the ETag value of the source object is equal to the ETag value specified in the request, the object can be downloaded. Otherwise, an error is returned.	OssClient::OSS_IF_MATCH
If-None-Match	The object download condition. If the ETag value of the source object is not equal to the ETag value specified in the request, the object can be downloaded. Otherwise, an error is returned.	OssClient::OSS_IF_NONE_MATCH

Note

- If the time specified by If-Modified-Since does not conform to the specification, the object and the 200 OK message are returned.
- You can use If-Modified-Since and If-Unmodified-Since as object download conditions at the same time. You can use If-Match and If-None-Match as object download conditions at the same time.
- If a request does not meet the condition specified in If-Unmodified-Since or If-Match, the 412 Precondition Failed error is returned.
- If a request does not meet the condition specified in If-Modified-Since or If-None-Match, the 304 Not Modified error is returned.

```
<? php
/**
 * Download an object if the object has been modified since the specified time.
 *
 * @param OssClient $ossClient OssClient instance
 * @param string $bucket Bucket name
 * @return null
 */
function getObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    try{
        $options = array(
            OssClient::OSS_HEADERS => array(
                OssClient::OSS_IF_MODIFIED_SINCE => "Fri, 13 Nov 2015 14:47:53 GMT"),
    );
        $content = $ossClient->getObject($bucket, $object, $options);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note

- You can obtain the object ETag value through `OssClient::getObjectMeta`.
- You can download an entire object through conditional download.

2.4.2.3.7. Manage objects

In OSS, you can manage objects in a bucket through a series of APIs, such as ListObjects, DeleteObject, CopyObject, and DoesObjectExist.

Note For the complete code, see GitHub.

List objects in a bucket

The following code provides an example of how to use `OssClient::listObjects` to list all objects in a bucket:

```
<? php
```

```
/**
 * List all directories and objects in a bucket. The ListObjects API is called cyclically based on the returne
d nextMarker until all objects and directories are listed.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function listAllObjects($ossClient, $bucket)
{
    // Create objects and virtual directories in the dir directory.
    for ($i = 0; $i < 100; $i += 1) {
        $ossClient->putObject($bucket, "dir/obj" . strval($i), "hi");
        $ossClient->createObjectDir($bucket, "dir/obj" . strval($i));
    }
    $prefix = 'dir/';
    $delimiter = '/';
    $nextMarker = '';
    $maxkeys = 30;
    while (true) {
        $options = array(
            'delimiter' => $delimiter,
            'prefix' => $prefix,
            'max-keys' => $maxkeys,
            'marker' => $nextMarker,
        );
        var_dump($options);
        try {
            $listObjectInfo = $ossClient->listObjects($bucket, $options);
        } catch (OssException $e) {
            printf(__FUNCTION__ . ": FAILED\n");
            printf($e->getMessage() . "\n");
            return;
        }
        // Obtain nextMarker to list the remaining objects. The reading starts with the object next to the la
st object previously obtained through the ListObjects API.
        $nextMarker = $listObjectInfo->getNextMarker();
        $listObject = $listObjectInfo->getObjectList();
        $listPrefix = $listObjectInfo->getPrefixList();
        var_dump(count($listObject));
        var_dump(count($listPrefix));
        if ($nextMarker === '') {
```

```
        if ($nextMarker === '') {
            break;
        }
    }
}
```

The following table describes the parameters of $options in the preceding code.

Key	Description
delimiter	The delimiter used to group objects by name. CommonPrefixes specify a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter.
prefix	The prefix that must be contained in the names (key) of the returned objects. Note that if you use a prefix to make a query, the returned key values still contain the prefix.
max-keys	The maximum number of objects returned for one request. If this parameter is not specified, the default value is 100. The maximum value cannot exceed 1,000.
marker	The starting position of the object list. Objects are sorted in the alphabetical order and those objects following this marker are listed.

Note The prefix, delimiter, marker, and max-keys parameters are all optional.

Determine whether a specified object exists

The following code provides an example of how to use `OssClient::doesObjectExist` to determine whether an object exists:

```
<? php
/**
 * Check whether an object exists.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function doesObjectExist($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    try{
        $exist = $ossClient->doesObjectExist($bucket, $object);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
    var_dump($exist);
}
```

Create a virtual directory

OSS does not use the folder concept. OSS stores all elements as objects. Creating a folder means creating an empty object. You can upload and download the object, but Apsara Stack Management Console displays the object whose name ends with a forward slash / as a directory.

```
<? php
/**
 * Create a virtual directory.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function createObjectDir($ossClient, $bucket) {
    try{
        $ossClient->createObjectDir($bucket, "dir");
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Delete an object

The following code provides an example of how to use `OssClient::deleteObject` to delete an object:

```
<? php
/**
 * Delete an object.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function deleteObject($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    try{
        $ossClient->deleteObject($bucket, $object);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note You cannot restore objects that are deleted.

Delete multiple objects

The following code provides an example of how to use `OssClient::deleteObjects` to delete multiple objects simultaneously:

```
<? php
/**
 * Delete multiple objects simultaneously.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function deleteObjects($ossClient, $bucket)
{
    $objects = array();
    $objects[] = "oss-php-sdk-test/upload-test-object-name.txt";
    $objects[] = "oss-php-sdk-test/upload-test-object-name.txt.copy";
    try{
        $ossClient->deleteObjects($bucket, $objects);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Copy objects

The following code provides an example of how to use `OssClient::copyObject` to copy an object:

```
<? php
/**
 * Copy an object.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function copyObject($ossClient, $bucket)
{
    $from_bucket = $bucket;
    $from_object = "oss-php-sdk-test/upload-test-object-name.txt";
    $to_bucket = $bucket;
    $to_object = $from_object . '.copy';
    try{
        $ossClient->copyObject($from_bucket, $from_object, $to_bucket, $to_object);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note You can use `OssClient::copyObject` to copy an object smaller than 1 GB. copy an object larger than 1 GB, use `OssClient::uploadPartCopy` .

Modify Object Meta

Object Meta describes the attributes of objects uploaded to OSS. These attributes are classified into two types: HTTP standard attributes (HTTP headers) and User Meta (user-defined Object Meta). You can set Object Meta when you upload or copy objects in various ways.

HTTP standard attributes include Cache-Control, Content-Disposition, Content-Encoding, Content-Language, Expires, Content-Length, Content-Type and Last-Modified.

This feature is designed for you to enrich the descriptions of objects. OSS regards all parameters prefixed with x-oss-meta- as User Meta, such as x-oss-meta-location. An object may have multiple similar parameters, but the total size of the user-defined Object Meta cannot exceed 8 KB. User Meta is returned when you download the object or obtain Object Meta.

You can use the COPY operation to modify the Object Meta of an existing object. If the source object URL and target object URL of the COPY operation are the same, the source Object Meta is directly replaced.

```
/**
 * Modify Object Meta
 * If the target object is identical with the source object, the Object Meta is modified. This is a feature of the copyObject API.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function modifyMetaForObject($ossClient, $bucket)
{
    $fromBucket = $bucket;
    $fromObject = "oss-php-sdk-test/upload-test-object-name.txt";
    $toBucket = $bucket;
    $toObject = $fromObject;
    $copyOptions = array(
        OssClient::OSS_HEADERS => array(
            'Expires' => '2018-10-01 08:00:00',
            'Content-Disposition' => 'attachment; filename="xxxxxx"',
            'x-oss-meta-location' => 'location',
        ),
    );
    try{
        $ossClient->copyObject($fromBucket, $fromObject, $toBucket, $toObject, $copyOptions);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Note

- You can use `Content-Type` to modify the object type.
- You can use `Content-Disposition` to control the object download behavior.

Obtain Object Meta

The following code provides an example of how to use `OssClient::getObjectMeta` to obtain Object Meta:

```
<? php
/**
 * Use getObjectMeta to obtain Object Meta.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function getObjectMeta($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    try {
        $objectMeta = $ossClient->getObjectMeta($bucket, $object);
    } catch (OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
    if (isset($objectMeta[strtolower('Content-Disposition')]) &&
        'attachment; filename="xxxxxx"' === $objectMeta[strtolower('Content-Disposition')]
    ) {
        print(__FUNCTION__ . ": ObjectMeta checked OK" . "\n");
    } else {
        print(__FUNCTION__ . ": ObjectMeta checked FAILED" . "\n");
    }
}
```

Set the ACL of an object

There are four permissions included in object ACLs: default, private, public-read, and public-read-write, as described in the following table.

ACL	Description	Corresponding value in the PHP SDK
Default	The object inherits the ACL of the bucket. This is the default object ACL.	default
private	The object is a private resource. Only the owner or authorized user has the read and write permissions on the object. A signature is required for anonymous access requests.	private

ACL	Description	Corresponding value in the PHP SDK
public-read	Only the owner or authorized user of an object has the read and write permissions on the object. Other users (including anonymous users) have only read permissions on the object.	public-read
public-read-write	The object is a read/write resource for the public. All users of an object have the read and write permissions on the object.	public-read-write

The ACL privileges of objects take precedence over those of buckets. For example, OSS allows users to access a public-read-write object in a bucket even though the bucket is private. If no ACL has been set for an object, its bucket ACL applies.

The following code provides an example of how to use `OssClient::putObjectAcl` to set the object ACL:

```
<? php
/**
 * Obtain the ACL of an object.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function putObjectAcl($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    $acl = "public-read";
    try {
        $ossClient->putObjectAcl($bucket, $object, $acl);
    } catch (OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
}
```

Obtain the ACL of an object

The following code provides an example of how to use `OssClient::getObjectAcl` to obtain the object ACL:

```
<? php
/**
 * Obtain the ACL of an object.
 *
 * @param OssClient $ossClient OssClient instance
 * @param $bucket string Bucket name
 * @return null
 */
function getObjectMeta($ossClient, $bucket)
{
    $object = "oss-php-sdk-test/upload-test-object-name.txt";
    try {
        $objectAcl = $ossClient->getObjectAcl($bucket, $object);
    } catch (OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": OK" . "\n");
    var_dump($objectAcl);
}
```

2.4.2.3.8. Authorized access

Add a signature to a URL for authorized temporary access

You can generate a signature and add it to a URL for temporary access. During URL generation, you can specify the URL expiration time to limit the access duration.

> **Note** For the complete code, see GitHub.

Use a private download link

The following code provides an example of how to generate a signature and add it to a URL of GetObject:

```
<? php
/**
 * Generate a signature for a URL of GetObject for read access control when the private permission is gr
anted.
 *
 * @param $ossClient OssClient OssClient instance
 * @param $bucket string bucket name
 * @return null
 */
function getSignedUrlForGettingObject($ossClient, $bucket)
{
    $object = "test/test-signature-test-upload-and-download.txt";
    $timeout = 3600; // The validity period of the URL is 3,600 seconds.
    try{
        $signedUrl = $ossClient->signUrl($bucket, $object, $timeout);
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": signedUrl: " . $signedUrl. "\n");
    /**
     * You can use similar code to access the URL with a signature, or access the URL with a signature in a
browser.
     */
    $request = new RequestCore($signedUrl);
    $request->set_method('GET');
    $request->send_request();
    $res = new ResponseCore($request->get_response_header(), $request->get_response_body(), $requ
est->get_response_code());
    if ($res->isOK()) {
        print(__FUNCTION__ . ": OK" . "\n");
    } else {
        print(__FUNCTION__ . ": FAILED" . "\n");
    };
}
```

Note The generated URL supports access through GET by default, which grants users direct access to related content through a browser.

Use a private upload link

If you want to allow users to perform other temporary operations (such as object the upload and deletion), you may need to generate a signed URL for another method. The following code provides an example of how to generate a signature for a URL of the PUT method:

```
<? php
/**
 * Generate a signature for a URL of PutObject for write access control when the private permission is gr
anted.
 *
 * @param OssClient $ossClient  OssClient instance
 * @param $bucket string bucket name
 * @return null
 * @throws OssException
 */
function getSignedUrlForPuttingObject($ossClient, $bucket)
{
    $object = "test/test-signature-test-upload-and-download.txt";
    $timeout = 3600;
    $options = NULL;
    try{
        $signedUrl = $ossClient->signUrl($bucket, $object, $timeout, "PUT");
    } catch(OssException $e) {
        printf(__FUNCTION__ . ": FAILED\n");
        printf($e->getMessage() . "\n");
        return;
    }
    print(__FUNCTION__ . ": signedUrl: " . $signedUrl. "\n");
    $content = file_get_contents(__FILE__);
    $request = new RequestCore($signedUrl);
    $request->set_method('PUT');
    $request->add_header('Content-Type', '');
    $request->add_header('Content-Length', strlen($content));
    $request->set_body($content);
    $request->send_request();
    $res = new ResponseCore($request->get_response_header(),
        $request->get_response_body(), $request->get_response_code());
    if ($res->isOK()) {
        print(__FUNCTION__ . ": OK" . "\n");
    } else {
        print(__FUNCTION__ . ": FAILED" . "\n");
    };
}
```

Use STS for uploads and downloads

Overview

OSS allows you to use Alibaba Cloud STS for temporary access authorization. Alibaba Cloud STS is a web service that provides a temporary access token to a cloud computing user. Through STS, you can grant a third-party application or federated user (whose user ID is managed by yourself) an access credential with a custom validity period and permissions.

Use an STS credential to create an OssClient

After you obtain a temporary STS credential for your OssClient, the OssClient is generated based on the security token and temporary Access Key (AccessKey ID and AccessKey Secret).

The following code provides an example of how to use a temporary STS credential to create an OssClient:

```
<? php
$accessKeyId = "<accessKeyId>";
$accessKeySecret = "<accessKeySecret>";
$securityToken = "<securityToken>";
$endpoint = "http://oss-cn-hangzhou.aliyuncs.com";
$ossClient = new OssClient($accessKeyId, $accessKeySecret, $endpoint, false, $securityToken);
```

2.4.2.3.9. Exception handling

If an exception occurs when you call the OssClient-class API, the related operation fails. Otherwise, the related operation succeeds. If an exception occurs, the data returned by the API is invalid. When an OssClient error occurs, OssException is thrown.

Exception handling example

```
try {
    $ossClient->createBucket($bucket);
} catch (OssException $e) {
    print("Exception:" . $e->getMessage() . "\n");
}
```

OssException

The OssException exception class is classified into two types:

- Client exceptions, such as invalid parameters and nonexistent files. You can use OssException::getMessage() to obtain exception information.
- Server exceptions, namely errors returned by OSS, such as no permissions and nonexistent objects. You can use OssException::getMessage() to obtain exception information. This type of exception also includes the following information:
  - HTTPStatus: the HTTP status code, obtained by using the getHTTPStatus() method.
  - ErrorCode: the error code returned by OSS, obtained with the getErrorCode() method.

- ErrorMessage: the error description provided by OSS, obtained with the getErrorMessage() method.
- RequestId: the universally unique identifier (UUID) of a request. If the problem persists, you can seek help from OSS development engineers and provide them with the request ID. You can obtain the request ID using getRequestId().
- Details: the original error message returned by OSS. You can obtain the error message using getDetails().

Common OSS error codes

Error code	Description	HTTP status code
AccessDenied	The error message returned when the access is denied.	403
BucketAlreadyExists	The error message returned when the bucket already exists.	409
BucketNotEmpty	The error message returned when the bucket is not empty.	409
EntityTooLarge	The error message returned when the entity is too large.	400
EntityTooSmall	The error message returned when the entity is too small.	400
FileGroupTooLarge	The error message returned when the object group is too large.	400
FilePartNotExist	The error message returned when the object part does not exist.	400
FilePartStale	The error message returned when the object part has expired.	400
InvalidArgument	The error message returned when the parameter format is invalid.	400
InvalidAccessKeyId	The error message returned when the AccessKey ID does not exist.	403
InvalidBucketName	The error message returned when the bucket name is invalid.	400
InvalidDigest	The error message returned when the digest is invalid.	400
InvalidObjectName	The error message returned when the object name is invalid.	400
InvalidPart	The error message returned when the part is invalid.	400
InvalidPartOrder	The error message returned when the part sequence is invalid.	400
InvalidTargetBucketForLogging	The error message returned when the logging operation involves an invalid target bucket.	400

Error code	Description	HTTP status code
InternalError	The error message returned when an internal OSS error occurs.	500
MalformedXML	The error message returned when the XML format is invalid.	400
MethodNotAllowed	The error message returned when the method is not supported.	405
MissingArgument	The error message returned when a parameter is missing.	411
MissingContentLength	The error message returned when the content length is missing.	411
NoSuchBucket	The error message returned when no such bucket exists.	404
NoSuchKey	The error message returned when no such key exists.	404
NoSuchUpload	The error message returned when no such multipart upload ID exists.	404
NotImplemented	The error message returned when the method cannot be implemented.	501
PreconditionFailed	The error message returned when a precondition error occurs.	412
RequestTimeTooSkewed	The error message returned when the duration between the request sending time and the server responding time exceeds 15 minutes.	403
RequestTimeout	The error message returned when the request has timed out.	400
SignatureDoesNotMatch	The error message returned when a signature error occurs.	403
InvalidEncryptionAlgorithmError	The error message returned when the specified encryption algorithm (entropy) is invalid.	400

2.4.2.4. C-SDK

2.4.2.4.1. Preface

Download the SDK

V3.4.0 (2017-02-22):

- Linux SDK package: aliyun_oss_c_sdk_v3.4.0.tar.gz
- Windows SDK package: aliyun_oss_c_sdk_v3.4.0.zip

- Source code: GitHub

Compatibility

- V3.*.* is compatible with V3.0.0.
- 3.0.0 is compatible with V2.*.*.
  - Compatible with Windows
  - Compatible with Linux APIs, except for the following linked list (aos_list_t) traversal APIs:
    - aos_list_for_each_entry
    - aos_list_for_each_entry_reverse
    - aos_list_for_each_entry_safe
    - aos_list_for_each_entry_safe_reverse
- V2.1.0 is compatible with V2.0.0.
- V2.0.0 is compatible with V1.0.0, except for the following structures and APIs:
  - oss_request_options_t
  - oss_get_object_to_buffer
  - oss_get_object_to_file
  - oss_get_object_to_buffer_by_url
  - oss_get_object_to_file_by_url
  - oss_init_multipart_upload
  - oss_complete_multipart_upload
- V1.0.0 is incompatible with V0.0.*.

Overview

This document describes how to install and use the OSS C SDK. This document assumes that you have enabled Apsara Stack OSS and created an AccessKey ID and AccessKey Secret. If you have not activated or do not know about OSS, log on to the OSS Product Homepage for more help.

2.4.2.4.2. Installation

This document describes prerequisites, installation, and sample projects of the OSS C SDK.

Prerequisites

- You have enabled Apsara Stack OSS and created an AccessKey ID and AccessKey Secret.
- If you have not activated or do not know about Apsara Stack OSS, log on to the OSS Product Homepage for details.
- If you have not created an AccessKey ID and AccessKey Secret, create an AccessKey in the Alibaba Cloud console.

Install the C SDK

The SDK supports Linux and Windows systems.

- Linux
  i. When installing the OSS C SDK in Linux, you must install CMake and the following third-party libraries: cURL, APR, APR-util, and Mini-XML. The following table describes parameters

required to install the OSS C SDK.

Parameter	Description	Version
CMake	Manages the build process of software using a compiler-independent method.	V2.6.0 or later
cURL	Resolves network issues.	V7.32.0 or later
APR-util	Resolves the issues of memory and different platforms.	1.5.2 or later
Mini-XML	Parses the XML string returned by a request.	V2.9

Install the OSS C SDK based on the following systems:

- Ubuntu or Debian

  Install CMake and third-party libraries:

  ```
  sudo apt-get install cmake libcurl4-openssl-dev libapr1-dev libaprutil1-dev libmxml-dev
  ```

- RedHat, Aliyun, or CentOS

  Install CMake and third-party libraries:

  ```
  sudo yum cmake install curl-devel apr-devel apr-util-devel mxml mxml-devel
  ```

  > **Note** If the YUM source does not contain the MXML installation package, use RPM to install MXML. Download the system-specific RPM package: 64-bit-specific RPM package or 32-bit-specific RPM package.
  >
  > Use the RPM package to install MXML:
  >
  > ```
  > rpm -ivh mxml-2.10-1.x86_64.rpm
  > ```

- SUSE

  Install CMake and third-party libraries:

  ```
  zypper install cmake libcurl-devel libapr1-devel libapr-util1-devel mxml-devel
  ```

- Other Linux OSs

  Run the following code to compile and install CMake, libcurl, APR, APR-util, and Mini-XML:

  ```
  ./configure  // The default installation path is /usr/local.
  make
  make install
  ```

  - CMake: download URL
  - libcurl: download URL. For more information, see libcurl Installation Guide.

    To use the Media C SDK, ensure that HTTPS is contained in the last line of Protocols after the ./configure command is run. If HTTPS is not contained in the last line of Protocols, install openssl-devel or another SSL SDK first and reinstall libcurl.
  - APR: download URL
  - APR-util: download URL

    You must use `—with-apr` to specify the directory of the APR package, such as `./configure --with-apr=/your/apr/install/path`.
  - Mini-XML: download URL

ii. Compile and install the OSS C SDK.

```
cmake .
make
make install
```

You can specify a path where third-party libraries cURL, APR, APR-util, and Mini-XML.are installed. The installation method is as follows:

```
cmake -f CMakeLists.txt // The build type is Release. Typical build types include Debug, Release, RelWithDebInfo, and MinSizeRel. Debug is used by default.
-DCMAKE_BUILD_TYPE = Release // Specify the build type.
-DCMAKE_INSTALL_PREFIX=/usr/local/ // Specify the path where third-party libraries cURL, APR, APR-util, and Mini-XML are installed.
-DCURL_INCLUDE_DIR=/usr/include/curl
-DCURL_LIBRARY=/usr/lib64/libcurl.so
-DAPR_INCLUDE_DIR=/usr/include/apr-1
-DAPR_LIBRARY=/usr/lib64/libapr-1.so
-DAPR_UTIL_INCLUDE_DIR=/usr/include/apr-1
-DAPR_UTIL_LIBRARY=/usr/lib64/libaprutil-1.so
-DMINIXML_INCLUDE_DIR=/usr/include
--DMINIXML_LIBRARY=/usr/lib64/libmxml.so// If Could not find apr-config/apr-1-config is reported during the build process, the cause is that the apr-1-config file does not exist in the default path. Add this file to the default path.
-DAPR_CONFIG_BIN=/path/to/bin/apr-1-config// If Could not find apu-config/apu-1-config is reported, add the apu-1-config file to the default path.
-DAPU_CONFIG_BIN=/path/to/bin/apu-1-config
```

- Windows
  i. Download the SDK.
     - Download the SDK directly
     - Download from GitHub
  ii. Install the SDK.

> **Note** If you use Visual Studio 2012 or later, you are prompted to choose whether to upgrade the project version to adapt to the latest version of the compiler and library. We recommend that you use a version that matches your project. If the project uses the compiler and libraries of the latest version, you can choose to upgrade the project. Otherwise, you do not need to upgrade the project.

Sample projects

The OSS C SDK provides a variety of sample programs for your reference or use. You can obtain sample programs from GitHub. The following table describes the sample files in the sample program.

Sample file	Description
oss_put_object_sample	Shows how to upload objects, including object upload from the memory or local files, object upload with MD5 verification, object upload with object metadata, and object upload based on a signed URL.

Sample file	Description
oss_get_object_sample.c	Shows how to download objects, including object download to the memory, object download to objects, range download, and object download based on a signed URL.
oss_append_object_sample.c	Shows how to perform append upload, including append upload from the memory and append upload from objects.
oss_multipart_upload_sample.c	Shows how to perform multipart upload, including multipart upload from the memory, multipart upload from local files, and multipart upload cancellation.
oss_resumable_sample.c	Shows how to perform resumable upload.
oss_head_object_sample.c	Shows how to obtain object metadata.
oss_delete_object_sample.c	Shows how to delete objects, including the deletion of a single object and multiple objects.
oss_callback_sample.c	Shows how to perform upload callback, including upload callback and multipart upload callback.
oss_progress_sample.c	Shows how to use a progress bar, including uploads, append upload, multipart upload, and download with a progress bar.
oss_crc_sample.c	Shows how to perform CRC verification for uploads and downloads.
oss_image_sample.c	Shows how to use image processing (IMG).

2.4.2.4.3. Initialization

Set an AccessKey

To access Apsara Stack OSS, you need a pair of valid access keys (AccessKey ID and AccessKey Secret) for signature authentication.

After obtaining the AccessKey ID and AccessKey Secret, follow the steps for initialization.

Initialize request options

To use the OSS C SDK, you need to initialize request options (oss_request_options_t). The config variable stores basic information for accessing OSS, such as the OSS endpoint, and the user's AccessKey ID and AccessKey Secret. The is_cname variable specifies whether to use CNAME to access OSS. The ctl variable sets the control information to access OSS.

```
void init_options(oss_request_options_t *options) {
    options->config = oss_config_create(options->pool);
    aos_str_set(&options->config->endpoint, "<Your endpoint>");
    aos_str_set(&options->config->access_key_id, "<Your AccessKey ID>");
    aos_str_set(&options->config->access_key_secret, "<Your AccessKey Secret>");
    options->config->is_cname = 0;
    options->ctl = aos_http_controller_create(options->pool, 0);
}
int main() {
    aos_pool_t *p;
    oss_request_options_t *options;
    /* Initialize the global variables at program startup and before all other logic. */
    if (aos_http_io_initialize(NULL, 0) ! = AOSE_OK) {
        return -1;
    }
    /* Initialize the memory pool and options. */
    aos_pool_create(&p, NULL);
    options = oss_request_options_create(p);
    init_options(options);
    /* Logic code */
    /* Release the memory pool resources including the memory allocated through the pool such as option
s */
    aos_pool_destroy(p);
    /* Release global resources before the program ends. */
    aos_http_io_deinitialize();
    return 0;
}
```

Note

- If you want to use HTTPS, you need only to use `https://` for the prefix when setting the endpoint.
- Multithreading is supported, but the aos_http_io_initialize and aos_http_io_deinitialize methods need only to be called in the main thread. They are not required in other threads.
- To set the underlying libcurl communication parameters of the OSS C SDK, set the ctl variable in the request options to control the minimum data upload speed, the connection timeout value, and the DNS cache expiration time.
- You can also use the ctl variable to obtain the performance parameters to access OSS through the OSS C SDK. Take data upload as an example. After uploading data, you can obtain a series of parameter indicators, such as the start time of the data upload (start_time), the time of uploading the first byte (first_byte_time), and the time elapsed when the data upload is finished (finish_time).

2.4.2.4.4. Quick start

This topic describes how to use the OSS C SDK to complete some basic operations.

Step 1: Initialize the OSS C SDK runtime environment.

When using the OSS C SDK, you must first initialize the runtime environment, and clear the runtime environment before you stop using it. The following code provides an example of how to initialize the OSS C SDK runtime environment:

```
int main(int argc, char *argv[])
{
    /* Call aos_http_io_initialize in main() to initialize global resources, such as the network and memory.*
/
    if (aos_http_io_initialize(NULL, 0) ! = AOSE_OK) {
        exit(1);
    }

    /* Call the OSS SDK API to upload or download an object. */
    /* ... The user logic code is omitted here. */

    /* Before the project ends, call aos_http_io_deinitialize to release allocated global resources. */
    aos_http_io_deinitialize();
    return 0;
}
```

Note

- You can use aos_http_io_initialize to initialize the OSS C SDK runtime environment. The first parameter can be used to customize the user agent content for statistics in the future.
- You can use aos_http_io_deinitialize to clear the OSS C SDK runtime environment.

Step 2: Initialize request options.

Use the following code to initialize request options for all operations of the OSS C SDK:

```
    /* Use aos_pool_t, which is equivalent to apr_pool_t, to manage the memory pool. The implementation code is in the apr library. */
    aos_pool_t *pool;
    oss_request_options_t *options;

    /* Recreate a new memory pool. The second parameter is NULL, indicating that the pool does not inher it any other memory pool. */
    aos_pool_create(&pool, NULL);

    /* Create and initialize options. This parameter includes endpoint, access_key_id, acces_key_secret, is _cname, and curl parameters among other global configuration information.
     * The options memory is allocated by the pool. After the pool is released, the options memory is also r eleased, indicating that you do not need to release the memory separately.
     */
    options = oss_request_options_create(pool);
    options->config = oss_config_create(options->pool);

    /* aos_str_set uses a char* string to initialize the aos_string_t data type. */
    aos_str_set(&options->config->endpoint, "<Your endpoint>");
    aos_str_set(&options->config->access_key_id, "<Your AccessKey ID>");
    aos_str_set(&options->config->access_key_secret, "<Your AccessKey Secret>");

    /* Determine whether CNAME is used. */
    options->config->is_cname = 0;

    /* Used to configure network parameters, such as timeout. */
    options->ctl = aos_http_controller_create(options->pool, 0);
```

Step 3: Create a bucket.

The following code provides an example of how to create a bucket:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *resp_headers;
oss_acl_e oss_acl = OSS_ACL_PRIVATE;
char *bucket_name = "<Your bucket name>";
aos_string_t bucket;

aos_pool_create(&p, NULL);

options = oss_request_options_create(p);
init_options(options);

/* Assign char* data to the aos_string_t bucket. */
aos_str_set(&bucket, bucket_name);
s = oss_create_bucket(options, &bucket, oss_acl, &resp_headers);

/* Determine whether the bucket is created successfully. */
if (aos_status_is_ok(s)) {
    printf("create bucket succeeded\n");
} else {
    printf("create bucket failed\n");
}

/* Release the memory pool after the request is executed. In other words, release the memory allocat
ed to various resources used for the request. */
aos_pool_destroy(p);
```

Note

- The bucket name must be unique in OSS. To create a bucket, you must select a unique bucket name.
- The response of oss_create_bucket is aos_status_t, which includes code (HTTP code), error_code, error_msg, and req_id. The req_id field helps investigate problems. Unless otherwise specified, other APIs also return aos_status_t.

Step 4: Upload an object.

Objects are the most basic data units in OSS. The following code provides an example of how to upload an object:

```
aos_pool_t *p;
oss_request_options_t *options;
```

```
aos_status_t *s;
aos_table_t *headers;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
aos_string_t bucket;
aos_string_t object;
char *data = "object content";
aos_list_t buffer;
aos_buf_t *content;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&object, object_name);
aos_str_set(&bucket, bucket_name);
headers = aos_table_make(p, 0);

/* Convert char* data to aos_list_t as required using the oss_put_object_from_buffer API. */
aos_list_init(&buffer);
content = aos_buf_pack(options->pool, data, strlen(data));
aos_list_add_tail(&content->node, &buffer);

/* Upload the object. */
s = oss_put_object_from_buffer(options, &bucket, &object, &buffer, headers, &resp_headers);

/* Determine whether the object is uploaded successfully. */
if (aos_status_is_ok(s)) {
    printf("put file succeeded\n");
} else {
    printf("put file failed\n");
}

/* Release resources. */
aos_pool_destroy(p);
```

Step 5: List all objects in a bucket.

After uploading objects to a bucket, use the following code to view the objects in the bucket:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
aos_string_t bucket;
oss_list_object_params_t *params;
oss_list_object_content_t *content;
int max_ret = 1000;
char *key;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);
params = oss_create_list_object_params(p);
params->max_ret = max_ret;
aos_str_set(&params->prefix, "<prefix>");
aos_str_set(&params->delimiter, "<delimiter>");
aos_str_set(&params->marker, "<marker>");

s = oss_list_object(options, &bucket, params, &resp_headers);

/* Determine whether all objects in the bucket are listed. */
if (aos_status_is_ok(s)) {
    printf("list file succeeded\n");
} else {
    printf("list file failed\n");
}

/* Obtain the name of each object. */
aos_list_for_each_entry(content, &params->object_list, node) {
    key = apr_psprintf(p, "%.*s", content->key.len, content->key.data);
}

/* Release resources. */
```

```
aos_pool_destroy(p);
```

Step 6: Download a specified object.

The following code provides an example of how to download a specified object in a simple way:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *headers;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
aos_string_t bucket;
aos_string_t object;
aos_list_t buffer;
aos_buf_t *content;
char *buf;
int64_t len = 0;
int64_t size = 0;
int64_t pos = 0;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&object, object_name);
aos_str_set(&bucket, bucket_name);
headers = aos_table_make(p, 1);

/* Download the object to the buffer. */
aos_list_init(&buffer);
s = oss_get_object_to_buffer(options, &bucket, &object, headers, &buffer, &resp_headers);

/* Determine whether the bucket is created successfully. */
if (aos_status_is_ok(s)) {
    printf("get file succeeded\n");
} else {
    printf("get file failed\n");
```

```
    }

    /* Convert the aos_list_t data in the buffer to char* and calculate the total length of the object read. *
/
    len = aos_buf_list_len(&buffer);
    buf = aos_pcalloc(p, len + 1);
    buf[len] = '\0';
    aos_list_for_each_entry(content, &buffer, node) {
        size = aos_buf_size(content);
            memcpy(buf + pos, content->pos, size);
            pos += size;
    }

    /* Release resources. */
    aos_pool_destroy(p);
```

2.4.2.4.5. Manage buckets

A bucket is a namespace in OSS and a management entity for advanced features such as billing, access control, and access logging. The name of each bucket is globally unique in OSS and cannot be modified. Every object stored in OSS must be included in a bucket.

Create a bucket

The following code provides an example of how to use `oss_create_bucket` to create a bucket and specify the bucket name:

```
aos_pool_t *p;
oss_request_options_t *options;
oss_acl_e oss_acl = OSS_ACL_PRIVATE;
char *bucket_name = "<Your bucket name>";
aos_string_t bucket;
aos_table_t *resp_headers;
aos_status_t *s;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);

/* Create the bucket. */
s = oss_create_bucket(options, &bucket, oss_acl, &resp_headers);
if (aos_status_is_ok(s)) {
   printf("create bucket succeeded\n");
} else {
   printf("create bucket failed\n");
}

aos_pool_destroy(p);
```

Note

- The bucket name must be globally unique.

Delete a bucket

The following code provides an example of how to use `oss_delete_bucket` to delete a specified bucket:

```
aos_pool_t *p;
oss_request_options_t *options;
char *bucket_name = "<Your bucket name>";
aos_string_t bucket;
aos_table_t *resp_headers;
aos_status_t *s;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);

/* Delete the bucket. */
s = oss_delete_bucket (options, &bucket, &resp_headers);
if (aos_status_is_ok(s)) {
   printf("delete bucket succeeded\n");
} else {
   printf("create bucket failed\n");
}

aos_pool_destroy(p);
```

Note

- If the bucket you want to delete contains objects, you need to delete the objects first.
- If the bucket to be deleted has unfinished upload requests, you need to use `oss_list_multipart_upload` and `oss_abort_multipart_upload` to abort the requests first.

Bucket ACL

You can set the ACL for a bucket to allow or forbid anonymous read or write operations on the bucket.

Obtain the ACL of a bucket

The following code provides an example of how to use `oss_get_bucket_acl` to check the ACL of a bucket:

```
aos_pool_t *p;
oss_request_options_t *options;
char *bucket_name = "<Your bucket name>";
aos_string_t bucket;
aos_table_t *resp_headers;
aos_status_t *s;
char *oss_acl;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);

/* Obtain the ACL of the bucket. */
s = oss_get_bucket_acl(options, &bucket,& oss_acl, &resp_headers);
if (aos_status_is_ok(s)) {
   printf("get bucket acl succeeded\n");
} else {
   printf("get bucket acl failed\n");
}

aos_pool_destroy(p);
```

Set the ACL for a bucket

The following code provides an example of how to use `oss_create_bucket` to set the ACL of a bucket:

```
aos_pool_t *p;
oss_request_options_t *options;
oss_acl_e oss_acl = OSS_ACL_PRIVATE;
char *bucket_name = "<Your bucket name>";
aos_string_t bucket;
aos_table_t *resp_headers;
aos_status_t *s;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);

/* Set the ACL of the bucket. */
s = oss_put_bucket_acl(options, &bucket, oss_acl, &resp_headers);
if (aos_status_is_ok(s)) {
   printf("put bucket acl succeeded\n");
} else {
   printf("put bucket acl failed\n");
}

aos_pool_destroy(p);
```

Note

- Only the bucket owner has the permission to set the ACL of the bucket.
- The oss_acl_e parameter used to set the ACL for a bucket (oss_acl_e) is set to an enumerated value. Valid values: OSS_ACL_PRIVATE, OSS_ACL_PUBLIC_READ, and OSS_ACL_PUBLIC_READ_WRITE.

2.4.2.4.6. Upload objects

Objects are the basic data units for user operations in OSS. The maximum size allowed for a single object varies with the data upload method. The PutObject method supports up to 5 GB for a single object. The multipart upload method supports up to 48.8 TB for a single object.

The OSS C SDK provides a variety of object upload methods. You can upload an object to OSS through any of the following methods:

- Simple upload

- Append upload
- Resumable upload
- Multipart upload

Simple upload

Upload an object from the buffer to OSS

The following code provides an example of how to call `oss_put_object_from_buffer` to upload data from the buffer to OSS:

```
void put_object_from_buffer()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    aos_table_t *headers = NULL;
    aos_table_t *resp_headers = NULL;
    oss_request_options_t *options = NULL;
    aos_list_t buffer;
    aos_buf_t *content = NULL;
    char *str = "test oss c sdk";
    aos_status_t *s = NULL;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    /* Initialize parameters. */
    aos_list_init(&buffer);
    content = aos_buf_pack(options->pool, str, strlen(str));
    aos_list_add_tail(&content->node, &buffer);
    /* Upload the object. */
    s = oss_put_object_from_buffer(options, &bucket, &object,
                &buffer, headers, &resp_headers);
    /* Determine whether the object is uploaded. */
    if (aos_status_is_ok(s)) {
        printf("put object from buffer succeeded\n");
    } else {
        printf("put object from buffer failed\n");
    }
    /* Release resources. */
    aos_pool_destroy(p);
}
```

Note For the complete code, see GitHub.

Upload a local file to OSS

The following code provides an example of how to call `oss_put_object_from_file` and specify

filepath to upload a local file to OSS:

```
void put_object_from_file()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    aos_table_t *headers = NULL;
    aos_table_t *resp_headers = NULL;
    oss_request_options_t *options = NULL;
    char *filename = __FILE__;
    aos_status_t *s = NULL;
    aos_string_t file;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    /* Initialize parameters. */
    headers = aos_table_make(options->pool, 1);
    apr_table_set(headers, OSS_CONTENT_TYPE, "image/jpeg");
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    aos_str_set(&file, filename);
    /* Upload the object. */
    s = oss_put_object_from_file(options, &bucket, &object, &file,
                                 headers, &resp_headers);
    /* Determine whether the object is uploaded. */
    if (aos_status_is_ok(s)) {
        printf("put object from file succeeded\n");
    } else {
        printf("put object from file failed\n");
    }
    /* Release resources. */
    aos_pool_destroy(p);
}
```

Note

- If you use this upload method, the size of the object to be uploaded cannot exceed 5 GB. You can use multipart upload to upload an object whose size exceeds 5 GB.
- For the complete code, see GitHub.

Append upload

OSS supports uploads of appendable objects. When using AppendObject to upload an object, you must specify the append position of the object. If this is a new object, set the append position to 0. If this object already exists in OSS, set the append position to the object length before the append operation.

- If the object does not exist, an appendable object is created when AppendObject is called.
- If the object exists, new content is appended to the end of the object when AppendObject is called.

Append upload uploads an object by appending data. An object uploaded by using the PutObject method is a normal object.

Append data from the buffer to OSS

The following code provides an example of how to use `oss_append_object_from_buffer` to upload data from the buffer to OSS:

```
void append_object_from_buffer()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    char *str = "test oss c sdk";
    aos_status_t *s = NULL;
    int64_t position = 0;
    aos_table_t *headers1 = NULL;
    aos_table_t *headers2 = NULL;
    aos_table_t *resp_headers = NULL;
    oss_request_options_t *options = NULL;
    aos_list_t buffer;
    aos_buf_t *content = NULL;
    char *next_append_position = NULL;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    /* Initialize parameters. */
    headers1 = aos_table_make(p, 0);
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    /* Obtain the position where data starts to be appended. */
    s = oss_head_object(options, &bucket, &object, headers1, &resp_headers);
    if (aos_status_is_ok(s)) {
        next_append_position = (char*)(apr_table_get(resp_headers,
                "x-oss-next-append-position"));
```

```
        position = atoi(next_append_position);
    }
    /* Append data. */
    headers2 = aos_table_make(p, 0);
    aos_list_init(&buffer);
    content = aos_buf_pack(p, str, strlen(str));
    aos_list_add_tail(&content->node, &buffer);
    s = oss_append_object_from_buffer(options, &bucket, &object,
            position, &buffer, headers2, &resp_headers);
    /* Determine whether the data is appended. */
    if (aos_status_is_ok(s))
    {
        printf("append object from buffer succeeded\n");
    } else {
        printf("append object from buffer failed\n");
    }
    /* Release resources. */
    aos_pool_destroy(p);
}
```

Note For the complete code, see GitHub.

Append data from a local file to OSS

The following code provides an example of how to call `oss_append_object_from_file` and specify filepath to append a local file to the object is OSS:

```
void append_object_from_file()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    aos_table_t *headers1 = NULL;
    aos_table_t *headers2 = NULL;
    aos_table_t *resp_headers = NULL;
    oss_request_options_t *options = NULL;
    char *filename = __FILE__;
    aos_status_t *s = NULL;
    aos_string_t file;
    int64_t position = 0;
    char *next_append_position = NULL;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
```

```
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    /* Initialize parameters. */
    headers1 = aos_table_make(options->pool, 0);
    headers2 = aos_table_make(options->pool, 0);
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    aos_str_set(&file, filename);
    /* Obtain the position where data starts to be appended. */
    s = oss_head_object(options, &bucket, &object, headers1, &resp_headers);
    if(aos_status_is_ok(s)) {
        next_append_position = (char*)(apr_table_get(resp_headers,
                    "x-oss-next-append-position"));
        position = atoi(next_append_position);
    }
    /* Append data. */
    s = oss_append_object_from_file(options, &bucket, &object,
                            position, &file, headers2, &resp_headers);
    /* Determine whether the data is appended. */
    if (aos_status_is_ok(s)) {
        printf("append object from file succeeded\n");
    } else {
        printf("append object from file failed\n");
    }
    /* Release resources. */
    aos_pool_destroy(p);
}
```

Note

- You cannot perform AppendObject for a non-appendable object. For example, if a normal object with the same name already exists and AppendObject is still called, OSS returns a 409 error with an error code of ObjectNotAppendable.
- If you perform the PutObject operation on an existing appendable object, this appendable object is overwritten by the new object and the object type is changed to normal.
- After the HeadObject operation is performed, OSS returns x-oss-object-type. For an appendable object, the object type is Appendable. For an appendable object, after the HeadObject operation is performed, the system also returns x-oss-next-append-position and x-oss-hash-crc64ecma.
- You can neither use CopyObject to copy an appendable object nor change the server-side encryption attribute of this object. You can use CopyObject to modify the User Meta of this object.
- For the complete code, see GitHub.

Resumable upload

You may fail to upload a large object if the network is unstable or if the program stops responding. In this case, you have to upload the object again, which causes resource waste. Objects may still fail to be uploaded after multiple attempts. Resumable upload supports concurrent uploads and the uploads of objects that failed to be uploaded. You can call `oss_resumable_clt_params_t` to control the resumable upload behavior. This operation involves the following parameters:

- partSize: the size of each part to be uploaded. Valid values: 100 KB to 5 GB. Unit: ***Byte***.
- thread_num: the size of concurrent threads. Default value: *1*.
- enable_checkpoint: indicates whether to enable resumable upload. This parameter is **disabled by default**.
- checkpoint_path: the path of the *checkpoint* file. The checkpoint file and the uploaded object share the same path (*{upload_file_path}.cp*) by default.

The principle of resumable upload is to split the object you want to upload into multiple parts and upload them sequentially. When all the parts are uploaded, the upload of the entire object is completed. During the upload, the upload progress is recorded in the *checkpoint* file. The next upload attempt starts from the position recorded in the *checkpoint* file if the first upload fails. This requires that the same *checkpoint* file for the previous upload be used. The *checkpoint* file is deleted after the resumable upload is completed.

```
void resumable_upload()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    aos_string_t filename;
    aos_status_t *s = NULL;
    int is_cname = 0;
    aos_table_t *headers = NULL;
    aos_table_t *resp_headers = NULL;
    aos_list_t resp_body;
    oss_request_options_t *options = NULL;
    oss_resumable_clt_params_t *clt_params;
    aos_pool_create(&p, NULL);
    options = oss_request_options_create(p);
    init_sample_request_options(options, is_cname);
    headers = aos_table_make(p, 0);
    aos_str_set(&bucket, BUCKET_NAME);
    aos_str_set(&object, "my_key.zip");
    aos_str_set(&filename, "local_big_file.zip");
    aos_list_init(&resp_body);
    // Start resumable upload.
    clt_params = oss_create_resumable_clt_params_content(p, 1024 * 100, 3, AOS_TRUE, NULL);
    s = oss_resumable_upload_file(options, &bucket, &object, &filename, headers, NULL,
        clt_params, NULL, &resp_headers, &resp_body);
    if (aos_status_is_ok(s)) {
        printf("upload succeeded\n");
    } else {
        printf("upload failed\n");
    }
    aos_pool_destroy(p);
}
```

Note For the complete code, see GitHub.

Multipart upload

Aside from simple upload, OSS also provides multipart upload. You can use multipart upload in many scenarios. These scenarios include but are not limited to:

- Resumable upload is required.
- The file to be uploaded is larger than 100 MB.

- The OSS server is frequently disconnected due to poor network conditions.
- Streaming upload of objects is required. The size of the object to be uploaded is unknown.
- Complete multipart upload through an easy-to-use method.

  The following code provides an example of how to upload an object with multipart upload through oss_upload_file, an easy-to-use method:

```
void test_upload_file()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    oss_request_options_t *options = NULL;
    aos_status_t *s = NULL;
    int part_size = 100 * 1024;
    aos_string_t upload_id;
    aos_string_t filepath;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    aos_str_null(&upload_id);
    aos_str_set(&filepath, __FILE__);
    /* Upload the object by using multipart upload. */
    s = oss_upload_file(options, &bucket, &object, &upload_id, &filepath,
                        part_size, NULL);
    /* Determine whether the object is uploaded. */
    if (aos_status_is_ok(s)) {
        printf("upload file succeeded\n");
    } else {
        printf("upload file failed\n");
    }
    /* Release resources. */
    aos_pool_destroy(p);
}
```

> Note
>
> - When oss_upload_file is used for multipart upload of an object and the upload ID is NULL, the upload ID can be obtained through aos_str_null(&upload_id). If the specified upload ID already exists, the size of each part to be uploaded must be the same as that in the previous upload with the specified upload ID.
> - When oss_upload_file is used for multipart upload of an object, you must specify the size of each part. The size of each part must exceed 100 KB. The part number ranges from 1 to 10,000. If a part number is beyond the range during object splitting, oss_upload_file automatically adjusts the size of each part.
> - When oss_upload_file is used for multipart upload of an object, if the specified upload ID already exists, the size of each part to be uploaded must be the same as that in the previous upload with the specified upload ID.
> - For the complete code, see GitHub.

- Complete multipart upload sequentially

  The step-by-step multipart upload method is flexible. The typical process is as follows:

  i. Initialize a multipart upload task (oss_init_multipart_upload).
  ii. Upload the parts sequentially or concurrently (oss_upload_part_from_file).
  iii. Complete the upload task (oss_complete_multipart_upload).

  - Initialization

    Use the following code to initialize a multipart upload task:

```
void init_multipart_upload()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    aos_table_t *headers = NULL;
    aos_table_t *resp_headers = NULL;
    oss_request_options_t *options = NULL;
    aos_string_t upload_id;
    oss_upload_file_t *upload_file = NULL;
    aos_status_t *s = NULL;
    oss_list_upload_part_params_t *params = NULL;
    aos_list_t complete_part_list;
    oss_list_part_content_t *part_content = NULL;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    /* Initialize parameters. */
    headers = aos_table_make(p, 1);
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    /* Initialize the multipart upload task to obtain an upload ID. */
    s = oss_init_multipart_upload(options, &bucket, &object,
                                  &upload_id, headers, &resp_headers);
    /* Determine whether the multipart upload task is initialized. */
    if (aos_status_is_ok(s)) {
        printf("Init multipart upload succeeded, upload_id:%.*s\n",
            upload_id.len, upload_id.data);
    } else {
        printf("Init multipart upload failed, upload_id:%.*s\n",
            upload_id.len, upload_id.data);
    }
    /* Upload each part. You can go to the next section to access the complete code, which is omitted
here. */
    /* Complete the multipart upload. You can go to the subsequent section to access the complete c
ode, which is omitted here. */
    /* Release resources. */
    aos_pool_destroy(p);
}
```

> **Note**
>
> - The response contains upload_id, which is a unique identifier of a multipart upload task. This upload_id will be used in subsequent operations.
> - The preceding code only shows how to initialize a multipart upload task. The code is incomplete.
> - For the complete code, see GitHub.
> - The order of parameters in version 1.0.0 is as follows: ...headers, upload_id.... The order of parameters in version 2.0.0 is: ...upload_id, headers....

- Upload local parts

  Use the following code to upload parts of a local file:

```
void multipart_upload_file()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    int is_cname = 0;
    aos_table_t *headers = NULL;
    aos_table_t *complete_headers = NULL;
    aos_table_t *resp_headers = NULL;
    oss_request_options_t *options = NULL;
    aos_string_t upload_id;
    oss_upload_file_t *upload_file = NULL;
    aos_status_t *s = NULL;
    oss_list_upload_part_params_t *params = NULL;
    aos_list_t complete_part_list;
    oss_list_part_content_t *part_content = NULL;
    oss_complete_part_content_t *complete_part_content = NULL;
    int part_num1 = 1;
    int part_num2 = 2;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    /* Initialize parameters. */
    headers = aos_table_make(p, 1);
    resp_headers = aos_table_make(options->pool, 5);
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    /* Initialize the multipart upload task and obtain the upload ID. You can go back to the previous s
ection to access the complete code, which is omitted here.*/
```

```
    /* Upload the first part. */
    upload_file = oss_create_upload_file(p);
    aos_str_set(&upload_file->filename, MULTIPART_UPLOAD_FILE_PATH);
    upload_file->file_pos = 0;
    upload_file->file_last = 200 * 1024; //200k
    s = oss_upload_part_from_file(options, &bucket, &object, &upload_id,
        part_num1, upload_file, &resp_headers);
    /* Determine whether the part is uploaded. */
    if (aos_status_is_ok(s)) {
        printf("Multipart upload from file succeeded\n");
    } else {
        printf("Multipart upload from file failed\n");
    }
    /* Upload the second part. */
    upload_file->file_pos = 200 *1024;//remain content start pos
    upload_file->file_last = get_file_size(MULTIPART_UPLOAD_FILE_PATH);
    s = oss_upload_part_from_file(options, &bucket, &object, &upload_id,
        part_num2, upload_file, &resp_headers);
    /* Determine whether the part is uploaded. */
    if (aos_status_is_ok(s)) {
        printf("Multipart upload from file succeeded\n");
    } else {
        printf("Multipart upload from file failed\n");
    }
    /* Complete the multipart upload. You can go to the next section to access the complete code, wh
ich is omitted here.*/
    /* Release resources. */
    aos_pool_destroy(p);
}
```

The main idea of the preceding code is to call `oss_upload_part_from_file` to upload each part.

> **Note**
>
> - oss_upload_part_from_file requires that the size of each part, except the last one, exceed 100 KB.
> - The part number ranges from 1 to 10,000. If a part number is beyond this range, OSS returns the InvalidArgument error code.
> - When each part is uploaded, the stream is directed to the starting position of the part.
> - The preceding code only shows how to initialize a multipart upload task. The code is incomplete.
> - For the complete code, see GitHub.

- Cancel a multipart upload task

```
void abort_multipart_upload()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    aos_table_t *headers = NULL;
    aos_table_t *resp_headers = NULL;
    oss_request_options_t *options = NULL;
    aos_string_t upload_id;
    aos_status_t *s = NULL;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    /* Initialize parameters. */
    headers = aos_table_make(p, 1);
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    /* Initialize the multipart upload task to obtain an upload ID. */
    s = oss_init_multipart_upload(options, &bucket, &object,
                                  &upload_id, headers, &resp_headers);
    if (aos_status_is_ok(s)) {
        printf("Init multipart upload succeeded, upload_id:%.*s\n",
               upload_id.len, upload_id.data);
    } else {
        printf("Init multipart upload failed\n");
    }
    /* Cancel the multipart upload task. */
    s = oss_abort_multipart_upload(options, &bucket, &object, &upload_id,
                                   &resp_headers);
    /* Determine whether the multipart upload task is cancelled. */
    if (aos_status_is_ok(s)) {
        printf("Abort multipart upload succeeded, upload_id::%.*s\n",
               upload_id.len, upload_id.data);
    } else {
        printf("Abort multipart upload failed\n");
    }
    /* Release resources. */
    aos_pool_destroy(p);
}
```

Note

- When a multipart upload task is canceled, you cannot use the same upload ID to perform any operations and the uploaded parts are also deleted.
- For the complete code, see GitHub.

2.4.2.4.7. Download objects

The OSS C SDK provides a variety of object download APIs. You can download an object from OSS through any of the following methods:

- Download an object to the buffer
- Download an object to a local file
- Range download

Download an object to the buffer

You can download an object to the buffer using `oss_get_object_to_buffer`.

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *headers;
aos_table_t *params;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
aos_string_t bucket;
aos_string_t object;
aos_list_t buffer;
aos_buf_t *content;
char *buf;
int64_t len = 0;
int64_t size = 0;
int64_t pos = 0;
aos_pool_create(&p, NULL);
/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);
/* Initialize parameters. */
aos_str_set(&object, object_name);
aos_str_set(&bucket, bucket_name);
headers = aos_table_make(p, 0);
params = aos_table_make(p, 0);
/* Download the object. */
```

```
aos_list_init(&buffer);
s = oss_get_object_to_buffer(options, &bucket, &object, &buffer, headers, params, &resp_headers);
if (aos_status_is_ok(s)) {
    printf("get object succeeded\n");
    /* Copy the downloaded content to the buffer. */
    len = aos_buf_list_len(&buffer);
    buf = aos_pcalloc(p, len + 1);
    buf[len] = '\0';
    aos_list_for_each_entry(content, &buffer, node) {
    size = aos_buf_size(content);
        memcpy(buf + pos, content->pos, size);
        pos += size;
    }
} else {
    printf("get object failed\n");
}
aos_pool_destroy(p);
```

Note

- Compared with V1.0.0, V2.0.0 adds params to the oss_get_object_to_buffer API, and allows headers and params to be NULL that is not supported in V1.0.0 and earlier.
- params is also added to oss_get_object_to_buffer_by_url and oss_get_object_to_file_by_url.
- For the complete code, see GitHub.

Download an object to a local file

You can use `oss_get_object_to_file` to download an object to a specified file.

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *headers;
aos_table_t *params;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
char *filepath = "<local file path>";
aos_string_t bucket;
aos_string_t object;
aos_string_t file;
aos_pool_create(&p, NULL);
/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);
/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);
aos_str_set(&object, object_name);
aos_str_set(&file, filepath);
headers = aos_table_make(p, 0);
params = aos_table_make(p, 0);
/* Download the object. */
s = oss_get_object_to_file(options, &bucket, &object, &file, headers, params, &resp_headers);
if (aos_status_is_ok(s)) {
   printf("get object succeeded\n");
} else {
   printf("get object failed\n");
}
aos_pool_destroy(p);
```

Note

- Compared with V1.0.0, V2.0.0 adds params to the oss_get_object_to_file API, and allows the headers and params to be NULL that is not supported in V1.0.0 and earlier.
- If a local file with the same name *filepath* already exists, the local file is overwritten.
- For the complete code, see GitHub.

Range download

You can set Range to specify the transmission range and download the object in the multipart mode. The following code provides an example of how to download an object to the buffer in the multipart mode:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *headers;
aos_table_t *params;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
aos_string_t bucket;
aos_string_t object;
aos_list_t buffer;
aos_pool_create(&p, NULL);
/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);
/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);
aos_str_set(&object, object_name);
params = NULL;
headers = aos_table_make(p, 1);
/* Set Range to read the object. The range of "bytes=20-100" covers characters between the 20th and th
e 100th. */
apr_table_set(headers, "Range", "bytes=20-100");
aos_list_init(&buffer);
/* Download the object by range. */
s = oss_get_object_to_buffer(options, &bucket, &object, headers, params, &buffer, &resp_headers);
if (aos_status_is_ok(s)) {
    printf("get object succeeded\n");
} else {
    printf("get object failed\n");
}
aos_pool_destroy(p);
```

2.4.2.4.8. Manage objects

View all objects

The following code provides an example of how to use `oss_list_object` to list all objects in a bucket:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
aos_string_t bucket;
oss_list_object_params_t *params;
oss_list_object_content_t *content;
int max_ret = 1000;
char *key;
aos_pool_create(&p, NULL);
options = oss_request_options_create(p);
init_options(options);
aos_str_set(&bucket, bucket_name);
params = oss_create_list_object_params(p);
params->max_ret = max_ret;
aos_str_set(&params->prefix, "<View the object prefix.>");
aos_str_set(&params->delimiter, "<View the object delimiter.>");
aos_str_set(&params->marker, "<View the object starting position.>");
s = oss_list_object(options, &bucket, params, &resp_headers);
if (aos_status_is_ok(s)) {
   printf("get object succeeded\n");
   /* Download the object. */
   aos_list_for_each_entry(content, &params->object_list, node) {
   key = apr_psprintf(p, "%.*s", content->key.len, content->key.data);
   }
} else {
   printf("get object failed\n");
}
aos_pool_destroy(p);
```

Note If the number of objects in the bucket is greater than 1,000, only 1,000 objects are returned by default. In the response, the value of truncated is true and the value of next_marker indicates the starting position of the next read. To increase the number of returned objects, you can modify the max_ret parameter or use the marker parameter for multiple reads.

Create a simulated directory

OSS is an object-based storage service. It has no directories. The creation of a simulation directory is essentially the creation of an object with the size of 0. You can download and upload the object. The object (folder) name ends with / in the OSS console. You can use the preceding method to create a simulated directory.

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *headers;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your folder name>";
aos_string_t bucket;
aos_string_t object;
char *data = "";
aos_list_t buffer;
aos_buf_t *content;
aos_pool_create(&p, NULL);
options = oss_request_options_create(p);
init_options(options);
aos_str_set(&bucket, bucket_name);
aos_str_set(&object, object_name);
headers = aos_table_make(p, 0);
aos_list_init(&buffer);
content = aos_buf_pack(options->pool, data, strlen(data));
aos_list_add_tail(&content->node, &buffer);
s = oss_put_object_from_buffer(options, &bucket, &object, &buffer, headers, &resp_headers);
if (aos_status_is_ok(s)) {
   printf("create dir succeeded\n");
} else {
   printf("create dir failed\n");
}
aos_pool_destroy(p);
```

Note For the complete code, see GitHub.

Set the HTTP header of an object

When uploading or copying an object to OSS, you can specify certain attributes of the object in addition to the object content. The attributes are called *Object Meta*. Object Meta is stored together with its object during uploads, and returned together with its object during downloads. The following code provides an example of how to set the expiration time for an object:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *headers;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
aos_string_t bucket;
aos_string_t object;
char *data = "<object content>";
aos_list_t buffer;
aos_buf_t *content;
aos_pool_create(&p, NULL);
options = oss_request_options_create(p);
init_options(options);
aos_str_set(&object, object_name);
aos_str_set(&bucket, bucket_name);
headers = aos_table_make(p, 0);
/* Set the HTTP header. */
headers = aos_table_make(p, 1);
apr_table_set(headers, "Expires", "Fri, 28 Feb 2012 05:38:42 GMT");
/* Read data and store it in the buffer. */
aos_list_init(&buffer);
content = aos_buf_pack(options->pool, data, strlen(data));
aos_list_add_tail(&content->node, &buffer);
s = oss_put_object_from_buffer(options, &bucket, &object, &buffer, headers, &resp_headers);
if (aos_status_is_ok(s)) {
   printf("put object succeeded\n");
} else {
   printf("put object failed\n");
}
aos_pool_destroy(p);
```

Note

- The following options are available for the HTTP header: Cache-Control, Content-Disposition, Content-Encoding, and Expires. For more information about options, see RFC2616.
- For the complete code, see GitHub.

Configure the user-defined Object Meta

OSS supports the user-defined Object Meta that describes an object. Example:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *headers;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
aos_string_t bucket;
aos_string_t object;
char *data = "<object content>";
aos_list_t buffer;
aos_buf_t *content;
aos_pool_create(&p, NULL);
options = oss_request_options_create(p);
init_options(options);
aos_str_set(&bucket, bucket_name);
aos_str_set(&object, object_name);
headers = aos_table_make(p, 1);
/* Set the user-defined Object Meta. */
apr_table_set(headers, "x-oss-meta-author", "oss");
/* Upload data to OSS. */
aos_list_init(&buffer);
content = aos_buf_pack(options->pool, data, strlen(data));
aos_list_add_tail(&content->node, &buffer);
s = oss_put_object_from_buffer(options, &bucket, &object, &buffer, headers, &resp_headers);
if (aos_status_is_ok(s)) {
   printf("put object succeeded\n");
} else {
   printf("put object failed\n");
}
aos_pool_destroy(p);
```

Note

- Object Meta is stored in HTTP headers during object uploads or downloads. Therefore, Object Meta cannot contain complex characters in accordance with HTTP.
- An object may have multiple similar parameters, but the total size of the user-defined Object Meta cannot exceed 8 KB.

Obtain Object Meta

Sometimes you need to obtain Object Meta after you upload the object to OSS or before you read the object, such as the length or the object type. In this case, you can use oss_object_head to obtain Object Meta. The following code provides an example of how to obtain the object length and type information:

```
void head_object()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    oss_request_options_t *options = NULL;
    aos_table_t *headers = NULL;
    aos_table_t *resp_headers = NULL;
    aos_status_t *s = NULL;
    char *content_length_str = NULL;
    char *object_type = NULL;
    int64_t content_length = 0;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    /* Initialize parameters. */
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    headers = aos_table_make(p, 0);
    /* Obtain Object Meta. */
    s = oss_head_object(options, &bucket, &object, headers, &resp_headers);
    if (aos_status_is_ok(s)) {
        /* Obtain the object length. */
        content_length_str = (char*)apr_table_get(resp_headers, OSS_CONTENT_LENGTH);
        if (content_length_str ! = NULL) {
            content_length = atoll(content_length_str);
        }
        /* Obtain the object type. */
        object_type = (char*)apr_table_get(resp_headers, OSS_OBJECT_TYPE);
        printf("head object succeeded, object type:%s, content_length:%ld\n",
               object_type, content_length);
    } else {
        printf("head object failed\n");
    }
    aos_pool_destroy(p);
}
```

Note

- When you call the oss_head_object API, it does not download the object content, but only reads Object Meta, including the system-level and user-defined Object Meta.
- For the complete code, see GitHub.

Copy objects

Within the same region, you can copy objects that you have the permission to operate. The following code provides an example of how to use `oss_copy_object` to copy an object:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t * headers;
aos_table_t *resp_headers;
char *source_bucket_name = "<Your source bucket name>";
char *source_object_name = "<Your source object name>";
char *dest_bucket_name = "<Your destination bucket name>";
char *dest_object_name = "<Your destination object name>";
aos_string_t source_bucket;
aos_string_t source_object;
aos_string_t dest_bucket;
aos_string_t dest_object;
aos_pool_create(&p, NULL);
options = oss_request_options_create(p);
init_options(options);
aos_str_set(&source_bucket, source_bucket_name);
aos_str_set(&source_object, source_object_name);
aos_str_set(&dest_bucket, dest_bucket_name);
aos_str_set(&dest_object, dest_object_name);
headers = aos_table_make(p, 0);
/* Copy the object. */
s = oss_copy_object(options, &source_bucket, &source_object, &dest_bucket, &dest_object, headers, &re
sp_headers);
if (aos_status_is_ok(s)) {
   printf("copy object succeeded\n");
} else {
   printf("copy object failed\n");
}
aos_pool_destroy(p);
```

Note

- Note that the source and destination buckets must be in the same region.
- If an object you want to copy is larger than 1 GB, we recommend that you use multipart copy.

Copy an object in the multipart copy mode

To copy an object larger than 500 MB, we recommend that you use `oss_upload_part_copy`. The following code provides an example of how to copy an object in the multipart copy mode:

```
aos_pool_t *p;
oss_request_options_t *options;
char *source_bucket_name = "<Your source bucket name>";
char *source_object_name = "<Your source object name>";
char *dest_bucket_name = "<Your destination bucket name>";
char *dest_object_name = "<Your destination object name>";
aos_string_t dest_bucket;
aos_string_t dest_object;
aos_string_t upload_id;
aos_table_t *init_headers;
aos_table_t *copy_headers;
aos_table_t *list_part_resp_headers;
aos_table_t *complete_resp_headers
aos_table_t *resp_headers;
aos_status_t *s;
oss_list_upload_part_params_t *list_upload_part_params;
oss_upload_part_copy_params_t *upload_part_copy_params1;
aos_list_t complete_part_list;
oss_list_part_content_t *part_content;
oss_complete_part_content_t *complete_content;
int part1 = 1;
int64_t range_start1 = 0;
int64_t range_end1 = 6000000;//not less than 5MB
int max_ret = 1000;
aos_pool_create(&p, NULL);
options = oss_request_options_create(p);
init_options(options);
aos_str_set(&dest_bucket, dest_bucket_name);
aos_str_set(&dest_object, dest_object_name);
init_headers = aos_table_make(p, 0);
s = oss_init_multipart_upload(options, &dest_bucket, &dest_object, init_headers, &upload_id, &resp_hea
ders);
```

```
/* Copy the first part. */
upload_part_copy_params1 = oss_create_upload_part_copy_params(p);
aos_str_set(&upload_part_copy_params1->source_bucket, source_bucket_name);
aos_str_set(&upload_part_copy_params1->source_object, source_object_name);
aos_str_set(&upload_part_copy_params1->dest_bucket, dest_bucket_name);
aos_str_set(&upload_part_copy_params1->dest_object, dest_object_name);
aos_str_set(&upload_part_copy_params1->upload_id, upload_id->data);
upload_part_copy_params1->part_num = part1;
upload_part_copy_params1->range_start = range_start1;
upload_part_copy_params1->range_end = range_end1;
copy_headers = aos_table_make(p, 0);
s = oss_upload_part_copy(options, upload_part_copy_params1, copy_headers, &resp_headers);
if (aos_status_is_ok(s)) {
    printf("upload part copy succeeded\n");
} else {
    printf("upload part copy failed\n");
}
/* Copy the rest parts. The code is omitted here.*/
...
/* List the parts. */
list_upload_part_params = oss_create_list_upload_part_params(p);
list_upload_part_params->max_ret = max_ret;
aos_list_init(&complete_part_list);
s = oss_list_upload_part(options, &dest_bucket, &dest_object, &upload_id,
list_upload_part_params, &list_part_resp_headers);
aos_list_for_each_entry(part_content, &list_upload_part_params->part_list, node) {
  complete_content = oss_create_complete_part_content(p);
  aos_str_set(&complete_content->part_number, part_content->part_number.data);
  aos_str_set(&complete_content->etag, part_content->etag.data);
  aos_list_add_tail(&complete_content->node, &complete_part_list);
}
/* Complete the multipart copy. */
s = oss_complete_multipart_upload(options, &dest_bucket, &dest_object, &upload_id, &complete_part_lis
t, &complete_resp_headers);
if (aos_status_is_ok(s)) {
    printf("complete multipart upload succeeded\n");
} else {
    printf("complete multipart upload failed\n");
}
aos_pool_destroy(p);
```

Delete objects

The following code provides an example of how to use `oss_delete_object` to delete an object:

```
void delete_object()
{
    aos_pool_t *p = NULL;
    aos_string_t bucket;
    aos_string_t object;
    oss_request_options_t *options = NULL;
    aos_table_t *resp_headers = NULL;
    aos_status_t *s = NULL;
    aos_pool_create(&p, NULL);
    /* Create and initialize options. */
    options = oss_request_options_create(p);
    init_options(options);
    aos_str_set(&bucket, "<Your bucket name>");
    aos_str_set(&object, "<Your object name>");
    /* Delete the object. */
    s = oss_delete_object(options, &bucket, &object, &resp_headers);
    /* Determine whether the object is deleted successfully. */
    if (aos_status_is_ok(s)) {
        printf("delete object succeed\n");
    } else {
        printf("delete object failed\n");
    }
    /* Release the resources. */
    aos_pool_destroy(p);
}
```

Note For the complete code, see GitHub.

Delete multiple objects

The following code provides an example of how to use `oss_delete_objects` to delete objects and use is_quiet to specify whether the deletion result is returned:

```
aos_pool_t *p;
aos_status_t *s;
aos_table_t *resp_headers;
oss_request_options_t *options;
char *bucket_name = "<Your bucket name>";
char *object_name1 = "<Your object name 1>";
char *object_name2 = "<Your object name 2>";
aos_string_t bucket;
aos_string_t object1;
aos_string_t object2;
oss_object_key_t *content1;
oss_object_key_t *content2;
aos_list_t object_list;
aos_list_t deleted_object_list;
int is_quiet = 1;
options = oss_request_options_create(p);
init_options(options);
aos_str_set(&bucket, bucket_name);
aos_str_set(&object1, object_name1);
aos_str_set(&object2, object_name2);
/* Create a list of objects you want to delete. */
aos_list_init(&object_list);
aos_list_init(&deleted_object_list);
content1 = oss_create_oss_object_key(p);
aos_str_set(&content1->key, object_name1);
aos_list_add_tail(&content1->node, &object_list);
content2 = oss_create_oss_object_key(p);
aos_str_set(&content2->key, object_name2);
aos_list_add_tail(&content2->node, &object_list);
/* Delete multiple objects. */
s = oss_delete_objects(options, &bucket, &object_list, is_quiet, &resp_headers, &deleted_object_list);
if (aos_status_is_ok(s)) {
    printf("delete objects succeeded\n");
} else {
    printf("delete objects failed\n");
}
aos_pool_destroy(p);
```

Delete multiple objects with a specified prefix

The following code provides an example of how to use `oss_delete_objects_by_prefix` to delete objects with a specified prefix:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *prefix_str = "<Prefix of objects to be deleted>";
aos_string_t bucket;
aos_string_t prefix;
aos_pool_create(&p, NULL);
options = oss_request_options_create(p);
init_options(options);
aos_str_set(&bucket, bucket_name);
aos_str_set(&prefix, prefix_str);
/* Delete objects with the specified prefix. */
s = oss_delete_objects_by_prefix(options, &bucket, &prefix);
if (aos_status_is_ok(s)) {
   printf("delete objects by prefix succeeded\n");
} else {
   printf("delete objects by prefix failed\n");
}
aos_pool_destroy(p);
```

Note

- You can delete a directory by specifying a prefix that is used to delete objects. For example, you can delete the dir directory by setting the prefix to dir/.
- If the prefix is a null string ("") or NULL, the whole bucket is deleted. Therefore, use caution when using this function.

2.4.2.4.9. Authorized access

Use STS for temporary access authorization

OSS allows you to use Alibaba Cloud STS for temporary access authorization. To use STS, perform the following steps:

1. Create a RAM user in Apsara Stack Management Console.
2. Create an STS role in Apsara Stack Management Console and assign the RAM user the permission to play this role.
3. Use the AccessKey ID and AccessKey Secret of the RAM user to apply for a temporary token from STS.

4. Use the authentication information in the temporary token to create an OSS client.
5. Access OSS from the OSS client.

Use an STS credential to create a request with a signature

After you obtain a temporary STS credential for your client, oss_request_options is generated based on the security token and temporary Access Key (AccessKey ID and AccessKey Secret). The following code provides an example of how to upload an object:

```
aos_pool_t *p;
oss_request_options_t *options;
aos_status_t *s;
aos_table_t *headers;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
aos_string_t bucket;
aos_string_t object;
char *data = "<object content>";
aos_list_t buffer;
aos_buf_t *content;

aos_pool_create(&p, NULL);

// init_oss_request_options using sts_token
/* Create options and use the STS token to initialize options. */
options = oss_request_options_create(p);
options->config = oss_config_create(options->pool);
aos_str_set(&options->config->endpoint, "<Your endpoint>");
aos_str_set(&options->config->access_key_id, "<Your temporary AccessKey ID>");
aos_str_set(&options->config->access_key_secret, "<Your temporary AccessKey Secret>");
aos_str_set(&options->config->sts_token, "<Your sts_token>");
options->config->is_cname = 0;
options->ctl = aos_http_controller_create(options->pool, 0);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);
aos_str_set(&object, object_name);
headers = aos_table_make(p, 0);
aos_list_init(&buffer);
content = aos_buf_pack(options->pool, data, strlen(data));
aos_list_add_tail(&content->node, &buffer);

/* Upload the object. */
```

```
s = oss_put_object_from_buffer_s(options, &bucket, &object, &buffer, headers, &resp_headers);
if (aos_status_is_ok(s)) {
    printf("put object succeeded\n");
} else {
    printf("put object failed\n");
}

aos_pool_destroy(p);
```

Add a signature to a URL for authorized access

You can generate a signature and add it to a URL for temporary access. During URL generation, you can specify the URL expiration time to limit the access duration.

Generate a signature and add it to a URL

Use `oss_gen_signed_url` to generate a signature and add it to a request URL.

- Generate a signature and add it to a URL of a download request

```
aos_pool_t *p;
oss_request_options_t *options;
aos_http_request_t *req;
char *url_str;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
aos_string_t bucket;
aos_string_t object;
apr_time_t now;
int64_t expire_time;
int one_hour = 3600; /* Unit: seconds. */

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);
aos_str_set(&object, object_name);
req = aos_http_request_create(p);
req->method = HTTP_GET;
now = apr_time_now(); //millisecond
expire_time = now / 1000000 + one_hour;

/* Generate a signature and add it to the URL. */
url_str = oss_gen_signed_url(options, &bucket, &object, expire_time, req);
printf("Temporary download url:%s\n", url_str);

aos_pool_destroy(p);
```

- Generate a signature and add it to a URL of an upload request

```
aos_pool_t *p;
oss_request_options_t *options;
aos_http_request_t *req;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
aos_string_t bucket;
aos_string_t object;
apr_time_t now;
int64_t expire_time;
int one_hour = 3600;
char *url_str = NULL;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);
aos_str_set(&object, object_name);
req = aos_http_request_create(p);
req->method = HTTP_PUT;
now = apr_time_now(); //millisecond
expire_time = now / 1000000 + one_hour;

/* Generate a signature and add it to the URL. */
url_str = oss_gen_signed_url((options, &bucket, &object, expire_time, req);
printf("Temporary upload url:%s\n", url_str);

aos_pool_destroy(p);
```

- Use a URL with a signature to send a request

  You can use a URL with a signature to download an object.

```
aos_pool_t *p;
oss_request_options_t *options;
aos_http_request_t *req;
aos_table_t *headers;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
```

```
char *filepath = "<local file path>";
aos_string_t bucket;
aos_string_t object;
aos_string_t file;
char *url_str;
apr_time_t now;
int64_t expire_time;
int one_hour = 3600;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);
aos_str_set(&object, object_name);
aos_str_set(&file, filepath);
headers = aos_table_make(p, 0);
req = aos_http_request_create(p);
req->method = HTTP_GET;
now = apr_time_now(); /* Unit: microseconds. */
expire_time = now / 1000000 + one_hour;

/* Generate a signature and add it to the URL. */
url_str = oss_gen_signed_url(options, &bucket, &object, expire_time, req);

/* Use the URL with a signature to download the object. */
s = oss_get_object_to_file_by_url(options, url_str, headers, &file, &resp_headers);
if (aos_status_is_ok(s)) {
    printf("get object succeeded\n");
} else {
    printf("get object failed\n");
}
aos_pool_destroy(p);
```

- Use a URL with a signature to upload an object

```
aos_pool_t *p;
int is_oss_domain = 1;// Whether a third-level domain name is used.
oss_request_options_t *options;
```

```
aos_http_request_t *req;
aos_table_t *headers;
aos_table_t *resp_headers;
char *bucket_name = "<Your bucket name>";
char *object_name = "<Your object name>";
char *filepath = "<local file path>";
aos_string_t bucket;
aos_string_t object;
aos_string_t file;
char *url_str;
apr_time_t now;
int64_t expire_time;
int one_hour = 3600;

aos_pool_create(&p, NULL);

/* Create and initialize options. */
options = oss_request_options_create(p);
init_options(options);

/* Initialize parameters. */
aos_str_set(&bucket, bucket_name);
aos_str_set(&object, object_name);
aos_str_set(&file, filepath);
headers = aos_table_make(p, 0);
req = aos_http_request_create(p);
req->method = HTTP_PUT;
now = apr_time_now(); /* Unit: microseconds. */
expire_time = now / 1000000 + one_hour;

/* Generate a signature and add it to the URL. */
url_str = oss_gen_signed_url(options, &bucket, &object, expire_time, req);

/* Use the URL with a signature to upload the object. */
s = oss_put_object_from_file_by_url(options, url_str, &file, headers, &resp_headers);
if (aos_status_is_ok(s)) {
    printf("put objects by signed url succeeded\n");
} else {
    printf("put objects by signed url failed\n");
}

aos_pool_destroy(p);
```

2.4.2.4.10. Error handling

Exception handling

If a request error is reported when OSS C SDK is used, the corresponding error message is displayed in aos_status_s. The attributes of aos_status_s include:

- code: the HTTP status code of the failed request. Type: integer.
- error_code: the OSS error code. Type: string.
- error_msg: the OSS error message. Type: string.
- req_id: the UUID that identifies the request. If you cannot solve the problem, you can seek help from OSS development engineers based on this req_id. Type: string.

Timeout handling

- Determine a timeout
  - If code in the returned aos_status_t parameter is 5XX, the server has an internal error. You can try to send the request again.
  - If code in the returned aos_status_t parameter is not 2XX and error_code is -992 or -995, the connection or request times out. You can try to send the request again.
  - You can use aos_should_retry(aos_status_t *) in the aos_status.h file to determine whether the error code returned requires a retry. If 1 is returned, you need to try again.
- Set timeout values
  - Set the connection timeout value. The parameter setting path is as follows: options > ctl > options > connect_timeout. Unit: seconds. Default value: 10.
  - Set the DNS timeout value. The parameter setting path is as follows: options > ctl > options > dns_cache_timeout. Unit: seconds. Default value: 60.
  - Set the request timeout value:
    - Set the minimum tolerable rate. The parameter setting path is as follows: options > ctl > options > speed_limit. Unit: bytes. Default value: 1,024, which is 1 KB.
    - Set the maximum tolerable duration. The parameter setting path is as follows: options > ctl > options > speed_time. Unit: seconds. Default value: 15.
    - If the preceding default values are used, a request times out when the transmission rate has been less than 1 Kbit/s for 15 consecutive seconds.

Common error codes

Error code	Description
AccessDenied	The error message returned when the access is denied.
BucketAlreadyExists	The error message returned when the bucket exists.
BucketNotEmpty	The error message returned when the bucket is not empty.
EntityTooLarge	The error message returned when the entity is too large.

Error code	Description
EntityTooSmall	The error message returned when the entity is too small.
FileGroupTooLarge	The error message returned when the object group is too large.
FilePartNotExist	The error message returned when the object part does not exist.
FilePartStale	The error message returned when the object part has expired.
InvalidArgument	The error message returned when the parameter format is incorrect.
InvalidAccessKeyId	The error message returned when the AccessKey ID does not exist.
InvalidBucketName	The error message returned when the bucket name is invalid.
InvalidDigest	The error message returned when the digest is invalid.
InvalidObjectName	The error message returned when the object name is invalid.
InvalidPart	The error message returned when the part is invalid.
InvalidPartOrder	The error message returned when the part sequence is invalid.
InvalidTargetBucketForLogging	The error message returned when the logging operation involves an invalid target bucket.
InternalError	The error message returned when an internal error occurs in OSS.
MalformedXML	The error message returned when an XML format is invalid.
MethodNotAllowed	The error message returned when the method is not supported.
MissingArgument	The error message returned when a parameter is not specified.
MissingContentLength	The error message returned when the content length is not configured.
NoSuchBucket	The error message returned when no such bucket exists.
NoSuchKey	The error message returned when no such object exists.
NoSuchUpload	The error message returned when no such multipart upload ID exists.
NotImplemented	The error message returned when the method cannot be implemented.
PreconditionFailed	The error message returned when the preconditioning fails.

Error code	Description
RequestTimeTooSkewed	The error message returned when the duration between the request sending time and the server responding time exceeds 15 minutes.
RequestTimeout	The error message returned when the request timed out.
SignatureDoesNotMatch	The error message returned when the signature is incorrect.
TooManyBuckets	The error message returned when the number of the user's buckets exceeds the limit.

2.4.2.5. Go-SDK

2.4.2.5.1. Installation

- GitHub: https://github.com/aliyun/aliyun-oss-go-sdk
- API documentation: https://godoc.org/github.com/aliyun/aliyun-oss-go-sdk/oss

Requirements

- You have enabled Apsara Stack OSS and created an AccessKey ID and AccessKey Secret.
- If you have not activated or do not know about Apsara Stack OSS, log on to the OSS Product Homepage for details.
- If you have not created an AccessKey ID and AccessKey Secret, create them through Apsara Stack Access Key Management.
- You have installed the Go compiling and running environment. If you have not installed the Go compiling and running environment, go to Install Go to download and install the compiling and running environment. After the Go compiling and running environment is installed, you need to set the correct GOPATH variable. For more information about GOPATH, run the `go help gopath`.

Installation

Install the SDK through GitHub

- Run `go get github.com/aliyun/aliyun-oss-go-sdk/oss` to obtain the remote code package.
- Use `import "github.com/aliyun/aliyun-oss-go-sdk/oss"` to import the OSS Go SDK package.
- For the sample program, go to the sample directory in *https://github.com/aliyun/aliyun-oss-go-sdk/*.

Note

- When you use the `go get` command for installation, no prompts are displayed on the interface. The installation may take a while under poor network conditions. Be patient. If the installation times out, run the `go get` command again for installation.
- After the installation succeeds, your installation path (the first path in the GOPATH variable) contains the Go SDK library *pkg/linux_amd64/github.com/aliyun/aliyun-oss-go-sdk/oss.a*. (win is in *pkg\windows_amd64\github.com\aliyun\aliyun-oss-go-sdk\oss.a*.) The source file is in *src/github.com/aliyun/aliyun-oss-go-sdk*. If the source file does not exist, install the SDK again.

Examples

Sample project

- Copy sample files. In the installation path of the OSS Go SDK (the first path of the GOPATH variable), access the code directory of the OSS Go SDK code directory*src\github.com\aliyun\aliyun-oss-go-sdk*. Copy the sample and sample.go directories from the SDK code directory to the src directory.
- Modify the configuration items such as endpoint, AccessKey ID, AccessKey Secret, and BucketName in sample/config.go.
- Run `go run src/sample.go` in your project directory.

Sample content

You can obtain the example code of the Go SDK in the sample directory at GitHub. The following table describes the sample files in the sample program.

Sample file	Content
new_bucket.go	Shows how to initialize the client and bucket.
put_object.go	Shows how to use simple upload and resumable upload.
append_object.go	Shows how to use append upload.
get_object.go	Shows how to use stream download, range download, and resumable download.
delete_object.go	Shows methods to delete a single object and delete objects simultaneously.
copy_object.go	Shows how to use object copy and resumable copy.
list_objects.go	Shows how to list objects usage such as list by default parameters and list by specified parameters.
object_meta.go	Shows how to set and read Object Meta.
object_acl.go	Shows how to set and read the object ACL.
cname_sample.go	Shows how to use CNAME.

Sample file	Content
create_bucket.go	Shows how to create a bucket.
list_buckets.go	Shows how to list bucket such as list by default parameters and list by specified parameters.
bucket_acl.go	Shows how to read/set bucket ACL (Bucket ACL).
bucket_referer.go	Shows how to set/read/clear bucket whitelist (Bucket Referer).
bucket_logging.go	Shows how to set/read/clear bucket logs (Bucket Logging).
bucket_lifecycle.go	Shows to set/read/clear lifecycles of objects in the bucket (Bucket Lifecycle).
bucket_cors.go	Shows how to set, read, and delete the CORS configuration of a bucket.

2.4.2.5.2. Quick start

This topic describes how to use the OSS Go SDK to access OSS, such as view the bucket list and object list, and upload, download, and delete objects. To use the OSS Go SDK, you need to run `import github.com/aliyun/aliyun-oss-go-sdk/oss` to obtain the OSS package.

Initialize a client

The following code provides an example of how to initialize (or creating) a client:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}
```

> **Note**
>
> - An endpoint is a domain name used to access OSS. For example, the endpoint used to access OSS in Hangzhou is *http://oss-cn-hangzhou.aliyuncs.com*.
> - The AccessKey ID and AccessKey Secret constitute an AccessKey (AK) to access OSS.
> - We recommend that you replace the values of Endpoint, AccessKeyId and AccessKeySecret with your actual values when you run the sample project.

View a bucket list

To view a bucket list, use the Client.ListBuckets API.

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

lsRes, err := client.ListBuckets()
if err ! = nil {
    // HandleError(err)
}

for _, bucket := range lsRes.Buckets {
    fmt.Println("bucket:", bucket.Name)
}
```

Note

- The bucket name must be unique in OSS. To create a bucket, you must select a unique bucket name.

Obtain a bucket

Operations on a bucket are implemented through client methods such as create or delete a bucket, and set or disable the bucket ACL, lifecycle, and hotlinking. Operations on an object are implemented based on its bucket such as upload, download, or delete an object and set the object ACL. The following code provides an example of how to use Client.Bucket to obtain the operation handle of a specified bucket:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}
```

View objects in a bucket

The following code provides an example of how to use the Bucket.ListObjects API to view the objects in a bucket:

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

lsRes, err := bucket.ListObjects()
if err ! = nil {
    // HandleError(err)
}

for _, object := range lsRes.Objects {
    fmt.Println("Object:", object.Key)
}
```

Upload objects

The following code provides an example of how to use the Bucket.PutObjectFromFile API to upload an object:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.PutObjectFromFile("my-object", "LocalFile")
if err ! = nil {
    // HandleError(err)
}
```

LocalFile is the path to which the local file you want to upload. After the object is successfully uploaded, you can use `Bucket.ListObjects` to view the uploaded object.

Download objects

The following code provides an example of how to use Bucket.GetObject API to download an object:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.GetObjectToFile("my-object", "LocalFile")
if err ! = nil {
    // HandleError(err)
}
```

LocalFile is the path that stores the object. After the object is downloaded, you can open the object to view its content.

Delete objects

The following code provides an example of how to use Bucket.DeleteObject to delete an object from a bucket:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.DeleteObject("my-object")
if err ! = nil {
    // HandleError(err)
}
```

After an object is deleted, you can use `Bucket.ListObjects` to view whether the object has been deleted.

2.4.2.5.3. Manage buckets

A bucket is a namespace in OSS and a management entity for advanced features such as billing, access control, and access logging.

View all buckets

You can use `Client.ListBuckets` to list all buckets of the current user and specify Prefix to list buckets with a specified prefix.

> **Note** The sample code of ListBuckets is stored in `sample/list_buckets.go`.

```
import (
    "fmt"
    "github.com/aliyun/aliyun-oss-go-sdk/oss"
)

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

// List buckets. You can list a maximum of 100 by default.
lsRes, err := client.ListBuckets()
if err ! = nil {
    // HandleError(err)
}
fmt.Println("buckets:", lsRes.Buckets)

// Specify a prefix to filter buckets.
lsRes, err = client.ListBuckets(oss.Prefix("my-bucket"))
if err ! = nil {
    // HandleError(err)
}
fmt.Println("buckets:", lsRes.Buckets)
```

Create a bucket

> **Note** The sample code of CreateBucket is stored in `sample/create_bucket.go`.

The following code provides an example of how to use `Client.CreateBucket` to create a bucket with a specified bucket name:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

err = client.CreateBucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}
```

If no ACL policy is specified when a bucket is created, the default ACL oss.ACLPrivate applies. You can specify an ACL policy when creating a bucket:

```
err = client.CreateBucket("my-bucket", oss.ACL(oss.ACLPublicRead))
if err ! = nil {
    // HandleError(err)
}
```

Note The bucket name must be globally unique.

Delete a bucket

The following code provides an example of how to use `Client.DeleteBucket` to delete a specified bucket:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

err = client.DeleteBucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}
```

Note

- If the bucket you want to delete contains objects, you need to delete the objects first.
- If the bucket to be deleted has unfinished upload requests, you need to use `Bucket.ListMultipartUploads` and `Bucket.AbortMultipartUpload` to abort the requests first. For more information about the use, see API Documents.

Check whether a bucket exists

The following code provides an example of how to use `Client.IsBucketExist` to check whether a bucket of the current user exists:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

isExist, err := client.IsBucketExist("my-bucket")
if err ! = nil {
    // HandleError(err)
}
```

Bucket ACL

You can set the ACL for a bucket to allow or forbid anonymous read or write operations on the bucket.

Note For more information about the sample code for bucket ACL, see `sample/bucket_acl.go`.

View the ACL of a bucket

The following code provides an example of how to use `Client.GetBucketACL` to view the bucket ACL:

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

aclRes, err := client.GetBucketACL("my-bucket")
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Bucket ACL:", aclRes.ACL)
```

Set the ACL for a bucket

The following code provides an example of how to use `Client.SetBucketACL` to set the bucket ACL:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

err = client.SetBucketACL("my-bucket", oss.ACLPublicRead)
if err ! = nil {
    // HandleError(err)
}
```

Note Bucket ACLs are classified into three types: private, public-read, and public-read-write, corresponding to the ACLPrivate, ACLPublicRead, and ACLPublicReadWrite constant parameters of the Go SDK, respectively.

2.4.2.5.4. Upload objects

The OSS Go SDK provides a variety of object upload APIs. You can upload an object to OSS through any of the following methods:

- Simple upload (PutObject), applicable to small objects
- Multipart upload (UploadFile), applicable to large objects
- Append upload (AppendObject)

Simple upload

- Upload data read from a data stream (io.Reader)

  You can use Bucket.PutObject to upload an object in a simple operation.

  > **Note** For the sample code of simple upload, see `sample/put_object.go`.

  - String upload

```
import "strings"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.PutObject("my-object", strings.NewReader("MyObjectValue"))
if err ! = nil {
    // HandleError(err)
}
```

- Byte array upload

```
import "bytes"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.PutObject("my-object", bytes.NewReader([]byte("MyObjectValue")))
if err ! = nil {
    // HandleError(err)
}
```

- Object stream upload

```
import "os"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

fd, err := os.Open("LocalFile")
if err ! = nil {
    // HandleError(err)
}
defer fd.Close()

err = bucket.PutObject("my-object", fd)
if err ! = nil {
    // HandleError(err)
}
```

- Upload a specified local file

  The following code provides an example of how to use Bucket.PutObjectFromFile to upload a specified local file and use the content of the local file as the object value:

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.PutObjectFromFile("my-object", "LocalFile")
if err ! = nil {
    // HandleError(err)
}
```

Note When you upload an object using the preceding method, ensure that the object size does not exceed 5 GB. To upload an object larger than 5 GB, use multipart upload.

- Specify Object Meta during upload

  When using a data stream to upload an object, you can specify Object Meta of one or more objects. The name of the metadata is case-insensitive. For instance, when you upload an object and define the metadata as name, and use Bucket.GetObjectDetailedMeta to access the object, X-Oss-Meta-Name is displayed as the result. Ignore case sensitivity during comparison or reading.

  The following table describes the Object Meta information that can be specified.

Name	Description
CacheControl	The Webpage caching behavior specified when the object is downloaded.
ContentDisposition	The name of an object during the download.
ContentEncoding	The content encoding type of an object during the download.
Expires	The expiration time. You can customize the expiration time format. We recommend that you use the http.TimeFormat.
ServerSideEncryption	The encryption algorithm that OSS uses to encrypt an object when the object is created. Valid value: AES256.
ObjectACL	The access permission granted by OSS for an object when the object is created.
Meta	Specifies the custom Object Meta, with X-Oss-Meta- as the prefix.

```
import (
    "strings"
    "time"
    "github.com/aliyun/aliyun-oss-go-sdk/oss"
)

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

expires := time.Date(2049, time.January, 10, 23, 0, 0, 0, time.UTC)
options := []oss.Option{
    oss.Expires(expires),
    oss.ObjectACL(oss.ACLPublicRead),
    oss.Meta("MyProp", "MyPropVal"),
}
err = bucket.PutObject("my-object", strings.NewReader("MyObjectValue"), options...)
if err ! = nil {
    // HandleError(err)
}
```

Note You can set Object Meta for Bucket.PutObject, Bucket.PutObjectFromFile, Bucket.UploadFile, and Bucket.UploadFile during object uploading.

- Create a simulated folder

  OSS does not use folders. All elements are stored as objects. However, you can use the following code to create simulated folders:

```
import "strings"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.PutObject("my-dir/", strings.NewReader(""))
if err ! = nil {
    // HandleError(err)
}
```

Note

- Creating a simulation folder means creating an empty object.
- You can download and upload the object. The object (folder) name ends with / in the OSS console.
- Therefore, you can create a simulated folder by using the preceding method.

Append upload

OSS allows you to use `Bucket.AppendObject` to upload appendable objects. When using this API to upload an object, you need to specify the append position of the object. If this is a new object, set the append position to 0. If this object already exists in OSS, set the append position to the object length before the append operation.

- If the object does not exists, an appendable object is created when `AppendObject` is called.
- If the object exists, new content is appended to the end of `AppendObject` .

Note For the sample code of append upload, see `sample/append_object.go` .

```
import "strings"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

var nextPos int64 = 0
// If the object is appended for the first time, the append position is 0, and the returned value is the p
osition for the next append.
nextPos, err = bucket.AppendObject("my-object", strings.NewReader("YourObjectValue"), nextPos)
if err ! = nil {
    // HandleError(err)
}

// Start the second append.
nextPos, err = bucket.AppendObject("my-object", strings.NewReader("YourObjectValue"), nextPos)
if err ! = nil {
    // HandleError(err)
}

// You can append content to an object multiple times.
```

Note

- You can append content to appendable object (objects created with `AppendObject`) only.
- You cannot copy oppendable objects.

When uploading a new object (the append position is 0), you can specify Object Meta. You are no longer be allowed to specify Object Meta in subsequent append upload operations on this object.

```
    // Specify Object Meta of a new object when uploading it.
    nextPos, err = bucket.AppendObject("my-object", strings.NewReader("YourObjectValue"), 0, oss.Meta(
"MyProp", "MyPropVal"))
    if err ! = nil {
        // HandleError(err)
    }
```

Multipart upload

You may fail to upload a large object if the network is unstable or the program crashes. In this scenario, you have to upload the object again, which is a waste of resources. If the network is unstable, you may need to try multiple times. You can use `Bucket.UploadFile` to achieve resumable upload. This API contains the following parameters:

- objectKey: the name of the object to be uploaded to OSS.
- filePath: the local path of the object you want to upload.
- partSize: the size of each part to be uploaded. The size ranges from 100 KB to 5 GB. The unit is byte.
- options: the optional items, including:
  - Routines: the number of concurrent uploads. The default value is 1, indicating no concurrent uploads.
  - Checkpoint: specifies whether resumable upload is enabled and the path of the checkpoint object. Resumable upload is disabled by default. You can set the path to the checkpoint object to null. If null is set, the *file.cp* file in the local directory is used for the path. *file* is the local file name.
  - For other metadata information, see Specify Object Meta during upload.

The principle is to split the object you want to upload into multiple parts and upload them sequentially. When all the parts are uploaded, the upload of the entire object is completed. The upload progress information is recorded during the upload process in the checkpoint object. If the upload of any part fails, the next upload starts from the recorded position in the checkpoint object. This requires that the same checkpoint object for the previous upload be used. be used in the next call. The checkpoint object is deleted after resumable upload is completed.

> **Note** For the sample code of multipart upload, see `sample/put_object.go`.

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

// The part size is 100 KB. Parts are uploaded through three coroutines concurrently. Resumable uploa
d is used.
err = bucket.UploadFile("my-object", "LocalFile", 100*1024, oss.Routines(3), oss.Checkpoint(true, ""))
if err ! = nil {
    // HandleError(err)
}
```

Note

- The SDK records the upload intermediate states in the cp object. Make sure that you have the write permission on the cp object.
- The cp object records the upload intermediate state information and has a checksum. This object cannot be edited. If this object is damaged, all parts need to be re-uploaded. When all parts are uploaded, the cp object is deleted.
- If the local file is modified during the upload, all parts are re-uploaded.
- You can use *oss.Checkpoint(true, "your-cp-file.cp")* as the path that stores the checkpoint object for resumable upload information.
- Use *bucket.UploadFile(objectKey, localFile, 100*1024)*. The multipart upload and resumable upload are not used by default.

- Obtain the information about all uploaded parts

  The following code provides an example of how to use Bucket.ListUploadedParts to obtain the uploaded parts of an object:

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

imur, err := bucket.InitiateMultipartUpload("my-object")
if err ! = nil {
    // HandleError(err)
}

lsRes, err := bucket.ListUploadedParts(imur)
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Parts:", lsRes.UploadedParts)
```

- Obtain all MultipartUpload tasks

  You can use `Bucket.ListMultipartUploads` to list all multipart upload tasks. The following table describes typical parameters.

Parameter	Description
Delimiter	The delimiter used to group objects by name. CommonPrefixes specify a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter.
MaxUploads	The maximum number of MultipartUpload tasks returned for one request. The default value is 1,000. The max-uploads value cannot exceed 1,000.
KeyMarker	The starting position of the MultipartUpload task list in the response. All the MultipartUpload tasks whose object names start with a letter that comes after the KeyMarker value in the alphabetic order are listed.
Prefix	The prefix that the names of returned objects must contain. Note that the object names returned for a query by the Prefix parameter still contain the specified prefix.

- Run the following code to list MultipartUpload tasks by using default parameter values:

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

lsRes, err := bucket.ListMultipartUploads()
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Uploads:", lsRes.Uploads)
```

- Run the following code to list MultipartUpload tasks with a specified prefix:

```
lsRes, err := bucket.ListMultipartUploads(oss.Prefix("my-object-"))
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Uploads:", lsRes.Uploads)
```

- Run the following code to list 100 (maximum) MultipartUpload tasks simultaneously:

```
lsRes, err := bucket.ListMultipartUploads(oss.MaxUploads(100))
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Uploads:", lsRes.Uploads)
```

- Run the following code to list MultipartUpload tasks (maximum) with a specified prefix:

```
lsRes, err := bucket.ListMultipartUploads(oss.Prefix("my-object-"), oss.MaxUploads(100))
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Uploads:", lsRes.Uploads)
```

2.4.2.5.5. Download objects

The OSS Go SDK provides a variety of object download APIs. You can download an object from OSS through any of the following methods:

- Download to the io.ReadCloser stream
- Download an object to a local file
- Multipart download

Download to the io.ReadCloser stream

Note You can obtain the example code for object downloads in `sample/get_object.go`.

- Download an object to a stream

```
import (
    "fmt"
    "io/ioutil"
    "github.com/aliyun/aliyun-oss-go-sdk/oss"
)

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

body, err := bucket.GetObject("my-object")
if err ! = nil {
    // HandleError(err)
}
data, err := ioutil.ReadAll(body)
if err ! = nil {
    // HandleError(err)
}
body.Close()
fmt.Println("data:", string(data))
```

Note After io.ReadCloser reads the data, you need to call the Close method to disable it.

- Download an object to the local buffer

```
import (
    "bytes"
    "io"
    "github.com/aliyun/aliyun-oss-go-sdk/oss"
)

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

body, err := bucket.GetObject("my-object")
if err ! = nil {
    // HandleError(err)
}
buf := new(bytes.Buffer)
io.Copy(buf, body)
body.Close()
```

- Download an object to a local object stream

```
import (
    "io"
    "os"
    "github.com/aliyun/aliyun-oss-go-sdk/oss"
)

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

body, err := bucket.GetObject("my-object")
if err ! = nil {
    // HandleError(err)
}
defer body.Close()

fd, err := os.OpenFile("LocalFile", os.O_WRONLY|os.O_CREATE, 0660)
if err ! = nil {
    // HandleError(err)
}
defer fd.Close()

io.Copy(fd, body)
```

Download an object to a local file

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.GetObjectToFile("my-object", "LocalFile")
if err ! = nil {
    // HandleError(err)
}
```

Multipart download

You may fail to download a large object if the network is unstable or the program crashes. In this case, you have to download the object again, which is a waste of resources. If the network is unstable, you may need to retry multiple times. You can use `Bucket.DownloadFile` to enable resumable download. The API has the following parameters:

- objectKey: the name of the object you want to download.
- filePath: the local file path to which the object is downloaded.
- partSize: the size of each part you want to download, in bytes. The size ranges from 1 B to 5 GB.
- options: the optional items, including:
  - Routines: the number of concurrent downloads. The default value is 1, indicating no concurrent downloads.
  - Checkpoint: specifies whether resumable download is enabled and the path of the checkpoint object. Resuamble download is disabled by default. You can set the path to the checkpoint object to null. If the path is not specified, the checkpoint object shares the directory with *file.cp*. *file* is the local file name.
  - For more information about download conditions, see Conditional download

The principle is to split the object you want to download into multiple parts and download them sequentially. When all parts are downloaded, the download of the entire object is completed. During the download, the download progress (recorded in the checkpoint object) and the downloaded parts are recorded. If a part fails to be downloaded, the next downloaded continues from the position recorded in the checkpoint object. This requires that the same checkpoint object for the previous download be used in the next invocation. The checkpoint object is deleted after the resumable download is completed.

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.DownloadFile("my-object", "LocalFile", 100*1024, oss.Routines(3), oss.Checkpoint(true, ""))
if err ! = nil {
    // HandleError(err)
}
```

Note

- The SDK records the download intermediate states in the cp object. Make sure that you have the write permission on the cp object.
- The cp object records the download intermediate state information and contains a checksum. You cannot edit this object. If the cp object is damaged, you need to download all parts again.
- If the object being downloaded is modified (the ETag value of the object changes) or parts are missing or modified, you need to download the entire object again.
- You can use *oss.Checkpoint(true, "your-cp-file.cp")* to store checkpoint objects during resumable download.
- Use *bucket.DownloadFile(objectKey, localFile, 100*1024)*. The multipart download and resumable download are disabled by default.

Conditional download

You can specify one or more conditions for downloading an object. The object can be downloaded only when all specified conditions are met. Otherwise, an error is returned and the object cannot be downloaded. The following table describes the available download conditions.

Name	Description
IfModifiedSince	The object download condition. If the specified time is earlier than the actual object modification time, the object can be downloaded. Otherwise, an error is returned.

Name	Description
IfUnmodifiedSince	The object download condition. If the specified time is equal to or later than the actual object modification time, the object can be downloaded. Otherwise, an error is returned.
IfMatch	The object download condition. If the ETag value of the source object is equal to the ETag value specified in the request, the object can be downloaded. Otherwise, an error is returned.
IfNoneMatch	The object download condition. If the ETag value of the source object is not equal to the ETag value specified in the request, the object can be downloaded. Otherwise, an error is returned.

```
import "time"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

date := time.Date(2015, time.November, 10, 23, 0, 0, 0, time.UTC)

// You cannot download the object if conditions are not met.
err = bucket.GetObjectToFile("my-object", "LocalFile", oss.IfModifiedSince(date))
if err == nil {
    // HandleError(err)
}

// You can download the object if conditions are met.
err = bucket.GetObjectToFile("my-object", "LocalFile", oss.IfUnmodifiedSince(date))
if err ! = nil {
    // HandleError(err)
}
```

> Note
>
> - To obtain the ETag value, use the Bucket.GetObjectDetailedMeta API.
> - You can specify conditions for the Bucket.GetObject, Bucket.GetObjectToFile, and Bucket.DownloadFile APIs.

Download a compressed object

You can download a compressed object. Currently, GZIP is supported for object compression. The Bucket.GetObject and Bucket.GetObjectToFile APIs support the download of compressed objects.

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.GetObjectToFile("my-object.txt", "LocalFile.gzip", oss.AcceptEncoding("gzip"))
if err ! = nil {
    // HandleError(err)
}
```

2.4.2.5.6. Manage objects

A bucket can contain a lot of objects. The SDK provides a series of APIs for you to conveniently manage the objects.

List objects in a bucket

You can use `Bucket.ListObjects` to list all objects in the current bucket. The following table describes typical parameters.

Parameter	Description
Delimiter	The delimiter used to group objects by name. CommonPrefixes specify a set of substrings of objects whose names share a specified prefix and end with the first specified delimiter.
Prefix	The prefix that must be contained in the names (key) of the returned objects. Note that if you use a prefix to make a query, the returned key values still contain the prefix.

Parameter	Description
MaxKeys	The maximum number of objects returned for one request. If this parameter is not specified, the default value 100 is used. The maximum value cannot exceed 1,000.
Marker	The starting position of the object list. Objects are sorted in the alphabetical order and those objects following this marker are listed.

Note The example code of ListObjects is stored in `sample/list_objects.go`.

- You can obtain the object list of a bucket by using the default parameters. The first 100 objects are returned by default.

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

lsRes, err := bucket.ListObjects()
if err ! = nil {
    // HandleError(err)
}

fmt.Println("Objects:", lsRes.Objects)
```

- You can specify the maximum number of objects that can be returned. A maximum of 1,000 objects can be returned.

```
lsRes, err := bucket.ListObjects(oss.MaxKeys(200))
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Objects:", lsRes.Objects)
```

- You can specify the prefix of objects to be returned. A maximum of 100 objects can be returned by default.

```
lsRes, err := bucket.ListObjects(oss.Prefix("my-object-"))
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Objects:", lsRes.Objects)
```

- You can specify the maximum number of objects that can be returned after a specified object. A maximum of 100 objects can be returned by default.

```
lsRes, err := bucket.ListObjects(oss.Marker("my-object-xx"))
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Objects:", lsRes.Objects)
```

- You can list all objects by page and set the maximum number of objects that can be returned each time to 200.

```
marker := oss.Marker("")
for {
    lsRes, err := bucket.ListObjects(oss.MaxKeys(200), marker)
    if err ! = nil {
        HandleError(err)
    }
    marker = oss.Marker(lsRes.NextMarker)

    fmt.Println("Objects:", lsRes.Objects)

    if ! lsRes.IsTruncated {
        break
    }
}
```

- You can list all objects after a specific object by page and set the maximum number of objects that can be returned each time to 50.

```
marker = oss.Marker("my-object-xx")
for {
    lsRes, err := bucket.ListObjects(oss.MaxKeys(50), marker)
    if err ! = nil {
        // HandleError(err)
    }

    marker = oss.Marker(lsRes.NextMarker)

    fmt.Println("Objects:", lsRes.Objects)

    if ! lsRes.IsTruncated {
        break
    }
}
```

- You can list all objects with a specified prefix by page and set the maximum number of objects that can be returned each time to 80.

```
prefix := oss.Prefix("my-object-")
marker := oss.Marker("")
for {
    lsRes, err := bucket.ListObjects(oss.MaxKeys(80), marker, prefix)
    if err ! = nil {
        // HandleError(err)
    }

    prefix = oss.Prefix(lsRes.Prefix)
    marker = oss.Marker(lsRes.NextMarker)

    fmt.Println("Objects:", lsRes.Objects)

    if ! lsRes.IsTruncated {
        break
    }
}
```

- Simulate the directory structure

  OSS is an object-based storage service. It has no directories. All objects stored in a bucket are uniquely identified by object key. The structure is not hierarchical. This structure makes OSS storage highly efficient. However, users want to be able to put objects into different directories when managing the objects, just like they do in a traditional file system. To this end, OSS provides a CommonPrefix feature to facilitate simulating a directory structure.

Assume that a bucket contains the following objects:

```
foo/x
foo/y
foo/bar/a
foo/bar/b
foo/hello/C/1
foo/hello/C/2
```

To list all the objects and subdirectories in a specified directory, use the ListObjects API.

```
lsRes, err := bucket.ListObjects(oss.Prefix("foo/"), oss.Delimiter("/"))
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Objects:", lsRes.Objects,"SubDir:", lsRes.CommonPrefixes)
```

In the response, lsRes.Objects indicates objects, including foo/x and foo/y, and lsRes.CommonPrefixes indicates subdirectories, including foo/bar/ and foo/hello/.

Determine whether a specified object exists

You can use `Bucket.IsObjectExist` to determine whether an object exists.

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

isExist, err := bucket.IsObjectExist("my-object")
if err ! = nil {
    // HandleError(err)
}
```

Delete an object

You can use `Bucket.DeleteObject` to delete an object.

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

err = bucket.DeleteObject("my-object")
if err ! = nil {
    // HandleError(err)
}
```

Delete multiple objects

You can use `Bucket.DeleteObjects` to delete multiple objects and specify DeleteObjectsQuiet to determine whether the result of the delete operation is returned. The deletion results are returned by default.

> **Note** For more information about the sample code for deleting objects, see sample/delete_object.go.

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

// The results of successfully deleted objects are returned by default.
delRes, err := bucket.DeleteObjects([]string{"my-object-1", "my-object-2"})
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Deleted Objects:", delRes.DeletedObjects)

// The deletion results are not returned.
_, err = bucket.DeleteObjects([]string{"my-object-3", "my-object-4"},
    oss.DeleteObjectsQuiet(true))
if err ! = nil {
    // HandleError(err)
}
```

Note

- If you use Bucket.DeleteObjects, you must specify at least one ObjectKey because it cannot be left unspecified.
- Bucket.DeleteObjects uses the XML package of Go in compliance with XML1.0. Do not use the features that XML1.0 does not support.

Obtain Object Meta

When uploading or copying an object to OSS, you can specify certain attributes of the object in addition to the object content. The attributes are called Object Meta. Object Meta is stored together with its object during uploads, and returned together with its object during downloads.

The object metadata in the SDK is indicated by Map. Other keys and values are of the string type, and **only contain simple characters visible to ASCII and cannot contain line breaks** The total size of Object Meta cannot exceed 8 KB.

Note

- Object Meta is stored in HTTP headers during object uploads or downloads. Therefore, Object Meta cannot contain complex characters in accordance with HTTP.
- The name of Object Meta is case-insensitive. The case sensitivity can be ignored during compare or read operations.

To obtain Object Meta of an object, use the Bucket.GetObjectDetailedMeta API.

Note For more information about the sample code for Object Meta, see sample/object_meta.go.

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

props, err := bucket.GetObjectDetailedMeta("my-object")
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Object Meta:", props)
```

Note The results returned through Bucket.GetObjectMeta exclude the ACL of the object. To obtain the ACL of an object, use the Bucket.GetObjectACL API.

Modify Object Meta

You can modify one or more pieces of Object Meta at a time. The following table describes the available Object Meta for an object.

Object Meta	Description
CacheControl	The Webpage caching behavior specified when the new object is downloaded.

Object Meta	Description
ContentDisposition	The object name specified when the new object is downloaded.
ContentEncoding	The content encoding format specified when the new object is downloaded.
Expires	The expiration time of the object. We recommend that you use the GMT format.
Meta	Specifies the custom Object Meta, with X-Oss-Meta- as the prefix.

To set Object Meta of an object, use the Bucket.SetObjectMeta API.

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

// Modify one piece of Object Meta at a time.
err = bucket.SetObjectMeta("my-object", oss.Meta("MyMeta", "MyMetaValue"))
if err ! = nil {
    // HandleError(err)
}

// Modify multiple pieces of Object Meta.
options := []oss.Option{
    oss.Meta("MyMeta", "MyMetaValue"),
    oss.Meta("MyObjectLocation", "HangZhou"),
}
err = bucket.SetObjectMeta("my-object", options...)
if err ! = nil {
    // HandleError(err)
}
```

Copy objects

You can use `Bucket.CopyObject` to copy objects within the same bucket and use `Bucket.CopyObjectToBucket` to copy objects to another bucket.

> **Note** For more information about the sample code for object copy, see sample/copy_objects.go.

- Copy an object within the same bucket

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

_, err = bucket.CopyObject("my-object", "descObjectKey")
if err ! = nil {
    // HandleError(err)
}
```

- Copy an object to another bucket

```
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

_, err = bucket.CopyObjectToBucket("my-object", "my-bucket-desc", "descObjectKey")
if err ! = nil {
    // HandleError(err)
}
```

- Process Object Meta during copy

  You can use MetadataDirective to process Object Meta in two ways during object copy (CopyObject/CopyObjectToBucket):

  - oss.MetaCopy: copies Object Meta of the source object.
  - oss.MetaReplace: overwrites the source Object Meta with the new Object Meta.

  The default value is oss.MetaCopy.

  When MetadataDirective is set to MetaReplace during copy, you can specify Object Meta of the new object, as described in the following table.

Object Meta	Description
CacheControl	The Webpage caching behavior specified when the new object is downloaded.
ContentDisposition	The object name specified when the new object is downloaded.
ContentEncoding	The content encoding format specified when the new object is downloaded.
Expires	The expiration time (in seconds) of the new object. For more information, see RFC2616.
ServerSideEncryption	The encryption algorithm that OSS uses to encrypt an object when the object is created.
ObjectACL	The ACL set when a new object is created in OSS.

Object Meta	Description
Meta	Specifies the custom Object Meta, with X-Oss-Meta- as the prefix.

```
import (
    "time"
    "github.com/aliyun/aliyun-oss-go-sdk/oss"
)

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

expires := time.Date(2049, time.January, 10, 23, 0, 0, 0, time.UTC)
options := []oss.Option{
    oss.MetadataDirective(oss.MetaReplace),
    oss.Expires(expires),
    oss.ObjectACL(oss.ACLPublicRead),
    oss.Meta("MyMeta", "MyMetaValue")}

_, err = bucket.CopyObject("my-object", "descObjectKey", options...)
if err ! = nil {
    // HandleError(err)
}
```

- Specify copy conditions

  You can specify conditions for object copy. An object can be copied only when the specified conditions are met. Otherwise, OSS returns an error and the object is not copied. The following table describes the available copy conditions.

Parameter	Description
CopySourceIfMatch	If the ETag value of the source object is equal to the ETag value specified in the request, OSS copies the object. Otherwise, OSS returns an error.

Parameter	Description
CopySourceIfNoneMatch	If the ETag value of the source object is not equal to the ETag value specified in the request, OSS copies the object. Otherwise, OSS returns an error.
CopySourceIfModifiedSince	If the specified time is equal to or later than the actual modification time of the source object, OSS copies the object. Otherwise, OSS returns an error.
CopySourceIfUnmodifiedSince	If the source object has been modified since the time specified in the request, OSS copies the object. Otherwise, OSS returns an error.

```
import (
    "fmt"
    "time"
    "github.com/aliyun/aliyun-oss-go-sdk/oss"
)

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

date := time.Date(2015, time.November, 10, 23, 0, 0, 0, time.UTC)
// Specify that the object is not copied because the condition is not met.
_, err = bucket.CopyObject("my-object", "descObjectKey", oss.CopySourceIfModifiedSince(date))
fmt.Println("CopyObjectError:", err)

// Specify that the object is copied because the condition is met.
_, err = bucket.CopyObject("my-object", "descObjectKey", oss.CopySourceIfUnmodifiedSince(date))
if err ! = nil {
    // HandleError(err)
}
```

Note Both Bucket.CopyObject and Bucket.CopyObjectToBucket can be used to process Object Meta and specify copy conditions during object copy.

2.4.2.5.7. Set ACLs

OSS allows you to set ACLs for buckets and objects separately, so that you can conveniently control how your resources are accessed. Three permissions included in the ACL are available for a bucket:

- public-read-write: Anonymous users are allowed to create, obtain, and delete objects in the bucket.
- public-read: Only the owner or authorized user of an object has the read and write permissions on the object, and other users (including anonymous users) have only read permissions on the object.
- private: Only the owner or authorized user has the read and write permissions on the object. A signature is required for anonymous access requests.

When a bucket is created, the ACL is set to Private by default. You can also use `Client.SetBucketACL` to set the bucket ACL. The preceding three permissions included in the ACL correspond to the constant parameters (ACLPublicReadWrite, ACLPublicRead, and ACLPrivate) of the Go SDK.

Bucket ACL

Note For more information about the sample code for bucket ACL configurations, see sample/bucket_acl.go.

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

// Set the ACL for a bucket.
err = client.SetBucketACL("my-bucket", oss.ACLPublicRead)
if err ! = nil {
    // HandleError(err)
}

// View the ACL of the bucket.
aclRes, err := client.GetBucketACL("my-bucket")
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Bucket ACL:", aclRes.ACL)
```

Object ACL

Four permissions included in ACLs are available for an object:

- default: The object inherits the ACL of the bucket to which it belongs. In other words, the ACL configuration of the object is the same as that of the bucket where the object is stored.
- Public-read-write: All users of an object have the read and write permissions on the object.
- public-read: Only the owner or authorized user of an object has the read and write permissions on the object. Other users (including anonymous users) have only read permissions on the object.
- private: Only the owner or authorized user has the read and write permissions on the object. A signature is required for anonymous access requests.

When you create an object, the default ACL is set. You can also use `Bucket.SetObjectACL` to set the object ACL. The preceding four permissions included in the ACL correspond to the constant parameters (ACLDefault, ACLPublicReadWrite, ACLPublicRead, and ACLPrivate) of the Go SDK.

> **Note** For the sample code for object ACL configurations, see sample/object_acl.go.

```
import "fmt"
import "github.com/aliyun/aliyun-oss-go-sdk/oss"

client, err := oss.New("Endpoint", "AccessKeyId", "AccessKeySecret")
if err ! = nil {
    // HandleError(err)
}

bucket, err := client.Bucket("my-bucket")
if err ! = nil {
    // HandleError(err)
}

// Set the ACL for an object.
err = bucket.SetObjectACL("my-object", oss.ACLPrivate)
if err ! = nil {
    // HandleError(err)
}

// View the ACL of the object.
aclRes, err := bucket.GetObjectACL("my-object")
if err ! = nil {
    // HandleError(err)
}
fmt.Println("Object ACL:", aclRes.ACL)
```

Note

- If the ACL of an object is set (not default), OSS preferentially authenticates the object ACL when the object is accessed, and ignores the bucket ACL.
- If anonymous access is allowed (where public-read or public-read-write is set for an object), you can use a Web browser to directly access the object, such as *http://bucket-name.oss-cn-hangzhou.aliyuncs.com/object.jpg*.

2.4.2.5.8. Troubleshooting

A unified API is returned if errors occur when the Go SDK is called. The unified API is defined as follows:

```
type error interface {
    Error() string
}
```

Other specific errors such as a timeout are further defined based on this error API. For example, HTTP request errors are returned as follows:

```
//net.Error
type Error interface {
    error
    Timeout() bool   // Is the error a timeout
    Temporary() bool // Is the error temporary
}
```

If the request errors occur when the OSS Go SDK is used, corresponding errors are returned. If HTTP request errors and I/O errors occur, errors preset in Go are returned. If an error occurs when the OSS server processes a request, the following error is returned, which is an implementation of the error API:

```
type ServiceError struct {
    Code      string    // The error code returned by OSS to a user.
    Message   string    // The error details provided by OSS.
    RequestId string    // The UUID that uniquely identifies the request.
    HostId    string    // The host ID that identifies the accessed OSS cluster.
    StatusCode int      // The HTTP status code.
}
```

If the HTTP status code returned by OSS is not as expected, the following error is returned, which is also an implementation of the error API:

```
type UnexpectedStatusCodeError struct {
    allowed []int    // The expected HTTP status code returned by OSS.
    got     int      // The actual HTTP status code returned by OSS.
}
```

OSS error codes

The following table describes the OSS error codes.

Error code	Description	HTTP status code
AccessDenied	The error message returned because access is denied.	403
BucketAlreadyExists	The error message returned because the bucket already exists.	409
BucketNotEmpty	The error message returned because the bucket is not empty.	409
EntityTooLarge	The error message returned because the entity is too large.	400
EntityTooSmall	The error message returned because the entity is too small.	400
FileGroupTooLarge	The error message returned because the object group is too large.	400
InvalidLinkName	The error message returned because the object to which the object link is linked already exists.	400
LinkPartNotExist	The error message returned because the object to which the object link is linked does not exist.	400
ObjectLinkTooLarge	The error message returned because the object link has too many objects.	400
FieldItemTooLong	The error message returned because the total length of all form fields in the post request exceeds the limit.	400
FilePartInterity	The error message returned because the object part has changed.	400

Error code	Description	HTTP status code
FilePartNotExist	The error message returned because the object part does not exist.	400
FilePartStale	The error message returned because the object part has expired.	400
IncorrectNumberOfFilesInPOSTRequest	The error message returned because the number of objects in the post request is incorrect.	400
InvalidArgument	The error message returned because the parameter format is invalid.	400
InvalidAccessKeyId	The error message returned when because AccessKey ID does not exist.	403
InvalidBucketName	The error message returned because the bucket name is invalid.	400
InvalidDigest	The error message returned because the digest is invalid.	400
InvalidEncryptionAlgorithmError	The error message returned because the specified encryption algorithm (entropy) is invalid.	400
InvalidObjectName	The error message returned because the object name is invalid.	400
InvalidPart	The error message returned because the part is invalid.	400
InvalidPartOrder	The error message returned because the part sequence is invalid.	400
InvalidPolicyDocument	The error message returned because the policy document is invalid.	400
InvalidTargetBucketForLogging	The error message returned because the destination bucket specified for access logging is invalid.	400

Error code	Description	HTTP status code
InternalError	The error message returned because an internal OSS error occurs.	500
MalformedXML	The error message returned because the XML format is invalid.	400
MalformedPOSTRequest	The error message returned because the format of the POST request body is invalid.	400
MaxPOSTPreDataLengthExceededError	The error message returned because the POST request body, excluding the object content uploaded, is too large.	400
MethodNotAllowed	The error message returned because the method is not supported.	405
MissingArgument	The error message returned because a required parameter is not specified.	411
MissingContentLength	The error message returned because the content length is not specified.	411
NoSuchBucket	The error message returned because no such bucket exists.	404
NoSuchKey	The error message returned because no such key exists.	404
NoSuchUpload	The error message returned because no such multipart upload ID exists.	404
NotImplemented	The error message returned because the method cannot be implemented.	501
PreconditionFailed	The error message returned because a precondition error occurs.	412
RequestTimeTooSkewed	The error message returned because the duration between the request sending time and the server responding time exceeds 15 minutes.	403

Error code	Description	HTTP status code
RequestTimeout	The error message returned because the request has timed out.	400
RequestIsNotMultiPartContent	The error message returned because the content-type value specified in the POST request is invalid.	400
SignatureDoesNotMatch	The error message returned because a signature error occurs.	403
TooManyBuckets	The error message returned because the number of the user's buckets exceeds the limit.	400
InvalidEncryptionAlgorithmError	The error message returned because the specified encryption algorithm (entropy) is invalid.	400

Note

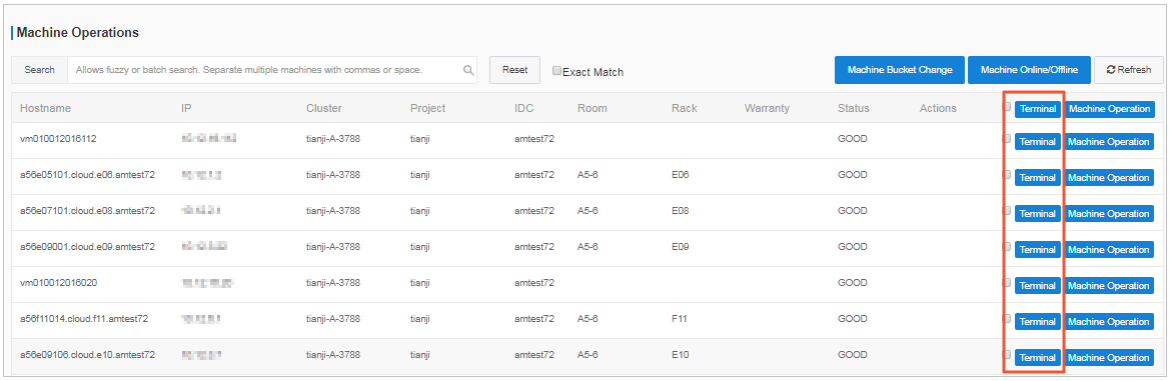
- In the preceding table, the error code is specified by the OssServiceError.Code parameter. The HTTP status code is specified by the OssServiceError.StatusCode parameter.
- If an operation not supported by OSS is performed to access a resource, OSS returns the 405 Method Not Allowed error.

2.4.3. Obtain an endpoint

You can obtain an endpoint of OSS in the Apsara Stack Operations console.

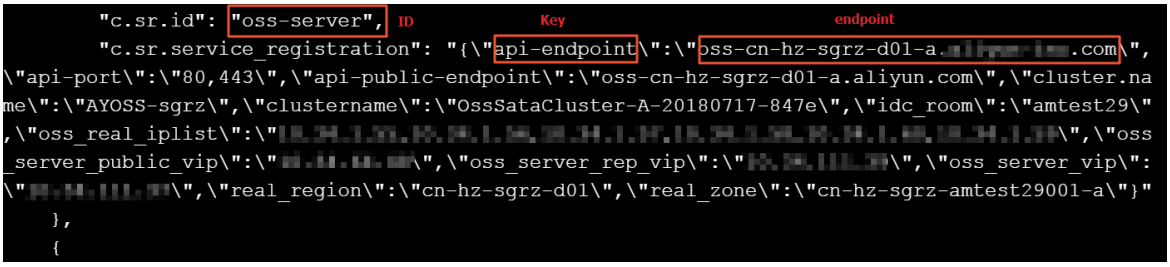
Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms > Apsara Stack Operations > Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. Choose **Operations > Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the command curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration" to obtain JSON data.

7. Obtain the endpoint of *OSS* based on the ID (*oss-server*) and key value (*api-endpoint*) of *OSS*.



2.4.4. Obtain an AccessKey pair

You can obtain an AccessKey pair in the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**. The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.5. Table Store

2.5.1. API reference

2.5.1.1. API-based operations

2.5.1.1.1. GetRow

Action

You can use the GetRow API to read data in a single row based on a specified primary key.

Request structure

```
message GetRowRequest {
   required string table_name = 1;
   required bytes primary_key = 2;   // The PlainBuffer encoding is binary.
   repeated string columns_to_get = 3; // If this parameter is not specified, all columns are read.
   optional TimeRange time_range = 4;
   optional int32 max_versions = 5;
   optional bytes filter = 7;
   optional string start_column = 8;
   optional string end_column = 9;
   optional bytes token = 10;
}
```

table_name:

- Type: string
- Required: yes
- This parameter specifies the name of the table containing the data to be read.

primary_key:

- Type: bytes
- Required: yes
- This parameter specifies all primary key columns in the row, including the primary key names and values. The primary key columns are encoded in the PlainBuffer format.

columns_to_get:

- Type: repeated string
- Required: no
- This parameter specifies the names of all columns to be returned. If the parameter is not configured, all columns of this row are returned.
- If the specified column does not exist, data in this column is not returned.
- If a duplicate column name exists, the response only includes this column once.
- In columns_to_get, the maximum number of strings is 128.

time_range:

- Type: TimeRange
- Required: At least one of the time_range and max_versions parameters must be specified.
- This parameter specifies the range of timestamps to read versions of data.
- The minimum timestamp value is 0. The maximum timestamp value is INT64.MAX.
- To query data within a time range, specify start_time and end_time.
- To query data within a specific timestamp, specify specific_time.
- Example: If the value of time_range is (100, 200), the timestamp of the returned column data must be within the range of [100, 200).

max_versions:

- Type: int32
- Required: At least one of the max_versions and time_range parameters must be specified.
- This parameter specifies the maximum number of versions of data to be returned.
- Example: If the value of max_versions is 2, data of a maximum of two versions is returned for each column.

filter:

- Type: bytes
- Required: no
- This parameter specifies the expression of the filtering condition.
- It indicates the binary data after the filter is serialized in the Protobuf format.

start_column:

- Type: string
- Required: no
- This parameter specifies the column to start to read from and is used to read wide rows.
- The response contains the specified starting column.
- The column names are sorted lexicographically.
- Example: If a table contains columns A, B, and C, and the value of start_column is B, the data is read starting from column B. Columns B and C are returned.

end_column:

- Type: string
- Required: no
- This parameter specifies the column to stop reading data and is used to read wide rows.
- The response does not contain the specified ending column.
- The column names are sorted lexicographically.
- Example: If a table contains columns A, B, and C, and the value of end_column is B, the reading stops at column B. Only column A is returned.

Response structure

```
message GetRowResponse {
   required ConsumedCapacity consumed = 1;
   required bytes row = 2; // The PlainBuffer encoding is binary.
}
```

consumed:

- Type: CapacityUnit
- This parameter specifies the number of CUs consumed by this operation.

row:

- Type: bytes
- The read data is encoded in the PlainBuffer format.
- If this row does not exist, null is returned.

CU consumption:

- If the requested row does not exist, one read CU is consumed.
- If the requested row exists, the number of consumed read CUs is calculated based on the following formula: Number of consumed read CUs = [(Size of all primary key columns in the row + Size of actually read attribute columns)/4 KB] rounded up.
- If the request times out and the results are undefined, a CU may or may not be consumed.
- If an internal error code is returned (HTTP status code: 5XX), this operation does not consume CUs. If other errors are returned, one read CU is consumed.

2.5.1.1.2. PutRow

Action

You can use the PutRow API to insert data into the specified row. If the row does not exist, a new row is added. If the row exists, the original row is overwritten.

Request structure

```
message PutRowRequest {
   required string table_name = 1;
   required bytes row = 2; // The PlainBuffer encoding is binary.
   required Condition condition = 3;
   optional ReturnContent return_content = 4;
}
```

table_name:

- Type: string
- Required: yes
- This parameter specifies the name of the table to write data to.

row:

- Type: bytes
- Required: yes
- This parameter specifies the data to be written into the row. It is in the PlainBuffer format and contains the primary key and attribute columns.

condition:

- Type: Condition
- Required: yes
- This parameter determines whether to perform the row existence check before writing data. It can be one of three values:
  - IGNORE indicates that the row existence check is not performed.
  - EXPECT_EXIST indicates that the row is expected to exist.
  - EXPECT_NOT_EXIST indicates that the row is not expected to exist.
- If the row is not expected to exist but it does, the row cannot be inserted and an error is returned. If the row is expected to exist but it does not, the row also fails to be inserted and an error is returned.

return_content:

- Type: ReturnContent
- Required: no
- This parameter specifies the data type after the row is written. Only the primary key is returned. It is used for the auto-increment function of the primary key column.

Response structure

```
message PutRowResponse {
 required ConsumedCapacity consumed = 1;
 optional bytes row = 2;
}
```

consumed:

- Type: ConsumedCapacity
- This parameter specifies the number of CUs consumed by this operation.

CU consumption:

- If this row does not exist:
  - If the value of the condition parameter is IGNORE, the number of consumed write CUs is calculated based on the following formula: Number of consumed write CUs = [(Size of primary key columns in the row + Size of attribute columns to be inserted)/4 KB] rounded up.
  - If the value of the condition parameter is EXPECT_NOT_EXIST, both write and read CUs are consumed. The number of consumed write CUs is calculated based on the following formula: Number of consumed write CUs = [(Size of primary key columns in the row + Size of attribute columns to be inserted)/4 KB] rounded up. The number of consumed read CUs is calculated based on the following formula: Number of consumed read CUs = (Size of primary key columns in the row/4 KB) rounded up.
  - If the value of the condition parameter is EXPECT_EXIST, the row fails to be inserted. One write CU and one read CU are consumed.
- If this row exists:
  - If the value of the condition parameter is IGNORE, the number of consumed write CUs is calculated based on the following formula: Number of consumed write CUs = [(Size of all primary key columns in the row + Size of attribute columns to be inserted)/4 KB] rounded up.
  - If the value of the condition parameter is EXPECT_EXIST, both write and read CUs are consumed. The number of consumed write CUs is calculated based on the following formula: Number of consumed write CUs = [(Size of all primary key columns in the row + Size of attribute columns to be inserted)/4 KB] rounded up. The number of consumed read CUs is calculated based on the following formula: Number of consumed read CUs = (Size of all primary key columns in the row/4 KB) rounded up.
  - If the value of the condition parameter is EXPECT_NOT_EXIST, the row fails to be inserted. One write CU and one read CU are consumed.
- Conditional Update:
  - If the operation succeeds, the number of consumed CUs are calculated based on the preceding formulas.
  - If the operation fails, one write CU and one read CU are consumed.
- If an internal error code is returned (HTTP status code: 5XX), this operation does not consume CUs. If other errors are returned, one write CU is consumed.
- If the request times out and the results are undefined, a CU may or may not be consumed.

row:

- Type: bytes
- This parameter specifies the returned data when return_content is set.
- If return_content is not set or no value is returned, NULL is returned.
- It is in the PlainBuffer format.

2.5.1.1.3. UpdateRow

Action

You can use the UpdateRow API to update the data of the specified row. If the row does not exist, a new row is added. If the row exists, the values of the specified columns are added, modified, or deleted based on the request content.

Request structure

```
message UpdateRowRequest {
 required string table_name = 1;
 required bytes row_change = 2;
 required Condition condition = 3;
 optional ReturnContent return_content = 4;
}
```

table_name:

- Type: string
- Required: yes
- This parameter specifies the name of the table whose data is to be updated.

row_change:

- Type: bytes
- Required: yes
- This parameter specifies the data to be updated. It is in the PlainBuffer format and contains the primary key and attribute columns.
- Table Store adds, modifies, or deletes the values for the attribute columns to be updated for this row based on the content of each UpdateType in row_change.
- Columns that exist in the row but does not exist in row_change are not affected.
- Values of UpdateType are as follows:
  - PUT: The UpdateType value must be a valid attribute column value. This indicates that if this column does not exist, a new column is added. If the column exists, it is overwritten.
  - DELETE: The UpdateType value must be null, while the timestamp must be specified. This indicates that the data of the specified version in the column is deleted.
  - DELETE_ALL: The UpdateType value and timestamp must be null. This indicates that all versions of the data in the column are deleted.

> Note Deleting all attribute columns of a row is not the same as deleting the row. If you want to delete the row, use the DeleteRow operation.

condition:

- Type: Condition
- Required: yes
- This parameter determines whether to perform existence check before data is updated. It can be one of two values:
  - IGNORE indicates that the row existence check is not performed.
  - EXPECT_EXIST indicates that the row is expected to exist.
- If the row is expected to exist but does not, the row cannot be updated and an error is returned. If the existence of the row is ignored, this operation succeeds regardless of the row existence.

return_content:

- Type: ReturnContent
- Required: no
- This parameter specifies the data type after the row is written. Only the primary key is returned. It is used for the auto-increment function of the primary key column.

Response structure

```
message UpdateRowResponse {
 required ConsumedCapacity consumed = 1;
 optional bytes row = 2;
}
```

consumed:

- Type: ConsumedCapacity
- This parameter specifies the number of CUs consumed by this operation.

CU consumption:

- If this row does not exist:
  - If the value of the condition parameter is IGNORE, the number of consumed write CUs is calculated based on the following formula: Number of consumed write CUs = [(Size of primary key columns in the row + Size of attribute columns to be updated)/4 KB] rounded up. If UpdateRow contains an attribute column to be deleted, only the column name length is included in the size of the attribute column.
  - If the value of the condition parameter is EXPECT_EXIST, the row fails to be inserted. One write CU and one read CU are consumed.
- If this row exists:
  - If the value of the condition parameter is IGNORE, the number of consumed write CUs is calculated based on the following formula: Number of consumed write CUs = [(Size of primary key columns in the row + Size of attribute columns to be updated)/4 KB] rounded up. If UpdateRow contains an attribute column to be deleted, only the column name length is included in the size of the attribute column.

  - If the value of the condition parameter is EXPECT_EXIST, both write and read CUs are consumed. The number of consumed write CUs is calculated with the same method used when the value of the condition parameter is IGNORE. The number of consumed read CUs is calculated based on the following formula: Number of consumed read CUs = (Size of primary key columns in the row/4 KB) rounded up.

- If the request times out and the results are undefined, a CU may or may not be consumed.
- If an internal error code is returned (HTTP status code: 5XX), this operation does not consume CUs. If other errors are returned, one write CU and one read CU are consumed.

row:

- Type: bytes
- This parameter specifies the returned data when return_content is set.
- If return_content is not set or no value is returned, NULL is returned.
- The returned data is in the PlainBuffer format.

2.5.1.1.4. DeleteRow

Action

You can use the DeleteRow API to delete a row of data.

Request structure

```
message DeleteRowRequest {
   required string table_name = 1;
   required bytes primary_key = 2; // The PlainBuffer encoding is binary.
   required Condition condition = 3;
   optional ReturnContent return_content = 4;
}
```

table_name:

- Type: string
- Required: yes
- This parameter specifies the name of the table whose data is to be updated.

primary_key:

- Type: bytes
- Required: yes
- This parameter specifies the primary key of the row to be deleted, which is in the PlainBuffer format.

condition:

- Type: Condition
- Required: yes
- This parameter determines whether to perform existence check before data updates. It can be one of two values:
  - IGNORE indicates that the row existence check is not performed.

  - EXPECT_EXIST indicates that the row is expected to exist.
- If this row is expected to exist but does not, the delete operation fails and an error is returned. If the existence of the row is ignored, this operation succeeds regardless of the row existence.

return_content:

- Type: ReturnContent
- Required: no
- This parameter specifies the data type after the row is written. Only the primary key is returned. It is used for the auto-increment function of the primary key column.

Response structure

```
message DeleteRowResponse {
 required ConsumedCapacity consumed = 1;
 optional bytes row = 2;
}
```

consumed:

- Type: ConsumedCapacity
- This parameter specifies the number of capacity units (CUs) consumed by this operation.

CU consumption:

- If this row does not exist:
  - If the value of the condition parameter is IGNORE, the number of consumed write CUs is calculated based on the following formula: Number of consumed write CUs = (Size of primary key columns in the row/4 KB) rounded up.
  - If the value of the condition parameter is EXPECT_EXIST, the row fails to be deleted, and one write CU and one read CU are consumed.
- If this row exists:
  - If the value of the condition parameter is IGNORE, the number of consumed write CUs is calculated based on the following formula: Number of consumed write CUs = (Size of primary key columns in the row/4 KB) rounded up.
  - If the value of the condition parameter is EXPECT_EXIST, both write and read CUs are consumed. The number of consumed write CUs and the number of consumed read CUs are calculated based on the following formula: Number of consumed read/write CUs = (Size of primary key columns in the row/4 KB) rounded up.
- If an internal error code is returned (HTTP status code: 5XX), this operation does not consume CUs. If other errors are returned, one write CU is consumed.
- If the request times out and the results are undefined, a CU may or may not be consumed.

row:

- Type: bytes
- This parameter specifies the returned data when return_content is set.
- If return_content is not set or no value is returned, NULL is returned.
- The returned data is in the PlainBuffer format.

2.5.1.1.5. GetRange

Action

You can use the GetRange API to read data within the specified primary key range.

Request structure

```
message GetRangeRequest {
   required string table_name = 1;
   required Direction direction = 2;
   repeated string columns_to_get = 3;  // If this parameter is not specified, all columns are read.
   optional TimeRange time_range = 4;
   optional int32 max_versions = 5;
   optional int32 limit = 6;
   required bytes inclusive_start_primary_key = 7; // The PlainBuffer encoding is binary.
   required bytes exclusive_end_primary_key = 8; // The PlainBuffer encoding is binary.
   optional bytes filter = 10;
   optional string start_column = 11;
   optional string end_column = 12;
}
```

table_name:

- Type: string
- Required: yes
- This parameter specifies the name of the table containing the data to be read.

direction:

- Type: Direction
- Required: yes
- This parameter specifies the query direction. If the query direction is FORWARD, the value of inclusive_start_primary must be smaller than that of exclusive_end_primary, and the rows in the response are sorted in ascending order of primary key values. If the query direction is BACKWARD, the value of inclusive_start_primary must be greater than that of exclusive_end_primary, and the rows in the response are sorted in descending order of primary key values.

columns_to_get:

- Type: repeated string
- Required: no
- This parameter specifies the names of all columns to be returned. If the parameter is not configured, all columns of each row in the read results are returned.
- If a duplicate column name exists, the response only includes this column once.
- In columns_to_get, the maximum number of strings is 128.

time_range:

- Type: TimeRange
- Required: At least one of the time_range and max_versions parameters must be specified.
- This parameter specifies the range of timestamps to read versions of data.
- The minimum timestamp value is 0. The maximum timestamp value is INT64.MAX.
- To query data within a time range, specify start_time and end_time.
- To query data within a specific timestamp, specify specific_time.
- Example: If the value of time_range is (100, 200), the timestamp of the data in the returned column must be within [100, 200).

max_versions:

- Type: int32
- Required: At least one of the max_versions and time_range parameters must be specified.
- This parameter specifies the maximum number of versions of data to be returned.
- Example: If the value of max_versions is 2, data of a maximum of two versions is returned for each column.

limit:

- Type: int32
- Required: no
- This parameter specifies the maximum number of returned rows to be read in a single operation. If the number of rows queried exceeds this value, the response includes a split point to record the position where read ends in this operation and facilitate the next read. This value must be greater than 0.
- Table Store returns a maximum of 5,000 rows of data not exceeding a total size of 4 MB regardless of the row existence.

inclusive_start_primary_key:

- Type: bytes
- Required: yes
- This parameter specifies the row that contains the starting primary key for the range to be read. If this row exists, the response contains it. It is encoded in the PlainBuffer format.

exclusive_end_primary_key:

- Type: bytes
- Required: yes
- This parameter specifies the row that contains the ending primary key for the range to be read. The response does not contain the row regardless of the row existence. It is encoded in the PlainBuffer format.
- For GetRange, the type of Column in inclusive_start_primary_key or exclusive_end_primary_key can be specialized to INF_MIN or INF_MAX. If the type of Column is set to INF_MIN, the value of the Column is always smaller than that of other Columns. If the type of Column is set to INF_MAX, its value is always greater than other Columns.

filter:

- Type: bytes
- Required: no
- This parameter specifies the filtering condition expression.
- It indicates the binary data after the filter is serialized in the Protobuf format.

start_column:

- Type: string
- Required: no
- This parameter specifies the column to start to read from and is used to read wide rows.
- The response contains the specified starting column.
- The column names are sorted lexicographically.
- Example: If a table contains columns A, B, and C, and the value of start_column is B, the data is read starting from column B. Columns B and C are returned.

end_column:

- Type: string
- Required: no
- This parameter specifies the column to stop reading data and is used to read wide rows.
- The response does not contain the specified ending column.
- The column names are sorted lexicographically.
- Example: If a table contains columns A, B, and C, and the value of end_column is B, the reading stops at column B. Only column A is returned.

Response structure

```
message GetRangeResponse {
   required ConsumedCapacity consumed = 1;
   required bytes rows = 2;
   optional bytes next_start_primary_key = 3;
}
```

consumed:

- Type: ConsumedCapacity
- This parameter specifies the number of CUs consumed by this operation.

rows:

- Type: bytes
- The value of this parameter is encoded in the PlainBuffer format.
- For all data read, if the direction in the request is FORWARD, all rows are sorted in ascending order of primary key values. If the direction in the request is BACKWARD, all rows are sorted in descending order of primary key values.
- primary_key_columns and attribute_columns for each row only contain the columns specified in columns_to_get. Their orders may not be consistent with the order of columns_to_get in the request. The order of primary_key_columns may not be consistent with the order specified when the table is created.
- If the specified columns_to_get in the request does not contain a primary key column, the primary key is within the query range. However, the row which does not contain any attribute column in columns_to_get is not contained in the response.

next_start_primary_key:

- Type: bytes

- This parameter specifies the split point information for this GetRange operation. The split point information is encoded in the PlainBuffer format.
- If this parameter is not configured, the response for this GetRange operation contains all data within the request range.
- If this parameter is configured, the response for this GetRange operation includes only the data within the [inclusive_start_primary_key, next_start_primary_key) range. If you want to obtain the remaining data, you must use next_start_primary_key as inclusive_start_primary_key, and retain exclusive_end_primary_key in the original request to proceed with the GetRange operation.

> **Note** Table Store limits the number of rows in the response of a GetRange operation to 5,000 rows, whose size cannot exceed 4 MB. Furthermore, the volume of returned data cannot exceed the currently remaining reserved read throughput. Even if no limit is set in the GetRange request, next_start_primary_key may still appear in the response. Therefore, when using GetRange, you must check whether the response has next_start_primary_key configured and proceed accordingly.

CU consumption:

- The number of read CUs consumed by the GetRange operation is calculated based on the following formula: Number of read CUs consumed by the GetRange operation = [(Size of primary key columns of the row within the query range + Size of actually read attribute columns)/4 KB] rounded up.
- If the request times out and the results are undefined, a CU may or may not be consumed.
- If an internal error code is returned (HTTP status code: 5XX), this operation does not consume CUs. If other errors are returned, one read CU is consumed.

2.5.1.1.6. BatchGetRow

Action

You can use the BatchGetRow API to simultaneously read data in several rows from one or more tables.

The BatchGetRow operation is a set of multiple GetRow operations. The execution, returning of results, and CU consumption of each individual operation are carried out independently.

Compared with the execution of a large number of GetRow operations, the use of BatchGetRow can reduce the request response time and increase the data read rate.

Request structure

```
message BatchGetRowRequest {
  repeated TableInBatchGetRowRequest tables = 1;
}
```

tables:

- Type: repeated TableInBatchGetRowRequest
- Required: yes
- This parameter specifies the information of rows to be read.

- The entire operation fails and returns an error if any of the following conditions appears in tables:
  - Any table listed in the tables parameter does not exist.
  - The name of any table does not comply with the table naming conventions.
  - The primary key is not specified for any row in a table, the primary key column name does not comply with the conventions, or the primary key column type is incorrect.
  - A column name in columns_to_get of any table does not comply with the column naming conventions.
  - Tables with the same name exist.
  - Any table in the tables contains rows with identical primary keys.
  - The total number of RowInBatchGetRowRequest in all tables exceeds 100.
  - Any table in the tables does not contain any RowInBatchGetRowRequest.
  - The value of columns_to_get of any table exceeds 128.

Response structure

```
message BatchGetRowResponse {
  repeated TableInBatchGetRowResponse tables = 1;
}
```

tables:

- Type: repeated TableInBatchGetRowResponse
- The value of this parameter corresponds to the data to be read in each table.
- The TableInBatchGetRowResponse object order in the response is the same as the TableInBatchGetRowRequest object order in BatchGetRowRequest. The object order of each RowInBatchGetRowResponse under TableInBatchGetRowResponse is the same as that of RowInBatchGetRowRequest under TableInBatchGetRowRequest.
- If a row does not exist or contains no data in the specified columns_to_get, a corresponding RowInBatchGetRowResponse still appears in TableInBatchGetRowResponse. However, the primary_key_columns and attribute_columns of the row are null.
- If a row fails to be read, the is_ok value in RowInBatchGetRowResponse for the row is false and the row is null.

> **Note** The BatchGetRow operation may partially fail at the row level. However, it still returns an HTTP status code of 200. The application must check for errors in RowInBatchGetRowResponse to confirm the execution results for each row and then proceed accordingly.

CU consumption:

- If the entire operation fails, it does not consume any CU.
- If the request times out and the results are undefined, a CU may or may not be consumed.
- In other situations, each RowInBatchGetRowRequest operation is considered as one GetRow operation when write CUs are calculated.

2.5.1.1.7. BatchWriteRow

Action

You can use the BatchWriteRow API to simultaneously insert, modify, or delete data in several rows in one or more tables.

It is a set of multiple PutRow, UpdateRow, and DeleteRow operations. The execution, returning of results, and capacity unit (CU) consumption of each individual operation are carried out independently.

Compared with the execution of a large number of write operations, the use of BatchWriteRow can reduce the request response time and increase the data write rate.

Request structure

```
message BatchWriteRowRequest {
  repeated TableInBatchWriteRowRequest tables = 1;
}
```

tables:

- Type: repeated TableInBatchWriteRowRequest
- Required: yes
- This parameter specifies the information of rows that require write operations.
- An error is returned if any of the following conditions occurs:
  - Any table listed in the tables parameter does not exist.
  - Tables with the same name exist.
  - The name of any table does not comply with the table naming conventions.
  - The primary key is not specified for any row in a table, the primary key column name does not comply with the conventions, or the primary key column type is incorrect.
  - For any attribute column in a table, the column name does not comply with the column naming conventions.
  - Any row in a table contains an attribute column with the same name as the primary key column.
  - The value of any primary key or attribute column in a table exceeds the upper limit.
  - Any table in the tables contains rows with identical primary keys.
  - The total number of rows for all tables listed in the tables parameter exceeds 200 or the total size of the data exceeds 4 MB.
  - If any table contains no rows, the OTSParameterInvalidException error is returned.
  - The number of columns included in any PutRowInBatchWriteRowRequest of a table exceeds 1,024.
  - The number of ColumnUpdate objects included in any UpdateRowInBatchWriteRowRequest in a table exceeds 1,024.

Response structure

```
message BatchWriteRowResponse {
  repeated TableInBatchWriteRowResponse tables = 1;
}
```

tables:

- Type: TableInBatchWriteRowResponse
- This parameter specifies the response information corresponding to the operations for each table. The response information contains the execution results, error codes, and number of CUs consumed.
- The TableInBatchWriteRowResponse object order in the response is the same as the TableInBatchWriteRowRequest object order in BatchWriteRowRequest. The RowInBatchWriteRowResponse object orders contained in put_rows, update_rows, and delete_rows in each TableInBatchWriteRowRequest are the same as the respective PutRowInBatchWriteRowRequest, UpdateRowInBatchWriteRowRequest, and DeleteRowInBatchWriteRowRequestobject orders contained in put_rows, update_rows, and delete_rows in TableInBatchWriteRowRequest.
- If a row fails to be read, the is_ok value of the row in RowInBatchWriteRowResponse is false.

> **Note** The BatchWriteRow operation may partially fail at the row level. However, it still returns an HTTP status code of 200. The application must check for errors in RowInBatchWriteRowResponse to confirm the execution results for each row and then proceed accordingly.

CU consumption:

- If the entire operation fails, it does not consume any CUs.
- If the request times out and the results are undefined, a CU may or may not be consumed.
- In other situations, each PutRowInBatchWriteRowRequest, UpdateRowInBatchWriteRowRequestDelete, or RowInBatchWriteRowRequest operation is considered as one write operation when write CUs are calculated.

2.5.1.1.8. CreateTable

Action

You can use the CreateTable API to create a table based on the specified table structure information.

Request structure

```
message CreateTableRequest {
    required TableMeta table_meta = 1;
    required ReservedThroughput reserved_throughput = 2;
    optional TableOptions table_options = 3;
    optional StreamSpecification stream_spec = 5;
}
```

table_meta:

- Type: TableMeta
- Required: yes
- This parameter specifies the structural information of the table you want to create. The value of table_name must be unique among the current instance. The value of ColumnSchemas in

primary_key must be between 1 and 4. The value of the name parameter in ColumnSchema of primary_key must comply with the naming conventions. The value of the type parameter can only be STRING, INTEGER, or BINARY.

- After a table is created, its schema cannot be modified.

reserved_throughput:

- Type: ReservedThroughput
- Required: yes
- This parameter specifies the initial reserved read/write throughput for the table to be created. The maximum reserved throughput is 5,000 for each table.
- The reserved read/write throughput settings for a table can be modified by using the UpdateTable operation.

table_options:

- Type: TableOptions
- Required: yes
- This parameter specifies TimeToLive and MaxVersions.

Response structure

```
message CreateTableResponse {
}
```

Note

- No read/write operation can be performed on a table immediately after it is created. Typically, you can perform read/write operations on a new table one minute after it is created.
- A single instance can contain up to 64 tables. If you need to raise the upper limit of the table quantity for a single instance, contact Alibaba Cloud customer service.

2.5.1.1.9. ListTable

Action

You can use the ListTable API to obtain the names of all tables created in the current instance.

Request structure

```
message ListTableRequest {
}
```

Response structure

```
message ListTableResponse {
    repeated string table_names = 1;
}
```

table_names:

- Type: repeated string
- This parameter specifies the names of all tables in the current instance.

Note

If a table is created, its table name can be returned by ListTableResponse, but this does not necessarily mean that this table can be read or written at the time.

2.5.1.1.10. DeleteTable

Action

You can use the DeleteTable API to delete the specified table in an instance.

Request structure

```
message DeleteTableRequest {
    required string table_name = 1;
}
```

table_name:

- Type: string
- Required: yes
- This parameter specifies the name of the table you want to delete.

Response structure

```
message DeleteTableResponse {
}
```

If the response of DeleteTable does not contain an error, the table has been deleted.

2.5.1.1.11. UpdateTable

Action

You can use the UpdateTable API to update the reserved read or write throughput settings of the specified table. New settings take effect within one minute of a successful update.

Request structure

```
message UpdateTableRequest {
    required string table_name = 1;
    optional ReservedThroughput reserved_throughput = 2;
    optional TableOptions table_options = 3;
    optional StreamSpecification stream_spec = 4;
}
```

table_name:

- Type: string
- Required: yes
- This parameter specifies the name of the table for which you want to modify the reserved read/write throughput settings.

reserved_throughput:

- Type: ReservedThroughput
- Required: yes
- This parameter specifies the reserved read/write throughput settings you want to modify for the table. New settings take effect within one minute of a successful update.
- You may modify the reserved read/write throughput settings of the table as required.
- You must specify a non-null value for either the read or write parameter of capacity_unit. Otherwise, the request fails and an error is returned.

table_options:

- Type: TableOptions
- Required: yes
- This parameter specifies TimeToLive and MaxVersions.

Response structure

```
message UpdateTableResponse {
   required ReservedThroughputDetails reserved_throughput_details = 1;
   required TableOptions table_options = 2;
}
```

reserved_throughput_details:

- Type: ReservedThroughputDetails
- After the update, the reserved read/write throughput settings information of the table contains the current reserved throughput settings, the time these settings were last updated, and the number of times they have been lowered on the current date.

table_options:

- Type: TableOptions
- The latest value of the table_options parameter after the modification.

Note

- The minimum interval between updates to the reserved read/write throughput of a table is two minutes. If the current UpdateTable operation is requested within two minutes of the previous operation, it will be rejected.
- The reserved read/write throughput of a table can be raised or lowered an unlimited number of times within a single day (from 00:00:00 to 00:00:00 the next day in UTC time).

2.5.1.1.12. DescribeTable

Action

Action

You can use the DescribeTable API to query the structure information and reserved read/write throughput value of the specified table.

Request structure

```
message DescribeTableRequest {
 required string table_name = 1;
}
```

table_name:

- Type: string
- Required: yes
- This parameter specifies the name of the table you want to query.

Response structure

```
message DescribeTableResponse {
   required TableMeta table_meta = 1;
   required ReservedThroughputDetails reserved_throughput_details = 2;
   required TableOptions table_options = 3;
   optional StreamDetails stream_details = 5;
   repeated bytes shard_splits = 6;
}
```

table_meta:

- Type: TableMeta
- This parameter specifies the schema of the table. The schema is the same as the schema provided when the table is created.

reserved_throughput_details:

- Type: ReservedThroughputDetails
- This parameter specifies the reserved read/write throughput settings information of the table. The information contains the current reserved read/write throughput settings, the time these settings were last updated, and the number of times they have been lowered on the current date.

table_options:

- Type: TableOptions
- This parameter specifies the latest value of the table_options parameter.

StreamSpecification:

- Type: StreamSpecification
- Required: no
- This parameter specifies whether to enable Stream-related attributes.

shard_splits:

- Type: bytes
- This parameter specifies the split points of all partitions in the current table.

2.5.1.1.13. ComputeSplitPointsBySize

Action

You can use the ComputeSplitPointsBySize API to logically split data in a table into several partitions whose sizes are close to the specified size. The API can return the split points between the partitions and prompt about hosts where the partitions reside. This API is typically used to implement plans on compute engines, such as concurrency plans.

Request structure

```
message ComputeSplitPointsBySizeRequest {
    required string table_name = 1;
    required int64 split_size = 2; // in 100MB
}
```

table_name:

- Type: string
- Required: yes
- This parameter specifies the name of the table that contains the data you want to split.

split_size:

- Type: int64
- Required: yes
- This parameter specifies the approximate size of each partition, rounded to the nearest 100 MB.

Response structure

```
message ComputeSplitPointsBySizeResponse {
    required ConsumedCapacity consumed = 1;
    repeated PrimaryKeySchema schema = 2;
    /**
     * Split points between splits, in the ascending order.
     *
     * A split is a consecutive range of primary keys,
     * whose data size is approximately split_size specified in the request.
     * The size could be hard to be precise.
     *
     * A split point is an array of primary-key column w.r.t. table schema,
     * which is never longer than that of table schema.
     * Tailing -inf will be omitted to reduce transmission payloads.
     */
    repeated bytes split_points = 3;
    /**
     * Locations where splits lie.
     *
     * By the managed nature of TableStore, these locations are no more than hints.
     * If a location is not suitable to be seen, an empty string will be placed.
     */
    message SplitLocation {
        required string location = 1;
        required sint64 repeat = 2;
    }
    repeated SplitLocation locations = 4;
}
```

consumed:

- Type: ConsumedCapacity
- This parameter specifies the number of CUs consumed by this request.

schema:

- Type: PrimaryKeySchema
- This parameter specifies the schema of the table. The schema is the same as the schema provided when the table is created.

split_points:

- Type: repeated bytes
- The split points between partitions. The split points must increase monotonically between the partitions. Each split point is a PlainBuffer-encoded line and contains only primary keys. The last -inf of each split point is not transmitted to reduce the volume of data transmitted.

locations:

- Type: repeated SplitLocation
- This parameter specifies the prompt about the hosts where the split points reside. It can be null.

For example, a table contains three columns of primary keys, where the first column is of the string type. After this API is called, five partitions are obtained, which are (-inf,-inf,-inf) to ("a",-inf,-inf), ("a",-inf,-inf) to ("b",-inf,-inf), ("b",-inf,-inf) to ("c",-inf,-inf), ("c",-inf,-inf) to ("d",-inf,-inf), and ("d",-inf,-inf) to (+inf,+inf,+inf). The first three partitions reside in machine-A, while the last two in machine-B. In this case, split_points is (example) `[("a"),("b"),("c"),("d")]`, whereas locations is (example) `"machine-A"*3, "machine-B"*2`.

CU consumption

The number of consumed read CUs is the same as that of the partitions. No write CUs are consumed.

2.5.1.1.14. ListStream

Action

You can use the ListStream API to obtain information about the stream that is enabled for all tables in the current instance.

Request structure

```
message ListStreamRequest {
    optional string table_name = 1;
}
```

table_name:

- Type: optional string
- This parameter specifies the name of the table for which the current stream is enabled.

Response structure

```
message ListStreamResponse {
    repeated Stream streams = 1;
}
message Stream {
    required string stream_id = 1;
    required string table_name = 2;
    required int64 creation_time = 3;
}
```

stream_id:

- Type: repeated string
- This parameter specifies the ID of the current stream.

table_name:

- Type: required string
- This parameter specifies the name of the table for which the current stream is enabled.

creation_time:

- Type: required int64
- This parameter specifies the time the current stream is enabled.

2.5.1.1.15. DescribeStream

Action

You can use the DescribeStream API to obtain information about the partitions of the current stream.

Request structure

```
message DescribeStreamRequest {
    required string stream_id = 1;
    optional string inclusive_start_shard_id = 2;
    optional int32 shard_limit = 3;
}
```

stream_id:

- Type: required string
- This parameter specifies the ID of the current stream.

inclusive_start_shard_id:

- Type: required string
- This parameter specifies the ID of the starting partition in a query.

shard_limit:

- Type: required string
- This parameter specifies the upper limit of the returned partition quantity in a single query.

Response structure

```
message DescribeStreamResponse {
    required string stream_id = 1;
    required int32 expiration_time = 2;
    required string table_name = 3;
    required int64 creation_time = 4;
    required StreamStatus stream_status = 5;
    repeated StreamShard shards = 6;
    optional string next_shard_id = 7;
}
message StreamShard {
    required string shard_id = 1;
    optional string parent_id = 2;
    optional string parent_sibling_id = 3;
}
```

stream_id:

- Type: required string
- This parameter specifies the ID of the current stream.

expiration_time:

- Type: required int32
- This parameter specifies the expiration time of the stream.

table_name:

- Type: required string
- This parameter specifies the name of the table for which the current stream is enabled.

creation_time:

- Type: required int32
- This parameter specifies the time the current stream is enabled.

stream_status:

- Type: required StreamStatus
- This parameter specifies the status of the current stream, which can be enabling or active.

shards:

- Type: required StreamShard
- This parameter specifies the information about the streamShard, including the partition ID, parent partition ID, and information about the neighbor partition of the parent partition (applicable when the parent partition is merged).

next_shard_id:

- Type: optional string
- This parameter specifies the start ID of the next partition in a paging query.

Note

Data reading for the parent partition must be completed before data of the current partition is read.

2.5.1.1.16. GetShardIterator

Action

You can use the GetShardIterator API to obtain the response of the start iterator for reading the record information of the current partition.

Request structure

```
message GetShardIteratorRequest {
    required string stream_id = 1;
    required string shard_id = 2;
}
```

stream_id:

- Type: required string
- This parameter specifies the ID of the current stream.

shard_id:

- Type: required string
- This parameter specifies the ID of the current partition.

Response structure

```
message GetShardIteratorResponse {
    required string shard_iterator = 1;
}
```

shard_iterator:

- Type: required string
- This parameter specifies the start iterator for reading the record of the current partition.

2.5.1.1.17. GetStreamRecord

Action

You can use the GetStreamRecord API to obtain the incremental content of the current partition.

Request structure

```
message GetStreamRecordRequest {
    required string shard_iterator = 1;
    optional int32 limit = 2;
}
```

shard_iterator:

- Type: required string
- This parameter specifies the iterator for reading the current partition next time.

Response structure

```
message GetStreamRecordResponse {
   message StreamRecord {
      required ActionType action_type = 1;
      required bytes record = 2;
   }
   repeated StreamRecord stream_records = 1;
   optional raw_string next_shard_iterator = 2;
   optional ConsumedCapacity consumed = 3;
}
```

StreamRecord:

- Type: repeated StreamRecord
- This parameter specifies the record entry for reading the current partition.

shard_iterator:

- Type: required string
- This parameter specifies the iterator for reading the current partition next time.

consumed:

- Type: ConsumedCapacity
- This parameter specifies the number of CUs consumed by this operation.
- The sum of data in all rows of a table for stream read is calculated based on the following formula: Number of consumed read CUs = (Size of actually read columns/4 KB) rounded up.

2.5.1.1.18. Table Store ProtocolBuffer message definitions

The detailed definitions of table_store.proto and table_store_filter.proto are as follows:

table_store.proto

```
package com.alicloud.openservices.tablestore.core.protocol;
message Error {
   required string code = 1;
   optional string message = 2;
}
enum PrimaryKeyType {
   INTEGER = 1;
   STRING = 2;
   BINARY = 3;
}
```

```
enum PrimaryKeyOption {
    AUTO_INCREMENT = 1;
}
message PrimaryKeySchema {
    required string name = 1;
    required PrimaryKeyType type = 2;
    optional PrimaryKeyOption option = 3;
}
message TableOptions {
    optional int32 time_to_live = 1; // This parameter value can be dynamically modified.
    optional int32 max_versions = 2; // This parameter value can be dynamically modified.
    optional int64 deviation_cell_version_in_sec = 5; // This parameter value can be dynamically modified.
}
message TableMeta {
    required string table_name = 1;
    repeated PrimaryKeySchema primary_key = 2;
}
enum RowExistenceExpectation {
    IGNORE = 0;
    EXPECT_EXIST = 1;
    EXPECT_NOT_EXIST = 2;
}
message Condition {
    required RowExistenceExpectation row_existence = 1;
    optional bytes column_condition     = 2;
}
message CapacityUnit {
    optional int32 read = 1;
    optional int32 write = 2;
}
message ReservedThroughputDetails {
    required CapacityUnit capacity_unit = 1; // This parameter indicates the current reserved throughput
of the table.
    required int64 last_increase_time = 2; // This parameter indicates the last time the reserved throughp
ut was raised.
    optional int64 last_decrease_time = 3; // This parameter indicates the last time the reserved throughp
ut was lowered.
}
message ReservedThroughput {
    required CapacityUnit capacity_unit = 1;
}
message ConsumedCapacity {
```

```
message ConsumedCapacity {
    required CapacityUnit capacity_unit = 1;
}
/* ############################################## CreateTable ################
############################## */
/**
 * table_meta is used to store unmodifiable schema attributes in a table. The ReservedThroughput and T
ableOptions attributes that can be modified are independently stored as the parameters for UpdateTab
le.
 * message CreateTableRequest {
 *       required TableMeta table_meta = 1;
 *       required ReservedThroughput reserved_throughput = 2;
 *       required TableOptions table_options = 3;
 * }
 */
message CreateTableRequest {
    required TableMeta table_meta = 1;
    required ReservedThroughput reserved_throughput = 2;
    optional TableOptions table_options = 3;
}
message CreateTableResponse {
}
/* ###########################################################################
################################## */
/* ############################################## UpdateTable ################
############################## */
message UpdateTableRequest {
    required string table_name = 1;
    optional ReservedThroughput reserved_throughput = 2;
    optional TableOptions table_options = 3;
}
message UpdateTableResponse {
    required ReservedThroughputDetails reserved_throughput_details = 1;
    required TableOptions table_options = 2;
}
/* ###########################################################################
################################## */
/* ############################################## DescribeTable ##############
############################## */
message DescribeTableRequest {
    required string table_name = 1;
}
```

```
message DescribeTableResponse {
  required TableMeta table_meta = 1;
  required ReservedThroughputDetails reserved_throughput_details = 2;
  required TableOptions table_options = 3;
  repeated bytes shard_splits = 6;
}
/* ##########################################################################
################################### */
/* ############################################## ListTable ##################
########################### */
message ListTableRequest {
}
/**
 * Only a simple name list is returned currently.
 */
message ListTableResponse {
  repeated string table_names = 1;
}
/* ##########################################################################
################################ */
/* ############################################## DeleteTable ################
############################ */
message DeleteTableRequest {
  required string table_name = 1;
}
message DeleteTableResponse {
}
/* ############################################## UnloadTable ################
############################ */
message UnloadTableRequest {
  required string table_name = 1;
}
message UnloadTableResponse {
}
/* ##########################################################################
################################### */
/**
 * The minimum value of the timestamp is 0. The maximum value of the timestamp is INT64.MAX.
 * 1. To query data of a time range, specify start_time and end_time.
 * 2. To query data of a specific timestamp, specify specific_time.
 */
```

```
message TimeRange {
    optional int64 start_time = 1;
    optional int64 end_time = 2;
    optional int64 specific_time = 3;
}
/* ################################################ GetRow ###################
########################### */
enum ReturnType {
    RT_NONE = 0;
    RT_PK = 1;
}
message ReturnContent {
    optional ReturnType return_type = 1;
}
/**
 * 1. You can specify the timestamp range or time to read the columns of the specified version.
 * 2. Intra-row split points are not currently supported.
 */
message GetRowRequest {
    required string table_name = 1;
    required bytes primary_key = 2; // It is encoded as InplaceRowChangeSet, but only contains primary k
ey.
    repeated string columns_to_get = 3; // If this parameter is not specified, all columns are read.
    optional TimeRange time_range = 4;
    optional int32 max_versions = 5;
    optional bytes filter = 7;
    optional string start_column = 8;
    optional string end_column = 9;
    optional bytes token = 10;
}
message GetRowResponse {
    required ConsumedCapacity consumed = 1;
    required bytes row = 2; // It is encoded as InplaceRowChangeSet.
    optional bytes next_token = 3;
}
/* ################################################################################
############################## */
/* ################################################ UpdateRow ##################
############################## */
message UpdateRowRequest {
    required string table_name = 1;
    required bytes row_change = 2;
```

```
    required bytes row_change = 2;
    required Condition condition = 3;
    optional ReturnContent return_content = 4;
}
message UpdateRowResponse {
    required ConsumedCapacity consumed = 1;
    optional bytes row = 2;
}
/* ##########################################################################
################################ */
/* ############################################## PutRow ####################
########################## */
/**
 * You can set a timestamp for each column instead of configuring a unified timestamp for the entire row
.
 */
message PutRowRequest {
    required string table_name = 1;
    required bytes row = 2; // It is encoded as InplaceRowChangeSet.
    required Condition condition = 3;
    optional ReturnContent return_content = 4;
}
message PutRowResponse {
    required ConsumedCapacity consumed = 1;
    optional bytes row = 2;
}
/* ##########################################################################
############################ */
/* ############################################## DeleteRow #################
############################ */
/**
 * Table Store only allows you to delete versions of all columns in a row. It does not allow you to:
 *  1. Delete the specified version and versions earlier than it.
 */
message DeleteRowRequest {
    required string table_name = 1;
    required bytes primary_key = 2; // It is encoded as InplaceRowChangeSet, but only contains primary k
ey.
    required Condition condition = 3;
    optional ReturnContent return_content = 4;
}
message DeleteRowResponse {
```

```
    required ConsumedCapacity consumed = 1;
    optional bytes row = 2;
}
/* ##########################################################################
################################ */
/* ############################################## BatchGetRow ################
################################ */
message TableInBatchGetRowRequest {
    required string table_name = 1;
    repeated bytes primary_key = 2; // It is encoded as InplaceRowChangeSet, but only contains primary k
ey.
    repeated bytes token = 3;
    repeated string columns_to_get = 4;  // If this parameter is not specified, all columns are read.
    optional TimeRange time_range = 5;
    optional int32 max_versions = 6;
    optional bytes filter = 8;
    optional string start_column = 9;
    optional string end_column = 10;
}
message BatchGetRowRequest {
    repeated TableInBatchGetRowRequest tables = 1;
}
message RowInBatchGetRowResponse {
    required bool is_ok = 1;
    optional Error error = 2;
    optional ConsumedCapacity consumed = 3;
    optional bytes row = 4; // It is encoded as InplaceRowChangeSet.
    optional bytes next_token = 5;
}
message TableInBatchGetRowResponse {
    required string table_name = 1;
    repeated RowInBatchGetRowResponse rows = 2;
}
message BatchGetRowResponse {
    repeated TableInBatchGetRowResponse tables = 1;
}
/* ##########################################################################
################################ */
/* ############################################## BatchWriteRow ###############
################################ */
enum OperationType {
```

```
    PUT = 1;
    UPDATE = 2;
    DELETE = 3;
}
message RowInBatchWriteRowRequest {
    required OperationType type = 1;
    required bytes row_change = 2; // It is encoded as InplaceRowChangeSet.
    required Condition condition = 3;
    optional ReturnContent return_content = 4;
}
message TableInBatchWriteRowRequest {
    required string table_name = 1;
    repeated RowInBatchWriteRowRequest rows = 2;
}
message BatchWriteRowRequest {
    repeated TableInBatchWriteRowRequest tables = 1;
}
message RowInBatchWriteRowResponse {
    required bool is_ok = 1;
    optional Error error = 2;
    optional ConsumedCapacity consumed = 3;
    optional bytes row = 4;
}
message TableInBatchWriteRowResponse {
    required string table_name = 1;
    repeated RowInBatchWriteRowResponse rows = 2;
}
message BatchWriteRowResponse {
    repeated TableInBatchWriteRowResponse tables = 1;
}
/* ##########################################################################
################################### */
/* ############################################## GetRange ###################
########################### */
enum Direction {
    FORWARD = 0;
    BACKWARD = 1;
}
message GetRangeRequest {
    required string table_name = 1;
    required Direction direction = 2;
    repeated string columns_to_get = 3;  // If this parameter is not specified, all columns are read.
```

```
    optional TimeRange time_range = 4;
    optional int32 max_versions = 5;
    optional int32 limit = 6;
    required bytes inclusive_start_primary_key = 7; // It is encoded as InplaceRowChangeSet, but only con
tains primary key.
    required bytes exclusive_end_primary_key = 8; // It is encoded as InplaceRowChangeSet, but only cont
ains primary key.
    optional bytes filter = 10;
    optional string start_column = 11;
    optional string end_column = 12;
    optional bytes token = 13;
}
message GetRangeResponse {
    required ConsumedCapacity consumed = 1;
    required bytes rows = 2; // It is encoded as InplaceRowChangeSet.
    optional bytes next_start_primary_key = 3; // If this parameter is not specified, all data is read. It is en
coded as InplaceRowChangeSet, but only contains primary key.
    optional bytes next_token = 4;
}
/* ##################### ComputeSplitPointsBySize ##################### */
message ComputeSplitPointsBySizeRequest {
    required string table_name = 1;
    required int64 split_size = 2; // in 100MB
}
message ComputeSplitPointsBySizeResponse {
    required ConsumedCapacity consumed = 1;
    repeated PrimaryKeySchema schema = 2;
    /**
     * Split points between splits, in the ascending order.
     *
     * A split is a consecutive range of primary keys,
     * whose data size is approximately split_size specified in the request.
     * The size could be hard to be precise.
     *
     * A split point is an array of primary-key column w.r.t. table schema,
     * which is never longer than that of table schema.
     * Tailing -inf will be omitted to reduce transmission payloads.
     */
    repeated bytes split_points = 3;
    /**
     * Locations where splits lie.
```

```
    *
    * By the managed nature of TableStore, these locations are no more than hints.
    * If a location is not suitable to be seen, an empty string will be placed.
    */
    message SplitLocation {
        required string location = 1;
        required sint64 repeat = 2;
    }
    repeated SplitLocation locations = 4;
}
```

table_store_filter.proto

```
package com.alicloud.openservices.tablestore.core.protocol;
enum FilterType {
    FT_SINGLE_COLUMN_VALUE = 1;
    FT_COMPOSITE_COLUMN_VALUE = 2;
    FT_COLUMN_PAGINATION = 3;
}
enum ComparatorType {
    CT_EQUAL = 1;
    CT_NOT_EQUAL = 2;
    CT_GREATER_THAN = 3;
    CT_GREATER_EQUAL = 4;
    CT_LESS_THAN = 5;
    CT_LESS_EQUAL = 6;
}
message SingleColumnValueFilter {
    required ComparatorType comparator = 1;
    required string column_name = 2;
    required bytes column_value = 3;
    required bool filter_if_missing = 4;
    required bool latest_version_only = 5;
}
enum LogicalOperator {
    LO_NOT = 1;
    LO_AND = 2;
    LO_OR = 3;
}
message CompositeColumnValueFilter {
    required LogicalOperator combinator = 1;
    repeated Filter sub_filters = 2;
}
message ColumnPaginationFilter {
    required int32 offset = 1;
    required int32 limit = 2;
}
message Filter {
    required FilterType type = 1;
    required bytes filter = 2;  // Serialized string of filter of the type.
}
```

2.5.1.2. DataType

2.5.1.2.1. ActionType

ActionType specifies the operation type in the response of the GetStreamRecord operation. Operation types include:

- PUT_ROW indicates that the operation type is PutRow.
- UPDATE_ROW indicates that the operation type is UpdateRow.
- DELETE_ROW indicates that the operation type is DeleteRow.

Enumeration values

```
enum ActionType {
    PUT_ROW = 1;
    UPDATE_ROW = 2;
    DELETE_ROW = 3;
}
```

2.5.1.2.2. CapacityUnit

CapacityUnit specifies the number of CUs consumed in an operation, or reserved read/write throughput of a table.

Data structure

```
message CapacityUnit {
    optional int32 read = 1;
    optional int32 write = 2;
}
```

read:

- Type: int32
- Description: the number of read CUs consumed by this operation or the reserved read throughput for this table.

write:

- Type: int32
- Description: the number of write CUs consumed by this operation or the reserved write throughput for this table.

2.5.1.2.3. ColumnPaginationFilter

ColumnPaginationFilter specifies the filtering conditions for reading wide rows. This API is applicable to the Filter function.

Data structure

```
message ColumnPaginationFilter {
 required int32 offset = 1;
 required int32 limit = 2;
}
```

offset:

- Type: int32
- Description: the position of the column to start reading from.

limit:

- Type: int32
- Description: the number of columns to be read.

2.5.1.2.4. ComparatorType

ComparatorType is an arithmetical operator. It includes the following enumeration types:

- CT_EQUAL indicates equal to.
- CT_NOT_EQUAL indicates not equal to.
- CT_GREATER_THAN indicates greater than.
- CT_GREATER_EQUAL indicates not smaller than.
- CT_LESS_THAN indicates smaller than.
- CT_LESS_EQUAL indicates not greater than.

Enumeration values

```
enum ComparatorType {
 CT_EQUAL = 1;
 CT_NOT_EQUAL = 2;
 CT_GREATER_THAN = 3;
 CT_GREATER_EQUAL = 4;
 CT_LESS_THAN = 5;
 CT_LESS_EQUAL = 6;
}
```

2.5.1.2.5. CompositeColumnValueFilter

CompositeColumnValueFilter specifies a group of conditions, for example, column_a > 5 AND column_b = 10. This API is applicable to the ConditionUpdate and Filter functions.

Data structure

```
message CompositeColumnValueFilter {
 required LogicalOperator combinator = 1;
 repeated Filter sub_filters = 2;
}
```

combinator:

- Type: LogicalOperator
- Description: the logical operator.

sub_filter:

- Type: Filter
- Description: the sub-condition expression.

2.5.1.2.6. Condition

Condition specifies the row judgment conditions in PutRow, UpdateRow, and DeleteRow. It contains the row_existence and column_condition parameters.

Data structure

```
message Condition {
   required RowExistenceExpectation row_existence = 1;
   optional bytes column_condition     = 2;
}
```

row_existence:

- Type: RowExistenceExpectation
- Description: the row existence check settings for this row.

column_condition:

- Type: bytes
- Description: the column condition settings. This parameter indicates the binary data (in bytes) after the filter is serialized in the Protobuf format.

2.5.1.2.7. ConsumedCapacity

ConsumedCapacity indicates the number of capacity units (CUs) consumed by an operation.

Data structure

```
message ConsumedCapacity {
   required CapacityUnit capacity_unit = 1;
}
```

capacity_unit:

- Type: CapacityUnit
- Description: the number of CUs consumed by this operation.

2.5.1.2.8. Direction

Direction indicates the data query order in the GetRange operation. The two Direction operations are:

- FORWARD indicates that the query proceeds in ascending order of primary key values.
- BACKWARD indicates that the query proceeds in descending order of primary key values.

Enumeration values

```
enum Direction {
 FORWARD = 0;
 BACKWARD = 1;
}
```

2.5.1.2.9. Error

Error indicates an error message returned when an operation fails. This parameter is also used to indicate errors for single-row requests in the BatchGetRow and BatchWriteRow operations.

Data structure

```
Error {
 required string code = 1;
 optional string message = 2;
}
```

code:

- Type: string
- Description: the error code for the specified single-row operation.

message:

- Type: string
- Description: the error message for the specified single-row operation.

2.5.1.2.10. Filter

Filter specifies the column-based conditions. This API is applicable to the Conditional Update and Filter functions.

Data structure

```
message Filter {
 required FilterType type = 1;
 required bytes filter = 2;
}
```

type:

- Type: FilterType
- Description: the column condition type.

filter:

- Type: bytes
- Description: the binary data generated after the condition statements of CompositeColumnValueFilter, ColumnPaginationFilter, or SingleColumnValueFilter are serialized in the Protobuf format.

2.5.1.2.11. PrimaryKeyOption

PrimaryKeyOption specifies the attribute value of a primary key. Currently, it only supports AUTO_INCREMENT.

Enumeration values

```
enum PrimaryKeyOption {
 AUTO_INCREMENT = 1;
}
```

2.5.1.2.12. FilterType

FilterType specifies the type for condition updates or filters. The types include:

- FT_SINGLE_COLUMN_VALUE indicates a single-column condition.
- FT_COMPOSITE_COLUMN_VALUE indicates a multi-column composite condition.
- FT_COLUMN_PAGINATION indicates a wide-row read condition.

Enumeration values

```
enum FilterType {
 FT_SINGLE_COLUMN_VALUE = 1;
 FT_COMPOSITE_COLUMN_VALUE = 2;
 FT_COLUMN_PAGINATION = 3;
}
```

2.5.1.2.13. LogicalOperator

LogicalOperator specifies the enumeration type. The enumeration types include:

- LO_NOT indicates NOT.
- LO_AND indicates AND.
- LO_OR indicates OR.

Enumeration values

```
enum LogicalOperator {
 LO_NOT = 1;
 LO_AND = 2;
 LO_OR = 3;
}
```

2.5.1.2.14. OperationType

OperationType indicates the modification method for one column in UpdateRow. The types of operations include:

- PUT indicates that a column is inserted or data in this column is overwritten.
- UPDATE indicates that a column is updated.
- DELETE indicates that a column is deleted.

Enumeration values

```
enum OperationType {
 PUT = 1;
 UPDATE = 2;
 DELETE = 3;
}
```

2.5.1.2.15. PartitionRange

PartitionRange specifies the partition range.

Data structure

```
message PartitionRange {
   required bytes begin = 1; // encoded as SQLVariant
   required bytes end = 2; // encoded as SQLVariant
}
```

begin:

- Type: bytes
- Description: the starting key of the partition. The partition range is a left-closed right-open interval, which includes the starting key.

end:

- Type: bytes
- Description: the ending key of the partition. The partition range is a left-closed right-open interval, which excludes the ending key.

2.5.1.2.16. PlainBuffer

PlainBuffer is used to format data in Table Store. This is because PlainBuffer delivers better serialization performance and small object resolution than Protocol Buffer.

Format definition

```
plainbuffer = tag_header row1  [row2]  [row3]
row = ( pk [attr] | [pk] attr | pk attr ) [tag_delete_marker] row_checksum;
pk = tag_pk cell_1 [cell_2] [cell_3]
attr  = tag_attr cell1 [cell_2] [cell_3]
cell = tag_cell cell_name [cell_value] [cell_op] [cell_ts] cell_checksum
cell_name = tag_cell_name  formated_value
cell_value = tag_cell_value formated_value
cell_op = tag_cell_op  cell_op_value
cell_ts = tag_cell_ts cell_ts_value
row_checksum = tag_row_checksum row_crc8
cell_checksum = tag_cell_checksum row_crc8
formated_value = value_type value_len value_data
value_type = int8
value_len = int32
cell_op_value = delete_all_version | delete_one_version
cell_ts_value = int64
delete_all_version = 0x01 (1byte)
delete_one_version = 0x03 (1byte)
```

Tag values

```
tag_header = 0x75 (4byte)
tag_pk = 0x01 (1byte)
tag_attr = 0x02 (1byte)
tag_cell = 0x03 (1byte)
tag_cell_name = 0x04 (1byte)
tag_cell_value = 0x05 (1byte)
tag_cell_op = 0x06 (1byte)
tag_cell_ts = 0x07 (1byte)
tag_delete_marker = 0x08 (1byte)
tag_row_checksum = 0x09 (1byte)
tag_cell_checksum = 0x0A (1byte)
```

ValueType values

The values of value_type in formated_value are as follows:

```
VT_INTEGER = 0x0
VT_DOUBLE = 0x1
VT_BOOLEAN = 0x2
VT_STRING = 0x3
VT_NULL = 0x6
VT_BLOB = 0x7
VT_INF_MIN = 0x9
VT_INF_MAX = 0xa
VT_AUTO_INCREMENT = 0xb
```

Checksum calculation

The basic logic to calculate the checksum is as follows:

- The name/value/type/timestamp of each cell is calculated.
- The delete mark of each row is calculated. A byte of 1 is added for each row that has a delete mark. A byte of 0 is added for each row that does not have a delete mark.
- After the checksum is calculated for each cell in a row, these cell checksums are used to calculate the row checksum. The CRC is performed only on the cells in the row, instead of data in the row.

C++ implementation:

```
void GetChecksum(uint8_t* crc, const InplaceCell& cell)
{
    Crc8(crc, cell.GetName());
    Crc8(crc, cell.GetValue(). GetInternalSlice());
    Crc8(crc, cell.GetTimestamp());
    Crc8(crc, cell.GetOpType());
}
void GetChecksum(uint8_t* crc, const InplaceRow& row)
{
    const std::deque<InplaceCell>& pk = row.GetPrimaryKey();
    for (size_t i = 0; i < pk.size(); i++) {
        uint8_t* cellcrc;
        *cellcrc = 0;
        GetChecksum(cellcrc, pk[i]);
        Crc8(crc, *cellcrc);
    }
    for (int i = 0; i < row.GetCellCount(); i++) {
        uint8_t* cellcrc;
        *cellcrc = 0;
        GetChecksum(cellcrc, row.GetCell(i));
        Crc8(crc, *cellcrc);
    }
    uint8_t del = 0;
    if (row.HasDeleteMarker()) {
        del = 1;
    }
    Crc8(crc, del);
}
```

Examples

A row contains two primary key columns and four attribute columns. The data types of the primary key columns are string and integer, while the data types in the attribute columns are string, integer, and double. The versions are 1001, 1002, and 1003. The fourth attribute column indicates whether to delete all versions.

- Primary key columns:
  - [pk1:string:iampk]
  - [pk2:integer:100]
- Attribute columns:
  - [column1:string:bad:1001]
  - [column2:integer:128:1002]

- [column3:double:34.2:1003]
- [column4:del_all_versions]

Encoding:

```
<Header starting>[0x75]
<Primary key column starting>[0x1]
<Cell1>[0x3][0x4][3][pk1][0x5][3][5][iampk]
<Cell2>[0x3][0x4][3][pk2][0x5][0][100]
<Attribute column starting>[0x2]
<Cell1>[0x3][0x4][7][column1][0x5][0x3][3][bad][0x7][1001]
<Cell2>[0x3][0x4][7][column2][0x5][0x0][128][0x7][1002]
<Cell3>[0x3][0x4][7][column3][0x5][0x1][34.2][0x7][1003]
<Cell4>[0x3][0x4][7][column4][0x5][0x6][1]
```

2.5.1.2.17. PrimaryKeySchema

PrimaryKeySchema specifies the attribute value of a primary key.

Data structure

```
message PrimaryKeySchema {
 required string name = 1;
 required PrimaryKeyType type = 2;
 optional PrimaryKeyOption option = 3;
}
```

name:

- Type: string
- Description: the name of the column.

type:

- Type: PrimaryKeyType
- Description: the type of the column.

option:

- Type: PrimaryKeyOption
- Description: the additional attribute value of the column.

2.5.1.2.18. PrimaryKeyType

PrimaryKeyType specifies the type of a primary key.

Enumeration data types

- INTEGER
- STRING

- BINARY

```
enum PrimaryKeyType {
 INTEGER = 1;
 STRING = 2;
 BINARY = 3;
}
```

2.5.1.2.19. ReservedThroughput

ReservedThroughput indicates the reserved read/write throughput value for a table.

Data structure

```
message ReservedThroughput {
 required CapacityUnit capacity_unit = 1;
}
```

capacity_unit:

- Type: CapacityUnit
- Description: the current reserved read/write throughput value for the table.

2.5.1.2.20. ReservedThroughputDetails

ReservedThroughputDetails indicates the reserved read/write throughput information of a table.

Data structure

```
message ReservedThroughputDetails {
   required CapacityUnit capacity_unit = 1;
   required int64 last_increase_time = 2;
   optional int64 last_decrease_time = 3;
   required int32 number_of_decreases_today = 4;
}
```

capacity_unit:

- Type: CapacityUnit
- Description: the reserved read/write throughput value for this table.

last_increase_time:

- Type: int64
- Description: the last time the reserved read/write throughput capacity was raised for this table. The value uses UTC time, in seconds.

last_decrease_time:

- Type: int64

- Description: the last time the reserved read/write throughput capacity was lowered for this table. The value uses UTC time, in seconds.

number_of_decreases_today:

- Type: int32
- Description: the number of times the reserved read/write throughput capacity was lowered for this table on the current calendar day.

2.5.1.2.21. ReturnContent

ReturnContent specifies the content of the returned data.

Data structure

```
message ReturnContent {
    optional ReturnType return_type = 1;
}
```

return_type:

- Type: ReturnType
- Description: the type of the returned data.

2.5.1.2.22. ReturnType

ReturnType specifies the type of the returned data.

Enumeration data types

```
enum ReturnType {
    RT_NONE = 0;
    RT_PK = 1;
}
```

- RT_NONE: the default value. This parameter indicates that no value is returned.
- RT_PK: This parameter indicates that the primary key is returned.

2.5.1.2.23. RowExistenceExpectation

RowExistenceExpectation specifies conditions for row existence. Enumeration types are as follows:

- IGNORE indicates that the row existence check is not performed.
- EXPECT_EXIST indicates that the row is expected to exist.
- EXPECT_NOT_EXIST indicates that this row is not expected to exist.

Enumeration values

```
enum RowExistenceExpectation {
    IGNORE = 0;
    EXPECT_EXIST = 1;
    EXPECT_NOT_EXIST = 2;
}
```

2.5.1.2.24. RowInBatchGetRowResponse

RowInBatchGetRowResponse indicates a row of data in the response of the BatchGetRow operation.

Data structure

```
message RowInBatchGetRowResponse {
 required bool is_ok = 1 [default = true];
 optional Error error = 2;
 optional ConsumedCapacity consumed = 3;
 optional bytes row = 4;
 optional bytes next_token = 5;
}
```

is_ok:

- Type: bool
- Description: determines whether the operation for this row succeeds. If true is returned, the row is read and error is invalid. If false is returned, the row fails to be read and the row is invalid.

error:

- Type: Error
- Description: the error message for this row operation.

consumed:

- Type: ConsumedCapacity
- Description: the number of capacity units consumed by this row operation.

row:

- Type: bytes
- The read data is encoded in the PlainBuffer format.
- If this row does not exist, null is returned.

next_token:

- Type: bytes
- This parameter specifies the starting position of a wide row in the next read operation. This function is currently unavailable.

2.5.1.2.25. RowInBatchWriteRowRequest

RowInBatchWriteRowRequest indicates the information of the row to be written, updated, or deleted in the BatchWriteRow operation.

Data structure

```
message RowInBatchWriteRowRequest {
   required OperationType type = 1;
   required bytes row_change = 2; // It is encoded as InplaceRowChangeSet.
   required Condition condition = 3;
   optional ReturnContent return_content = 4;
}
```

type:

- Type: OperationType
- Description: the operation type.

row_change:

- Type: bytes
- Description: the data in a row that contains the primary key and attribute columns. The columns are encoded in the PlainBuffer format.

condition:

- Type: Condition
- Description: the value of conditional update, including the row existence condition and column-based condition.

return_content:

- Type: ReturnContent
- Required: no
- This parameter specifies the data type after the row is written. Currently, only the primary key is returned, which is used for the auto-increment function of the primary key column.

2.5.1.2.26. RowInBatchWriteRowResponse

RowInBatchWriteRowResponse indicates the write operation result for a row in the response of the BatchWriteRow operation.

Data structure

```
message RowInBatchWriteRowResponse {
 required bool is_ok = 1 [default = true];
 optional Error error = 2;
 optional ConsumedCapacity consumed = 3;
}
```

is_ok:

- Type: bool

- Description: determines whether the operation for this row succeeds. If the value is true, the row is written and error is invalid. If the value is false, this row fails to be written.

error:

- Type: Error
- Description: the error message for this row operation.

consumed:

- Type: ConsumedCapacity
- Description: the number of capacity units consumed by this row operation.

2.5.1.2.27. SingleColumnValueFilter

SingleColumnValueFilter specifies a single condition, for example, column_a > 5. This API is applicable to the ConditionUpdate and Filter functions.

Data structure

```
message SingleColumnValueFilter {
 required ComparatorType comparator = 1;
 required string column_name = 2;
 required bytes column_value = 3;
 required bool filter_if_missing = 4;
 required bool latest_version_only = 5;
}
```

comparator:

- Type: ComparatorType
- Description: the comparison type.

column_name:

- Type: string
- Description: the column name.

column_value:

- Type: bytes
- Description: the value of ColumnValue serialized by protobuf.

filter_if_missing:

- Type: bool
- Description: determines whether a filtering condition is applicable if the column of a row does not exist. Assume that the condition is column_a > 0, and the value of filter_if_missing is true. If column_a does not exist for a row, the condition column_a > 0 is true.

latest_version_only:

- Type: bool
- Description: determines whether a condition is applicable only for the latest version. If the value is true, the value of the latest version is checked to determine whether it meets the condition. If the value is false, the values of all versions are checked to determine whether they meet the conditions.

2.5.1.2.28. StreamDetails

StreamDetails indicates the stream information of a table.

Data structure

```
message StreamDetails {
    required bool enable_stream = 1;
    optional string stream_id = 2;
    optional int32 expiration_time = 3;
    optional int64 last_enable_time = 4;
}
```

enable_stream:

- Type: required bool
- Description: determines whether stream is enabled for the table.

stream_id:

- Type: optional string
- Description: the ID of the table stream.

expiration_time:

- Type: optional int32
- Description: the expiration time of the table stream.

last_enable_time:

- Type: optional int64
- Description: the time to enable the table stream.

2.5.1.2.29. StreamRecord

StreamRecord indicates a row of data in the response of the GetStreamRecord operation.

Data structure

```
message StreamRecord {
    required ActionType action_type = 1;
    required bytes record = 2;
}
```

action_type:

- Type: required ActionType
- Description: the operation type of the row.

record:

- Type: required bytes
- Description: the data content of the row.

2.5.1.2.30. StreamSpecification

StreamSpecification indicates the stream specification of a table.

Data structure

```
message StreamSpecification {
    required bool enable_stream = 1;
    optional int32 expiration_time = 2;
}
```

enable_stream:

- Type: bool
- Description: determines whether stream is enabled for the table.

expiration_time:

- Type: int32
- Description: the expiration time of the table stream.

2.5.1.2.31. TableInBatchGetRowRequest

TableInBatchGetRowRequest indicates the request information of the table to be read in the BatchGetRow operation.

Data structure

```
message TableInBatchGetRowRequest {
    required string table_name = 1;
    repeated bytes primary_key = 2; // The primary key columns are encoded in the PlainBuffer format.
    repeated bytes token = 3;
    repeated string columns_to_get = 4;  // If this parameter is not specified, all columns are read.
    optional TimeRange time_range = 5;
    optional int32 max_versions = 6;
    optional bool cache_blocks = 7 [default = true]; // This parameter specifies whether the read data is written to BlockCache.
    optional bytes filter = 8;
    optional string start_column = 9;
    optional string end_column = 10;
}
```

table_name:

- Type: string
- Description: the name of the table.

primary_key:

- Type: repeated bytes

- Required: yes
- This parameter specifies all primary key columns in the row, including the primary key names and values. The primary key columns are encoded in the PlainBuffer format.

token:

- Type: repeated bytes
- Required: no
- This parameter specifies the starting position of a wide row in the next read operation. This function is currently unavailable.

columns_to_get:

- Type: repeated string
- Description: the names of all columns to be returned from this table.

time_range:

- Type: TimeRange
- Required: At least one of the time_range and max_versions parameters must be specified.
- This parameter specifies the range of timestamps to read versions of data.
- Unit: millisecond. The minimum value of the timestamp is 0. The maximum value of the timestamp is INT64.MAX.
- To query data of a time range, specify start_time and end_time.
- To query data of a specific timestamp, specify specific_time.
- Example: If the value of time_range is (100, 200), the timestamp of the returned column data must be within the range of [100, 200).

max_versions:

- Type: int32
- Required: At least one of the max_versions and time_range parameters must be specified.
- This parameter specifies the maximum number of versions of data to be returned.
- Example: If the value of max_versions is 2, data of a maximum of two versions is returned for each column.

cache_blocks:

- Type: bool
- Required: no
- This parameter specifies whether the read data is written to BlockCache.
- The default value is true.
- This parameter cannot be set to false.

filter:

- Type: bytes
- Required: no
- This parameter specifies the expression of the filtering condition.
- It indicates the binary data after the filter is serialized in the Protobuf format.

start_column:

- Type: string
- Required: no

- This parameter specifies the first column to be read. It is useful for reading wide rows.
- The response contains the specified starting column.
- The column names are sorted lexicographically.
- Example: If a table contains columns A, B, and C, and the value of start_column is B, the data is read starting from column B. Columns B and C are returned.

end_column:

- Type: string
- Required: no
- This parameter specifies the last column to be read. It is useful for reading wide rows.
- The response does not contain the specified ending column.
- The column names are sorted lexicographically.
- Example: If a table contains columns A, B, and C, and the value of end_column is B, the reading stops at column B. Only column A is returned.

2.5.1.2.32. TableInBatchGetRowResponse

TableInBatchGetRowResponse indicates data in a table in the response of the BatchGetRow operation.

Data structure

```
message TableInBatchGetRowResponse {
 required string table_name = 1;
 repeated RowInBatchGetRowResponse rows = 2;
}
```

table_name:

- Type: string
- Description: the name of the table.

rows:

- Type: repeated RowInBatchGetRowResponse
- Description: data of all rows read from the table.

2.5.1.2.33. TableInBatchWriteRowRequest

TableInBatchWriteRowRequest indicates the request information of the table to be written in the BatchWriteRow operation.

Data structure

```
message TableInBatchWriteRowRequest {
 required string table_name = 1;
 repeated RowInBatchWriteRowRequest rows = 2;
}
```

table_name:

- Type: string
- Description: the name of the table.

rows:

- Type: repeated RowInBatchWriteRowRequest
- Description: the information of the row to be inserted, updated, or deleted in the table.

2.5.1.2.34. TableInBatchWriteRowResponse

TableInBatchWriteRowResponse indicates the write results for a table in the BatchWriteRow operation.

Data structure

```
message TableInBatchWriteRowResponse {
 required string table_name = 1;
 repeated RowInBatchWriteRowResponse put_rows = 2;
 repeated RowInBatchWriteRowResponse update_rows = 3;
 repeated RowInBatchWriteRowResponse delete_rows = 4;
}
```

table_name:

- Type: string
- Description: the name of the table.

put_rows:

- Type: RowInBatchWriteRowResponse
- Description: the result of the PutRow operation for the table.

update_rows:

- Type: RowInBatchWriteRowResponse
- Description: the result of the UpdateRow operation for the table.

delete_rows:

- Type: RowInBatchWriteRowResponse
- Description: the result of the DeleteRow operation for the table.

2.5.1.2.35. TableMeta

TableMeta indicates the structure information of a table.

Data structure

```
message TableMeta {
 required string table_name = 1;
 repeated PrimaryKeySchema primary_key = 2;
}
```

table_name:

- Type: string
- Description: the name of the table.

primary_key:

- Type: PrimaryKeySchema
- Description: all primary key columns for the table.

2.5.1.2.36. TableOptions

TableOptions indicates the table parameters, including TimeToLive and MaxVersions.

Data structure

```
message TableOptions {
    optional int32 time_to_live = 1; // This parameter value can be dynamically modified.
    optional int32 max_versions = 2; // This parameter value can be dynamically modified.
    optional int64 deviation_cell_version_in_sec = 5; // This parameter value can be dynamically modified.
}
```

time_to_live:

- Type: int32
- Description: the retention time of data stored in this table, in seconds.

max_versions:

- Type: int32
- Description: the maximum number of versions stored in this table.

deviation_cell_version_in_sec:

- Type: int64
- Description: the maximum version deviation. This parameter is used to forbid writing data that deviates from the expected output. For example, if the value of deviation_cell_version_in_sec is 1,000 and the current timestamp is 10,000, the allowed timestamp range to be written is [10,000 - 1,000, 10,000 + 1,000].

2.5.1.2.37. TimeRange

TimeRange specifies the timestamp range or timestamp value to query.

Data structure

```
message TimeRange {
    optional int64 start_time = 1;
    optional int64 end_time = 2;
    optional int64 specific_time = 3;
}
```

start_time:

- Type: int64
- Description: the starting timestamp, in milliseconds. The minimum value of the timestamp is 0. The maximum value of the timestamp is INT64.MAX.

end_time:

- Type: int64
- Description: the ending timestamp, in milliseconds. The minimum value of the timestamp is 0. The maximum value of the timestamp is INT64.MAX.

specific_time:

- Type: int64
- Description: the specific timestamp, in milliseconds. You can set either specific_time to query a specific timestamp, or a combination of start_time and end_time to query a range of timestamps. The minimum value of the timestamp is 0. The maximum value of the timestamp is INT64.MAX.

2.5.2. SDK reference

2.5.2.1. Java SDK

2.5.2.1.1. Quick start

This topic describes how to obtain and use the Table Store Java SDK.

Environment preparation

You must have a RAM user and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the Java SDK.

Install the Java SDK

Use Maven

To use the Table Store Java SDK in Maven, you only need to add the corresponding dependency to the pom.xml file:

```
<dependency>
    <groupId>com.aliyun.openservices</groupId>
    <artifactId>tablestore</artifactId>
    <version>4.3.1</version>
</dependency>
```

Use the Java SDK

To call the Java SDK, perform the following steps:

1. Create and initialize an instance.
2. Create an API request and set its parameters.
3. Initiate the request and handle its response or exception.

2.5.2.1.2. Use the SDK

2.5.2.2. Python SDK

2.5.2.2.1. Quick start

This topic describes how to obtain and use the Table Store Python SDK.

Environment preparation

You must have a RAM user and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the Python SDK. For more information about how to obtain and view your AccessKey pair in Apsara Stack Management Console, see Obtain an AccessKey pair.

Install the Python SDK

Use one of the following methods to install the Python SDK:

- Method 1: Use pip.

  The command to install the Python SDK is as follows:

  ```
  sudo pip install tablestore
  ```

- Method 2: Use GitHub.

  Make sure that you have installed git, and then run the following command:

  ```
  git clone https://github.com/aliyun/aliyun-tablestore-python-sdk.git
  sudo python setup.py  install
  ```

- Method 3: Use source code.

  i. Download the SDK package.

  ii. Decompress the SDK package, and then run the following command:

  ```
  sudo python setup.py install
  ```

Use the Python SDK

To call the Alibaba Cloud Python SDK, perform the following steps:

1. Create a client instance. When creating the client instance, you must obtain the Region ID, AccessKey ID, and AccessKey Secret.
2. Create an API request and set its parameters.
3. Initiate the request and handle its response or exception.

2.5.2.2.2. Use the SDK

2.5.2.3. C++ SDK

2.5.2.3.1. Quick start

This topic describes how to obtain and use the Table Store C++ SDK.

Environment preparation

You must have a RAM user and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the C++ SDK. For more information about how to obtain and view your AccessKey pair in Apsara Stack Management Console, see Obtain an AccessKey pair.

Install the C++ SDK

For more information about how to install the C++ SDK, see Installation.

Use the C++ SDK

To call the C++ SDK, perform the following steps:

1. Create an instance.
2. Create an API request and set its parameters.
3. Initiate the request and handle its response or exception.

2.5.2.3.2. Use the SDK

2.5.2.4. Go SDK

2.5.2.4.1. Quick start

The Go SDK allows you to access Table Store without performing complex programming operations. This topic describes how to obtain and use the Go SDK.

Environment preparation

You must have a RAM user and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the Go SDK. For more information about how to obtain and view your AccessKey pair in Apsara Stack Management Console, see Obtain an AccessKey pair.

Install the Go SDK

The command to install the Go SDK is as follows:

```
go get github.com/aliyun/aliyun-tablestore-go-sdk
```

Use the Go SDK

To call the Go SDK, perform the following steps:

1. Create an instance.
2. Create an API request and set its parameters.
3. Initiate the request and handle its response or exception.

2.5.2.4.2. Use the SDK

2.5.2.5. NodeJS SDK

2.5.2.5.1. Quick start

The NodeJS SDK allows you to access Table Store without performing complex programming operations. This topic describes how to obtain and use the NodeJS SDK.

Environment preparation

- You must have a RAM user and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the NodeJS SDK. For more information about how to obtain and view your AccessKey pair in Apsara Stack Management Console, see Obtain an AccessKey pair.
- The NodeJS SDK is applicable to Node.js V4.0 and later.

Install the NodeJS SDK

npm

The command to install the NodeJS SDK is as follows:

```
npm install tablestore
```

> **Note** If you encounter any network problems when using npm, you can use cnpm, which is the npm image provided by Taobao.

Use the NodeJS SDK

To call the NodeJS SDK, perform the following steps:

1. Create and initialize an instance.
2. Create an API request and set its parameters.
3. Initiate the request and handle its response or exception.

2.5.2.5.2. Use the SDK

2.5.2.6. .NET SDK

2.5.2.6.1. Quick start

The .NET SDK allows you to access Table Store without performing complex programming operations. This topic describes how to obtain and use the .NET SDK.

Environment preparation

- You must have a RAM user and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the .NET SDK. For more information about how to obtain and view your AccessKey pair in Apsara Stack Management Console, see Obtain an AccessKey pair.
- The .NET SDK is applicable to .NET Framework 4.0 and later.

Install the .NET SDK

To call the SDK of a service, you must install the SDK core library and the SDK of the service. For example, to call the Table Store SDK, you need to obtain and install the SDK core library and the SDK of Table Store. Use either of the following methods to install the .NET SDK:

- Add DLL references
  i. Download the SDK installation package. The Aliyun.TableStore.dll file is in the bin directory.
  ii. In Visual Studio, go to **Solution Explorer** and locate your project. Right-click the project name and choose **Reference** > **Add Reference** from the shortcut menu.
  iii. In the Add Reference dialog box that appears, click **Browse**, and find the directory that contains the SDK package.
  iv. Select the Aliyun.TableStore.dll file in the bin directory and click **OK**.
- Add a project reference
  i. If you want to use the source code to install the SDK package downloaded from GitHub, right-click **Solution** and choose **Add** > **Existing Project** from the shortcut menu.
  ii. In the dialog box that appears, select the aliyun-tablestore-sdk.csproj file, and click **Open**.
  iii. Right-click **Your Project**, and choose **Reference** > **Add Reference** from the shortcut menu. In the dialog box that appears, select the **Project** tab, click the aliyun-tablestore-sdk project, and click **OK**.

Use the .NET SDK

To call the .NET SDK, perform the following steps:

1. Create and initialize an instance.
2. Create an API request and set its parameters.
3. Initiate the request and handle its response or exception.

2.5.2.6.2. Use the SDK

2.5.2.7. Obtain an AccessKey pair

You can obtain the AccessKey pair on the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**.

   The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.6. Network Attached Storage (NAS)

2.6.1. List of operations by function

APIs lists the APIs provided by NAS.

APIs

Number	Category	API	Description
1	Region	DescribeRegions	Returns all region IDs.
2	NAS	CreateFileSystem	Creates a NAS instance.
3	NAS	DeleteFileSystem	Deletes an existing NAS instance.
4	NAS	DescribeFileSystems	Returns the description of a NAS instance.
5	NAS	ModifyFileSystem	Modifies the information of a NAS instance.
6	Mount point	CreateMountTarget	Create a mount point.
7	Mount point	DeleteMountTarget	Deletes an existing mount point.
8	Mount point	DescribeMountTargets	Returns the description of a mount point.
9	Mount point	ModifyMountTarget	Modifies the attributes of a mount point.
10	Permission group	CreateAccessGroup	Creates a permission group.
11	Permission group	DeleteAccessGroup	Deletes an existing permission group.
12	Permission group	DescribeAccessGroups	Returns the description of a permission group.

Number	Category	API	Description
13	Permission group	ModifyAccessGroup	Modifies the attributes of a permission group.
14	Permission group	CreateAccessRule	Creates a permission rule.
15	Permission group	DeleteAccessRule	Deletes an existing permission rule.
16	Permission group	DescribeAccessRules	Returns the description of a permission rule.
17	Permission group	ModifyAccessRule	Modifies the attributes of a permission rule.

2.6.2. Make API requests

2.6.2.1. Common parameters

Common request parameters

Common request parameters are available to all APIs.

Common request parameters

Name	Type	Required	Description
Format	String	No	The type of response. Valid values: JSON and XML. Default value: JSON.
Version	String	Yes	The API version, which is represented as a date in the format of `YYYY-MM-DD`. The current API version is 2017-06-26.
AccessKeyId	String	Yes	The AccessKey ID that is used to access services. For more information, see Obtain an AccessKey pair.
Signature	String	Yes	The string that represents signature.
SignatureMethod	String	Yes	The type of signature. Valid value: HMAC-SHA1.

Name	Type	Required	Description
Timestamp	String	Yes	The time when you send the request. Specify the time in the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time must be in UTC. For example, 2017-05-26T12:00:00Z.
SignatureVersion	String	Yes	The version of the signature algorithm. The current version is 1.0.
SecurityToken	String	No	If Security Token Service (STS) credentials are required, you must specify this parameter.
SignatureNonce	String	No	A unique random number. This parameter is used to prevent replay attacks. You must use different random numbers for different requests.

Sample request

```
GET https://nas.regionid.example.com/?Action=<Action>
&Format=xml
&Version=2017-06-26
&AccessKeyId=key-test
&Signature=Pc5***%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&Timestamp=2012-06-01T12:00:00Z
...
```

Common response parameters

Whenever you send an API request, a GUID that is included in the **RequestId** parameter will be returned to you regardless of whether the request is successful.

Common response parameters

Name	Type	Description
RequestId	Integer	The GUID generated by Alibaba Cloud for the request.

Sample response

XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<An API name+Response>
 <! --Returned RequestId-->
 <RequestId> 6D9F62C5-BF52-447C-AA34-C77F7AFCCC12</RequestId>
 <! --Response parameters-->
</An API name+Response>
```

JSON format

```
{
 "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
 /* Response parameters*/
}
```

2.6.2.2. Structure of a request

Endpoints

The format of a NAS API endpoint is as follows: Obtain an endpoint

Protocols

You can send API requests by using HTTP or HTTPS. We recommend that you use HTTPS to ensure high security.

Request methods

You can send requests by using the HTTP GET method. With this method, you must specify request parameters in the request URL.

Request parameters

You must specify the required operation for the Action parameter of each request, such as `DescribeRegions`. Each operation must include common request parameters and other request parameters that are specific to an operation.

Character encoding

Requests or responses are all encoded by `UTF-8`.

2.6.3. Region

2.6.3.1. DescribeRegions

Description

Return all region IDs.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `DescribeRegions`.
PageSize	Integer	FALSE	The number of regions that are displayed on each page. Default value: 10.
PageNumber	Integer	FALSE	The page number of the list, which starts from 1.

Response parameters

Parameter	Type	Description
TotalCount	Integer	The total number of returned region information records
PageSize	Integer	The number of regions that are displayed on each page
PageNumber	Integer	The page number of the list
Regions	RegionType	The region description

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=DescribeRegions
&PageSize=2
&PageNumber=1
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeRegionsResponse>
 <PageNumber>1</PageNumber>
 <TotalCount>4</TotalCount>
 <PageSize>2</PageSize>
 <RequestId>A70BEE5D-76D3-49FB-B58F-1F398211A5C3</RequestId>
 <Regions>
  <Region>
   <RegionId>cn-hangzhou</RegionId>
   <LocalName>China (Hangzhou)</LocalName>
  </Region>
  <Region>
   <RegionId>cn-shanghai</RegionId>
   <LocalName>China (Shanghai)</LocalName>
  </Region>
 </Regions>
</DescribeRegionsResponse>
```

- JSON format

```
{
 "TotalCount": 4,
 "PageSize": 2,
 "RequestId": "A70BEE5D-76D3-49FB-B58F-1F398211A5C3",
 "PageNumber": 1,
 "Regions": {
  "Region": [
   {
    "RegionId":"cn-hangzhou",
    "LocalName": "China (Hangzhou)"
   },
   {
    "RegionId": "cn-shanghai",
    "LocalName": "China (Shanghai)"
   }
  ]
 }
}
```

2.6.4. NAS instance

2.6.4.1. CreateFileSystem

Description

You can call this operation to create a file system.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this value to `CreateFileSystem`.
StorageType	String	Yes	The type of the file system. Valid values: Performance and Capacity.
ProtocolType	String	Yes	The type of protocol used by the file system.
Description	String	No	The description of the file system. Space ( ) characters are not allowed.
VolumeSize	Long	No	The size of the file system to be created. Note If you do not specify a value for this parameter, the default size of a Performance-type file system is 10 PB and the default size of a Capacity-type file system is 1 PB.

Response parameters

Name	Type	Description
FileSystemId	String	The new file system ID.

Examples

Sample request

```
GET https://nas.regionid.example.com/?Action=CreateFileSystem
&StorageType=Performance
&ProtocolType=NFS
&Description=balabala
&<Common request parameters>
...
```

Sample response

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CreateFileSystemResponse>
 <FileSystemId>1ca404a666</FileSystemId>
 <RequestId>98696EF0-1607-4E9D-B01D-F20930B68845</RequestId>
</CreateFileSystemResponse>
```

- JSON format

```
{
 "RequestId": "98696EF0-1607-4E9D-B01D-F20930B68845",
 "FileSystemId": "1ca404a666"
}
```

2.6.4.2. DeleteFileSystem

Description

You can call this operation to delete an existing NAS instance.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `DeleteFileSystem`.
FileSystemId	String	TRUE	The ID of the NAS instance to be deleted.

Response parameters

None

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=DeleteFileSystem
&FileSystemId=1ca404a348
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteFileSystemResponse>
 <RequestId>9E15E394-38A6-457A-A62A-D9797C9A0262</RequestId>
</DeleteFileSystemResponse>
```

- JSON format

```
{
 "RequestId": "9E15E394-38A6-457A-A62A-D9797C9A0262"
}
```

2.6.4.3. DescribeFileSystems

Description

You can call this operation to retrieve a list of file systems and the details of each file system.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this value to `DescribeFileSystems`.
FileSystemId	String	No	The file system ID.
PageSize	Integer	No	The number of file systems that are displayed on each page. Default value: 10.
PageNumber	Integer	No	The number of a page. The number starts at 1.

Response parameters

Name	Type	Description
TotalCount	Integer	The total number of file systems.
PageSize	Integer	The number of file systems that are displayed on each page.
PageNumber	Integer	The number of a page.
FileSystems	FileSystemType	The file system description.
VolumeSize	Long	The size of the file system to be created. Unit: GB

Examples

Sample request

```
GET https://nas.regionid.example.com/?Action=DescribeFileSystems
&FileSystemId=109c042666
&<Common request parameters>
...
```

Sample response

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeFileSystemsResponse>
 <PageNumber>1</PageNumber>
 <TotalCount>1</TotalCount>
 <PageSize>1</PageSize>
 <RequestId>035B3A3A-E514-4B41-B906-5D906CFBD65F</RequestId>
 <FileSystems>
  <FileSystem>
   <FileSystemId>109c042666</FileSystemId>
   <ProtocolType>NFS</ProtocolType>
   <VolumeSize>10240</VolumeSize>
   <RegionId>cn-hangzhou</RegionId>
   <CreateTime>2017-05-27T15:43:06CST</CreateTime>
   <Destription/>
   <MountTargets>
    <MountTarget>
     <MountTargetDomain>109c042666-wjb85.regionid.nas.example.com</MountTargetDomain>
    </MountTarget>
   </MountTargets>
   <StorageType>Performance</StorageType>
   <MeteredSize>1611661312</MeteredSize>
  </FileSystem>
 </FileSystems>
</DescribeFileSystemsResponse>
```

- JSON format

```
{
 "FileSystems": {
  "FileSystem": [
   {
    "StorageType": "Performance",
    "ProtocolType": "NFS",
    "CreateTime": "2017-05-27T15:43:06CST",
  "VolumeSize": "10240",
    "Destription": "",
    "MountTargets": {
     "MountTarget": {
      {
       "MountTargetDomain": "109c042666-wjb85.regionid.nas.example.com"
      }
     ]
    },
    "FileSystemId": "109c042666",
    "RegionId": "cn-hangzhou",
    "MeteredSize": 1611661312
   }
  ]
 },
 "TotalCount": 1,
 "PageSize": 1,
 "RequestId": "035B3A3A-E514-4B41-B906-5D906CFBD65F",
 "PageNumber": 1
}
```


2.6.4.4. ModifyFileSystem

Description

You can call this operation to modify the NAS instance information.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `ModifyFileSystem`.
FileSystemId	String	TRUE	The NAS instance ID.

Parameter	Type	Required	Description
Description	String	FALSE	The description. Space characters are not allowed.

Response parameters

None

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=ModifyFileSystem
&FileSystemId=1ca404a666
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyFileSystemResponse>
 <RequestId>5BC5CB97-9F28-42FE-84A4-0CD0DF4211C8</RequestId>
</ModifyFileSystemResponse>
```

- JSON format

```
{
 "RequestId": "5BC5CB97-9F28-42FE-84A4-0CD0DF4211C8"
}
```

2.6.5. Mount point

2.6.5.1. CreateMountTarget

Description

You can call this operation to create a mount point.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `CreateMountTarget`.

Parameter	Type	Required	Description
FileSystemId	String	TRUE	The NAS instance ID.
AccessGroupName	String	TRUE	The permission group name.
NetworkType	String	TRUE	The network type. Valid values: VPC and Classic.
VpcId	String	FALSE	The VPC ID.
VSwitchId	String	FALSE	The VSwitch ID.

Response parameters

Parameter	Type	Description
MountTargetDomain	String	The domain name of the mount point

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=CreateMountTarget
&FileSystemId=174494b666
&AccessGroupName=classic-test
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CreateMountTargetResponse>
  <RequestId>70EACC9C-D07A-4A34-ADA4-77506C42B023</RequestId>
  <MountTargetDomain>174494b666-xog95.regionid.nas.example.com</MountTargetDomain>
</CreateMountTargetResponse>
```

- JSON format

```
{
  "RequestId": "70EACC9C-D07A-4A34-ADA4-77506C42B023",
  "MountTargetDomain": "174494b666-xog95.regionid.nas.example.com"
}
```

2.6.5.2. DeleteMountTarget

Description

You can call this operation to delete an existing mount point.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `DeleteMountTarget`.
FileSystemId	String	TRUE	The NAS instance ID.
MountTargetDomain	String	TRUE	The domain name of the mount point.

Response parameters

None

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=DeleteMountTarget
&FileSystemId=174494b666
&MountTargetDomain=174494b666-xog95.regionid.nas.example.com
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteMountTargetResponse>
 <RequestId>5BC5CB97-9F28-42FE-84A4-0CD0DF4211C8</RequestId>
</DeleteMountTargetResponse>
```

- JSON format

```
{
 "RequestId": "5BC5CB97-9F28-42FE-84A4-0CD0DF4211C8"
}
```

2.6.5.3. DescribeMountTargets

Description

You can call this operation to retrieve a list of mount points and the details of each mount point.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this value to `DescribeMountTargets`.
FileSystemId	String	Yes	The file system ID.
MountTargetDomain	String	No	The name of the mount point.
PageSize	Integer	No	The number of mount points that are displayed on each page. Default value: 10.
PageNumber	Integer	No	The number of a page. The number starts at 1.

Response parameters

Name	Type	Description
TotalCount	Integer	The total number of mount points.
PageSize	Integer	The number of mount points that are displayed on each page.
PageNumber	Integer	The number of a page.
MountTargets	MountTargetType	A list of mount points and the details of each mount point.

Examples

Sample request

```
GET https://nas.regionid.example.com/?Action=DescribeMountTargets
&FileSystemId=1ca404a666
&<Common request parameters>
...
```

Sample response

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<? xml version="1.0" encoding="UTF-8"? >
<DescribeMountTargetsResponse>
 <PageNumber>1</PageNumber>
 <TotalCount>1</TotalCount>
 <PageSize>1</PageSize>
 <RequestId>3BAB90FD-B4A0-48DA-9F09-2B963510A0EF</RequestId>
 <MountTargets>
  <MountTarget>
   <Status>Active</Status>
   <NetworkType>Vpc</NetworkType>
   <VswId>vsw-2zevmwkwyztjuoffg****</VswId>
   <VpcId>vpc-2zesj9afh3y518k9o****</VpcId>
   <MountTargetDomain>1ca404a666-XXXXX.regionid.nas.example.com</MountTargetDomain>
   <AccessGroup>DEFAULT_VPC_GROUP_NAME</AccessGroup>
  </MountTarget>
 </MountTargets>
</DescribeMountTargetsResponse>
```

- JSON format

```
{
 "TotalCount": 1,
 "PageSize": 1,
 "RequestId": "3BAB90FD-B4A0-48DA-9F09-2B963510A0EF",
 "PageNumber": 1,
 "MountTargets": {
  "MountTarget": [
   {
    "Status": "Active",
    "VswId": "vsw-2zevmwkwyztjuoffg****",
    "VpcId": "vpc-2zesj9afh3y518k9o****",
    "MountTargetDomain": "1ca404a666-.regionid.nas.example.com",
    "NetworkType": "Vpc",
    "AccessGroup": "DEFAULT_VPC_GROUP_NAME"
   }
  ]
 }
}
```

2.6.5.4. ModifyMountTarget

Description

You can call this operation to modify the information of a mount point.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `ModifyMountTarget`.
FileSystemId	String	TRUE	The NAS instance ID.
MountTargetDomain	String	TRUE	The domain name of the mount point.
AccessGroupName	String	FALSE	The permission group name.
Status	String	FALSE	The status. Valid values: Active and Inactive.

Response parameters

None

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=ModifyMountTarget
&FileSystemId=1ca404a666
&MountTargetDomain=1ca404a666
&Status=Inactive
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyMountTargetResponse>
  <RequestId>FF387D95-34C4-4879-B65A-99D1FA1B65CD</RequestId>
</ModifyMountTargetResponse>
```

- JSON format

```
{
  "RequestId": "FF387D95-34C4-4879-B65A-99D1FA1B65CD"
}
```

2.6.6. Permission group

2.6.6.1. CreateAccessGroup

Description

You can call this operation to create a permission group.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `CreateAccessGroup`.
AccessGroupName	String	TRUE	The permission group name.
AccessGroupType	String	TRUE	The permission group type. Valid values: VPC and Classic.
Description	String	FALSE	The permission group description. It is the same as the permission group name by default.

Response parameters

Parameter	Type	Description
AccessGroupName	String	The permission group name

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=CreatAccessGroup
&AccessGroupName=classic-test
&AccessGroupType=Classic
&Description=classic test access group
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CreateAccessGroupResponse>
 <RequestId>55C5FFD6-BF99-41BD-9C66-FFF39189F4F8</RequestId>
 <AccessGroupName>classic-test</AccessGroupName>
</CreateAccessGroupResponse>
```

- JSON format

```
{
 "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8",
 "AccessGroupName ": "classic-test"
}
```

2.6.6.2. CreateAccessRule

Description

You can call this operation to create a permission rule.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `CreateAccessRule`.
AccessGroupName	String	TRUE	The permission group name.
SourceCidrIp	String	TRUE	The IP address or address segment.
RWAccessType	String	FALSE	The access permission type. Valid values: • RDWR (default) • RDONLY
UserAccessType	String	FALSE	The user permission type. Valid values: • no_squash (default) • root_squash • all_squash

Parameter	Type	Required	Description
Priority	Integer	FALSE	The priority. Valid values: 1 to 100. Default value: 1.

Response parameters

Parameter	Type	Description
AccessRuleId	String	The rule serial number

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=CreatAccessRule
&AccessGroupName=classic-test
&SourceCidrIp=10.0.0.1/32
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CreateAccessRuleResponse>
 <AccessRuleId>1</AccessRuleId>
 <RequestId>A323836B-5BC6-45A6-8048-60675C23EE2A</RequestId>
</CreateAccessRuleResponse>
```

- JSON format

```
{
 "RequestId": "A323836B-5BC6-45A6-8048-60675C23EE2A",
 "AccessRuleId": "1"
}
```

2.6.6.3. DeleteAccessGroup

Description

You can call this operation to delete an existing permission group.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `DeleteAccessGroup`.
AccessGroupName	String	TRUE	The permission group name.

Response parameters

None

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=DeleteAccessGroup
&AccessGroupName=classic-test
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteAccessGroupResponse>
 <RequestId>5BC5CB97-9F28-42FE-84A4-0CD0DF4211C8</RequestId>
</DeleteAccessGroupResponse>
```

- JSON format

```
{
 "RequestId": "9E15E394-38A6-457A-A62A-D9797C9A0262"
}
```

2.6.6.4. DeleteAccessRule

Description

You can call this operation to delete an existing permission rule.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `DeleteAccessRule`.
AccessGroupName	String	TRUE	The permission group name.
AccessRuleId	String	TRUE	The rule serial number.

Response parameters

None

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=CreatAccessRule
&AccessGroupName=classic-test
&AccessRuleId=1
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteAccessRuleResponse>
 <RequestId>5B4511A7-C99E-4071-AA8C-32E2529DA963</RequestId>
</DeleteAccessRuleResponse>
```

- JSON format

```
{
 "RequestId": "5B4511A7-C99E-4071-AA8C-32E2529DA963",
}
```

2.6.6.5. DescribeAccessGroups

Description

You can call this operation to return the description of a permission group.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `DescribeAccessGroups`.
AccessGroupName	String	FALSE	The permission group name.
PageSize	Integer	FALSE	The number of permission groups that are displayed on each page. Default value: 10.
PageNumber	Integer	FALSE	The page number of the list, which starts from 1.

Response parameters

Parameter	Type	Description
TotalCount	Integer	The total number of permission groups
PageSize	Integer	The number of permission groups that are displayed on each page
PageNumber	Integer	The page number of the list
AccessGroups	String	The permission group description

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=DescribeAccessGroups
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeAccessGroupsResponse>
 <PageNumber>1</PageNumber>
 <TotalCount>2</TotalCount>
 <PageSize>2</PageSize>
 <RequestId>3E569F4A-F743-490B-AC01-A8088F5C17A1</RequestId>
 <AccessGroups>
  <AccessGroup>
   <Description>DEFAULT ACCESS GROUP NAME</Description>
   <RuleCount>1</RuleCount>
   <AccessGroupType>Vpc</AccessGroupType>
   <AccessGroupName>DEFAULT_VPC_GROUP_NAME</AccessGroupName>
   <MountTargetCount>8</MountTargetCount>
  </AccessGroup>
  <AccessGroup>
   <Description>This is a classic test access group~</Description>
   <RuleCount>0</RuleCount>
   <AccessGroupType>Classic</AccessGroupType>
   <AccessGroupName>classic-test</AccessGroupName>
   <MountTargetCount>0</MountTargetCount>
  </AccessGroup>
 </AccessGroups>
</DescribeAccessGroupsResponse>
```

- JSON format

```
{
 "AccessGroups": {
  "AccessGroup": [
   {
    "RuleCount": 1,
    "AccessGroupType": "Vpc",
    "Description": "DEFAULT ACCESS GROUP NAME",
    "AccessGroupName": "DEFAULT_VPC_GROUP_NAME",
    "MountTargetCount": 8
   },
   {
    "RuleCount": 0,
    "AccessGroupType": "Classic",
    "Description": "This is a classic test access group~",
    "AccessGroupName": "classic-test",
    "MountTargetCount": 0
   }
  ]
 },
 "TotalCount": 2,
 "PageSize": 2,
 "RequestId": "2514F97E-FFF0-4A1F-BF04-729CEAC64B6F",
 "PageNumber": 1
}
```


2.6.6.6. DescribeAccessRules

Description

You can call this operation to retrieve a list of permission group rules and the details of each rule.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this value to `DescribeAccessRules`.
AccessGroupName	String	Yes	The name of the permission group.
AccessRuleId	String	No	The rule ID.

Name	Type	Required	Description
PageSize	Integer	No	The number of rules that are displayed on each page. Default value: 10.
PageNumber	Integer	No	The number of a page. The number starts at 1.

Response parameters

Name	Type	Description
TotalCount	Integer	The total number of rules.
PageSize	Integer	The number of rules that are displayed on each page.
PageNumber	Integer	The number of a page.
AccessRules	AccessRules	The description of a rule.

Examples

Sample request

```
GET https://nas.regionid.example.com/?Action=DescribeAccessRules
&AccessGroupName=classic-test
&<Common request parameters>
...
```

Sample response

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeAccessRulesResponse>
 <AccessRules>
  <AccessRule>
   <SourceCidrIp>10.0.XX.XX/32</SourceCidrIp>
   <AccessRuleId>1</AccessRuleId>
   <RWAccess>RDWR</RWAccess>
   <UserAccess>no_squash</UserAccess>
   <Priority>1</Priority>
  </AccessRule>
 </AccessRules>
 <PageNumber>1</PageNumber>
 <TotalCount>1</TotalCount>
 <PageSize>1</PageSize>
 <RequestId>86D89E82-4297-4343-8E1E-A2495B35CC70</RequestId>
</DescribeAccessRulesResponse>
```

- JSON format

```
{
 "TotalCount": 1,
 "PageSize": 1,
 "RequestId": "86D89E82-4297-4343-8E1E-A2495B35CC70",
 "PageNumber": 1,
 "AccessRules": {
  "AccessRule": [
   {
    "RWAccess": "RDWR",
    "UserAccess": "no_squash",
    "Priority": 1,
    "SourceCidrIp": "10.0.XX.XX/32",
    "AccessRuleId": "1"
   }
  ]
 }
}
```

2.6.6.7. ModifyAccessGroup

Description

You can call this operation to modify a permission group.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `ModifyAccessGroup`.
AccessGroupName	String	TRUE	The permission group name.
Description	String	FALSE	The permission group description.

Response parameters

None

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=ModifyAccessGroup
&AccessGroupName=classic-test
&Description=classic-test
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyAccessGroupResponse>
  <RequestId>ED2AE737-9D50-4CA4-B0DA-31BD610C2363</RequestId>
</ModifyAccessGroupResponse>
```

- JSON format

```
{
  "RequestId": "ED2AE737-9D50-4CA4-B0DA-31BD610C2363"
}
```

2.6.6.8. ModifyAccessRule

Description

You can call this operation to delete a permission rule.

Request parameters

Parameter	Type	Required	Description
Action	String	TRUE	The operation that you want to perform. Set the value to `ModifyAccessRule`.
AccessGroupName	String	TRUE	The permission group name.
AccessRuleId	String	TRUE	The rule serial number.
SourceCidrIp	String	FALSE	The IP address or address segment.
RWAccessType	String	FALSE	The access permission type.
UserAccessType	String	FALSE	The user permission type.
Priority	Integer	FALSE	The priority. Valid values: 1 to 100. Default value: 1.

Response parameters

None

Examples

Sample requests

```
GET https://nas.regionid.example.com/?Action=ModifyAccessRule
&AccessGroupName=classic-test
&AccessRuleId=1
&SourceCidrIp=192.168.0.1
&RWAccessType=RDWR
&UserAccessType=all_squash
&<Common request parameters>
...
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyAccessRuleResponse>
  <RequestId>6299428C-3861-435D-AE54-9B330A0007C8</RequestId>
</ModifyAccessRuleResponse>
```

- JSON format

```
{
  "RequestId": "6299428C-3861-435D-AE54-9B330A0007C8",
}
```

2.6.7. Appendix: Error codes

An error code consists of four components, as listed in Error codes.

Error codes

Component	Description
HttpCode	The HTTP response code that complies with HTTP syntax
Code	The error code
Message	The error message
Advice	The recommended solution

Error codes

HTTP status code	Code	Message	Advice
500	InternalError	A system internal error occurred.	Please try again later.
503	ServiceUnavailable	This service is unavailable right now.	Please try again later.
504	ServiceTimeout	Service request timed out.	Please try again later.
503	SubRam.CheckFailed	The sub user ram check has failed due to some internal error.	Please try again later.
503	VpcRam.CheckFailed	The Vpc ram check has failed due to some internal error.	Please try again later.
503	VpcSubRam.CheckFailed	The Vpc sub user ram check has failed due to some internal error.	Please try again later.
400	MissingParameter.callerUid	Request parameter missing: callerUid is not specified.	Add the callerUid request parameter.

HTTP status code	Code	Message	Advice
400	MissingParameter.RegionId	Request parameter missing: RegionId of the domain name is not specified.	Add the RegionId field to the domain name.
400	MissingParameter.VSwitchId	Request parameter missing: VSwitchId is not specified.	Add the VSwitchId request parameter.
400	MissingParameter.VpcId	Request parameter missing: VpcId is not specified.	Add the VpcId request parameter.
400	InvalidParameter.StorageType	Invalid request parameter: StorageType is invalid.	Set StorageType to Performance or Capacity.
400	InvalidParameter.ProtocalType	Invalid request parameter: ProtocalType is invalid.	Set ProtocalType to NFS.
400	InvalidParameter.Description	Invalid request parameter: Description contains invalid characters.	Set Description to a string that contains English letters and special characters such as at signs (@), number signs (#), dollar signs ($), underscores (_), plus signs (+), and hyphens (-).
404	InvalidFileSystem.NotFound	The specified NAS instance does not exist.	The specified NAS instance does not exist or has been deleted.
403	InvalidFileSystem.AlreadyExisted	The specified NAS instance already exists.	Call DescribeFileSystems and specify the NAS instance ID to view the instance information.
404	InvalidMountTarget.NotFound	The specified mount point does not exist.	The specified mount point does not exist or has been deleted.
404	InvalidAccessGroup.NotFound	The specified permission group does not exist.	The specified permission group does not exist or has been deleted.

HTTP status code	Code	Message	Advice
403	InvalidAccessGroup.AlreadyExisted	The specified permission group already exists.	Call DescribeMountTargets and specify the permission group to view its information.
403	InvalidAccessGroup.AlreadyAttached	The specified permission group has been bound to a mount point.	Unbind the permission group from the mount point before deleting the permission group.
404	InvalidAccessRule.NotFound	The specified permission rule does not exist.	The specified permission rule does not exist or has been deleted.
404	InvalidLocatin.NotFound	The specified location does not exist.	The requested location does not exist or is not providing services.
404	InvalidRegionId.NotFound	The specified region does not exist.	The requested region does not exist or is not providing services.
404	InvalidAZone.NotFound	The specified zone does not exist.	The requested zone does not exist or is not providing services.
404	InvalidVpc.NotFound	The specified VPC does not exist.	Create a VPC first.
404	InvalidVip.NotFound	The specified VIP does not exist.	Make sure that there are available IP addresses in your VPC.
404	InvalidLBid.NotFound	The specified LBid does not exist.	Please try again later.
404	InvalidVpcTunnelId.NotFound	The specified VPC tunnelId does not exist.	Check the VPC information first.
404	InvalidVpc.CreationFailed	The specified vpc instance creation failed.	Make sure that the VPC information is correct and there is an available IP address for the VPC, and then try again.
403	OperationDenied.DefaultAccessGroupCannotDelete	Operation not allowed: The default permission group cannot be deleted.	You can only edit custom permission groups.

HTTP status code	Code	Message	Advice
403	OperationDenied.DefaultAccessGroupCannotModify	Operation not allowed: The default permission group cannot be modified.	You can only edit custom permission groups.
403	OperationDenied.NetworkTypeNotMatched	Operation not allowed: The mount point network type does not match the AccessGroupType.	Make sure that the NetworkType of the mount point and the AccessGroupType of the permission group are consistent.
403	OperationDenied.MountTargetNotEmpty	Operation not allowed: The specified NAS instance already has a mount point. Delete the existing mount point first.	Delete the existing mount points first.
403	OperationDenied.FileSystemCountsExceeded	The number of NAS instances has already reached the upper limit (a user can create a maximum of 10 NAS instances).	To raise the limit, contact technical support.
403	OperationDenied.MountTargetCountsExceeded	The number of mount points has already reached the upper limit (a maximum of two mount points can be created for each NAS instance).	To raise the limit, contact technical support.
403	OperationDenied.AccessGroupCountsExceeded	The number of permission groups has already reached the upper limit.	To raise the limit, contact technical support.
403	OperationDenied.AccessRuleCountsExceeded	The number of permission rules has already reached the upper limit.	To raise the limit, contact technical support.
403	Forbidden.InvalidUserType	No permission: The user type is invalid.	Sorry, this API does not support your account type.
403	Forbbiden.Ram	User not authorized to operate on the specified resource, or this API doesn't support RAM.	Access RAM to grant required NAS permissions.

HTTP status code	Code	Message	Advice
403	NotQualified	No public beta qualification yet	Please initiate an application for a trial of the related features. If your application fails to be approved, contact the technical support.

Error response examples

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<Error>
 <RequestId>B71B4C68-6C6B-4D4B-AD70-8951BD7D188E</RequestId>
 <HostId>nas.regionid.example.com</HostId>
 <Code>InvalidFileSystem.NotFound</Code>
 <Message>The specified NAS instance does not exist.</Message>
</Error>
```

- JSON format

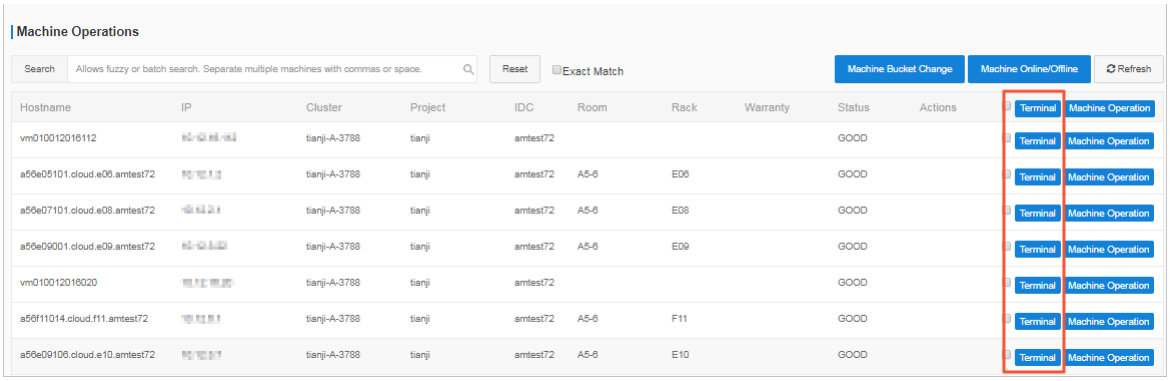
```
{
 "RequestId": "B71B4C68-6C6B-4D4B-AD70-8951BD7D188E",
 "HostId": " nas.regionid.example.com ",
 "Code": "InvalidFileSystem.NotFound",
 "Message": "The specified NAS instance does not exist."
}
```

2.6.8. Obtain an endpoint

You can obtain the product endpoint in Apsara Stack Operations.

Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms > Apsara Stack Operations > Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. Choose **Operations > Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the command **curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration"** to obtain JSON data.

7. Based on the ID (*nas-yaochi*) and key value (*nas.openapi.endpoint*) of a *NAS* file system, you can locate the endpoint of the *NAS* file system.

2.6.9. Obtain an AccessKey pair

You can obtain the AccessKey pair on the Apsara Stack console.

Obtain an AccessKey pair of a department

You can obtain an AccessKey pair of a department as follows:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

You can obtain an AccessKey pair of a personal account as follows:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**. The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.7. Apsara File Storage for HDFS

2.7.1. API reference

2.7.1.1. List of operations by function

This topic introduces the Apsara File Storage for HDFS operations that you can call.

> **Note** This API reference is intended for HDFS API version 2018-02-28.

No.	Category	Operation	Description
1	Regions	ListRegions	Queries all region IDs.
2	Region	GetRegion	Queries the configuration information in a specified region.
3	File system	CreateFileSystem	Creates a file system instance.
4	File system	DeleteFileSystem	Deletes an existing file system instance.
5	File system	ModifyFileSystem	Modifies the attributes of a file system.

No.	Category	Operation	Description
6	File system	GetFileSystem	Queries the detailed information about a file system instance.
7	File system	ListFileSystems	Queries the detailed information about multiple file system instances.
8	Permission	CreateAccessGroup	Creates a permission group.
9	Permission	DeleteAccessGroup	Deletes a permission group.
10	Permission	ModifyAccessGroup	Modifies the attributes of a permission group.
11	Permission	GetAccessGroup	Queries detailed information about a permission group.
12	Permission	ListAccessGroups	Queries detailed information about permission groups in batches.
13	Permission	CreateAccessRule	Creates a permission rule.
14	Permission	DeleteAccessRule	Deletes a permission rule.
15	Permission	ModifyAccessRule	Modifies attributes about a rule.
16	Permission	GetAccessRule	Queries detailed information about a permission rule.
17	Permission	ListAccessRules	Queries detailed information about permission rules in batches.
18	Mount point	CreateMountPoint	Creates a mount point.
19	Mount point	DeleteMountPoint	Deletes a mount point.
20	Mount point	ModifyMountPoint	Modifies the attributes of a mount point.

No.	Category	Operation	Description
21	Mount point	GetMountPoint	Queries detailed information about a mount point.
22	Mount point	ListMountPoints	Queries detailed information about mount points in batches.

2.7.1.2. Make API requests

2.7.1.2.1. Common parameters

This topic describes the common request parameters and response parameters of Apsara File Storage for HDFS.

Common request parameters

Common request parameters must be included in the request of each API.

Common request parameters

Parameter	Type	Required	Description
Format	String	No	The type of the returned value. Valid values: JSON and XML. Default value: JSON.
Version	String	Yes	The API version, in the format of `YYYY-MM-DD`. The current version is 2018-02-28.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature string.
SignatureMethod	String	Yes	The signature method. Set this parameter to HMAC-SHA1.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time must be in UTC. For example, 2017-05-26T12:00:00Z.

Parameter	Type	Required	Description
SignatureVersion	String	Yes	The signature algorithm version. The current version is 1.0.
SecurityToken	String	No	The security token. This parameter is required when STS credentials are used.
SignatureNonce	String	No	A unique random number. This parameter is used to prevent replay attacks. You must use a different random number for each request.

Sample requests

```
GET https://dfs.regionid.example.com/?Action=<Action>
&Format=xml
&Version=2018-02-28
&AccessKeyId=key-test
&Signature=Pc5WB8gokVn0xfeu%2FZV%2BiNM1dg****
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&Timestamp=2012-06-01T12:00:00Z
...
```

Common response parameters

The system returns a unique identifier (**RequestId**) for each API request, regardless of whether the API operation was called successfully.

Common response parameters

Parameter	Type	Description
RequestId	Integer	The unique ID of the request.

Sample responses

XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<Operation name+Response>
 <! --Returned request tag-->
 <RequestId> 6D9F62C5-BF52-447C-AA34-C77F7AFCCC12</RequestId>
 <! --Returned results-->
</Operation name+Response>
```

JSON format

```
{
 "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
 /* Response data */
}
```

2.7.1.2.2. Request structure

This topic describes the endpoints, protocols, methods, parameters, and encoding methods involved in the request structure.

Endpoints

For information about how to query the endpoints of Apsara File Storage for HDFS APIs, see Obtain an endpoint.

Protocols

You can send API requests over HTTP or HTTPS. For security considerations, we recommend that you use HTTPS.

Methods

You can call an API operation by sending an HTTP GET request. If you use this method, the request parameters must be included in the request URL.

Request parameters

For each request, you must specify the Action parameter (such as `ListRegions`), common request parameters, and API-specific parameters.

Encoding

Requests and responses are encoded using `UTF-8`.

2.7.1.3. Regions

2.7.1.3.1. ListRegions

You can call this operation to query the IDs of all regions that support Apsara File Storage for HDFS deployment.

Request parameters

Parameter	Type	Required	Description
StartOffset	Integer	FALSE	The start position. Default value: 1.
Limit	Integer	FALSE	The maximum number of entries to return. Default value: 10.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of entries returned. Maximum value: the value of the Limit parameter.
Regions	Array(Region)	The list of region IDs.
Region.Index	Integer	The serial number of the region.
Region.RegionId	String	The ID of the zone.
Region.RegionName	String	The name of the region.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=ListRegions
&StartOffset=10
&Limit=10
&<Common request parameters>
```

Sample responses

- JSON format

```
{
 "Regions": {
  {
   "Index": 3,
   "RegionId": "cn-shanghai",
   "RegionName": "China (Hangzhou)"
  }
 ],
 "TotalCount": 1,
 "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```


2.7.1.3.2. GetRegion

You can call this operation to query the configuration information of each zone in a region, namely the storage medium types that the user can purchase and the supported access interfaces. Configurations may vary with zones.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
AvailableZones	Array(AvailableZone)	The list of zones.
AvailableZone.ZoneId	String	The ID of the zone.
AvailableZone.Options	Array(Option)	The list of configurations.
AvailableZone.Option.ProtocolType	String	The interface protocol type. Set this parameter to HDFS. This value indicates Hadoop FileSystem.
AvailableZone.Option.StorageType	String	The type of the storage medium. Set this parameter to STANDARD.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=GetRegion
&InputRegionId=cn-hangzhou
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "AvailableZones": [
    {
      "Options": [
        {
          "ProtocolType": "HDFS",
          "StorageType": "STANDARD"
        }
      ],
      "ZoneId": "cn-hangzhou-b"
    }
  ],
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.4. File systems

2.7.1.4.1. CreateFileSystem

You can call this operation to create a file system instance.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
ZoneId	String	TRUE	The ID of the zone.
ProtocolType	String	TRUE	The interface protocol type. Set this parameter to HDFS.

Parameter	Type	Required	Description
StorageType	String	TRUE	The type of the storage medium. Set this parameter to STANDARD.
Description	String	FALSE	The custom description. Maximum length: 100 bytes.
FileSystemName	String	TRUE	The name of the file system instance. This parameter cannot be an empty string. Specify a globally unique value to avoid confusion. Maximum length: 100 bytes.
SpaceCapacity	Long	TRUE	The estimated capacity of the file system instance. Unit: GB. When the amount of stored data reaches this value, write requests fail, but stored data is not affected.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
FileSystemId	String	The ID of the file system instance.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=CreateFileSystem
&InputRegionId=cn-hangzhou
&ZoneId=cn-hangzhou-b
&ProtocolType=HDFS
&StorageType=STANDARD
&Description=This is the first Apsara File Storage for HDFS instance of my company.
&FileSystemName=MyFirstDFS
&SpaceCapacity=1024
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "FileSystemId": "037cb4****",
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.4.2. DeleteFileSystem

You can call this operation to delete an existing file system instance. The file system instance to be deleted must have no mount points. If the file system instance to be deleted has a mount point, deletion fails.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
FileSystemId	String	TRUE	The ID of the specified file system instance.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=DeleteFileSystem
&InputRegionId=cn-hangzhou
&FileSystemId=037cb4****
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.4.3. ModifyFileSystem

You can call this operation to modify the attributes of a file system, such as name, description, and estimated capacity.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
FileSystemId	String	TRUE	The ID of the specified file system instance.
FileSystemName	String	FALSE	The name of the file system. This parameter cannot be an empty string. Specify a globally unique value to avoid confusion. Maximum length: 100 bytes.
SpaceCapacity	Long	FALSE	The estimated capacity of the file system instance. Unit: GB.
Description	String	FALSE	The custom description. Maximum length: 100 bytes.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=ModifyFileSystem
&InputRegionId=cn-hangzhou
&FileSystemId=037cb4****
&FileSystemName=MyFirstDFS
&SpaceCapacity=1024
&Description=This is the first Apsara File Storage for HDFS instance of my company.
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.4.4. GetFileSystem

You can call this operation to query the detailed information about a file system instance.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
FileSystemId	String	TRUE	The ID of the specified file system instance.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
FileSystem	Struct	The detailed information about the file system.

Parameter	Type	Description
FileSystem.RegionId	String	The ID of the region.
FileSystem.ZoneId	String	The ID of the zone.
FileSystem.FileSystemName	String	The name of the file system instance.
FileSystem.Description	String	The description of the file system instance.
FileSystem.ProtocolType	String	The interface protocol type.
FileSystem.StorageType	String	The type of the storage medium.
FileSystem.SpaceCapacity	Long	The estimated capacity of the file system instance. Unit: GB.
FileSystem.MountPointCount	Long	The number of mount points.
FileSystem.FileSystemId	String	The ID of the file system instance.
FileSystem.CreateTime	String	The time at which the file system was created.
FileSystem.UsedSpaceSize	Float	The space in use. Unit: GB.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=GetFileSystem
&InputRegionId=cn-hangzhou
&FileSystemId=037cb4****
&<Common request parameters>
```

Sample responses

- JSON format

```
{
 "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8",
 "FileSystem": {
  "SpaceCapacity": 1024,
  "Description": "This is the first Apsara File Storage for HDFS instance of my company.",
  "ProtocolType": "HDFS",
  "UsedSpaceSize": 100.0,
  "RegionId": "cn-hangzhou",
  "FileSystemId": "037cb4****",
  "ZoneId": "cn-hangzhou-b",
  "StorageType": "STANDARD",
  "FileSystemName": "MyFirstDFS",
  "CreateTime": "2018-01-18 12:50:00",
  "MountPointCount": 2
 }
}
```


2.7.1.4.5. ListFileSystems

You can call this operation to query the detailed information about multiple file system instances.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
StartOffset	Integer	FALSE	The start position. Default value: 1.
Limit	Integer	FALSE	The maximum number of entries to return. Default value: 10.
OrderBy	String	FALSE	The sorting field. Valid values: CreateTime, FileSystemName, SpaceCapacity, and UsedSpaceSize. Default value: CreateTime.
OrderType	String	FALSE	The ordering mode. ASC indicates ascending order and DESC indicates descending order. Default value: ASC.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Parameter	Type	Description
TotalCount	Integer	The number of entries returned. Maximum value: the value of the Limit parameter.
FileSystems	Array(Filesystem)	The list of detailed information about file systems.
FileSystem.RegionId	String	The ID of the region.
FileSystem.ZoneId	String	The ID of the zone.
FileSystem.FileSystemName	String	The name of the file system instance.
FileSystem.Description	String	The description of the file system instance.
FileSystem.ProtocolType	String	The interface protocol type.
FileSystem.StorageType	String	The type of the storage medium.
FileSystem.SpaceCapacity	Long	The estimated capacity of the file system instance. Unit: GB.
FileSystem.MountPointCount	Long	The number of mount points.
FileSystem.FileSystemId	String	The ID of the file system instance.
FileSystem.CreateTime	String	The time at which the file system instance was created.
FileSystem.UsedSpaceSize	Float	The space in use. Unit: GB.

Examples

Sample requests

```
GET https://dfs.cn-hangzhou.aliyuncs.com/?Action=ListFileSystems
&InputRegionId=cn-hangzhou
&StartOffset=10
&Limit=10
&OrderBy=CreateTime
&OrderType=ASC
&<Common request parameters>
```

Sample responses

- JSON format

```
{
 "TotalCount": 1,
 "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8",
 "FileSystems": [
  {
   "SpaceCapacity": 1024,
   "Description": "This is the first Apsara File Storage for HDFS instance of my company.",
   "ProtocolType": "HDFS",
   "UsedSpaceSize": 100.0,
   "RegionId": "cn-hangzhou",
   "FileSystemId": "037cb4****",
   "ZoneId": "cn-hangzhou-b",
   "StorageType": "STANDARD",
   "FileSystemName": "MyFirstDFS",
   "CreateTime": "2018-01-18 12:50:00",
   "MountPointCount": 2
  }
 ]
}
```


2.7.1.5. Permissions

2.7.1.5.1. CreateAccessGroup

You can call this operation to create a permission group.

Note Each permission group can contain multiple permission rules. A permission group is a list of IP addresses that are allowed to access the file system. When mounting a file system instance, you must specify a permission group to define the IP address range allowed to access the file system instance.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
AccessGroupName	String	TRUE	The name of the permission group. Maximum length: 100 bytes.

Parameter	Type	Required	Description
NetworkType	String	TRUE	The type of the permission group. Set this parameter to VPC.
Description	String	FALSE	The description of the permission group. Maximum length: 100 bytes.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
AccessGroupId	String	The ID of the permission group.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=CreateAccessGroup
&InputRegionId=cn-hangzhou
&AccessGroupName=my-online-cluster-policy
&NetworkType=VPC
&Description=Special policy for online cluster segments
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8",
  "AccessGroupId": "c5ffd6-bf99****"
}
```

2.7.1.5.2. DeleteAccessGroup

You can call this operation to delete an existing permission group.

Note A permission group can be deleted only when it is not associated with any mount points. All rules in the permission group are deleted along with the permission group.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
AccessGroupId	String	TRUE	The ID of the permission group.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=DeleteAccessGroup
&InputRegionId=cn-hangzhou
&AccessGroupId=c5ffd6-bf99****
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.5.3. ModifyAccessGroup

You can call this operation to modify the attributes of a permission group.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
AccessGroupId	String	TRUE	The ID of the permission group.
AccessGroupName	String	FALSE	The new permission group name. Maximum length: 100 bytes.

Parameter	Type	Required	Description
Description	String	FALSE	The new permission group description. Maximum length: 100 bytes.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=ModifyAccessGroup
&InputRegionId=cn-hangzhou
&AccessGroupId=c5ffd6-bf99****
&AccessGroupName=my-online-cluster-policy
&Description=Special policy for online cluster segments
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.5.4. GetAccessGroup

You can call this operation to query information about a permission group.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
AccessGroupId	String	TRUE	The ID of the permission group.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
AccessGroup	Struct	The detailed information about the permission group.
AccessGroup.RegionId	String	The ID of the zone.
AccessGroup.AccessGroupName	String	The name of the permission group.
AccessGroup.NetworkType	String	The type of the permission group.
AccessGroup.Description	String	The description of the permission group.
AccessGroup.AccessGroupId	String	The ID of the permission group.
AccessGroup.CreateTime	String	The time the permission group was created.
AccessGroup.RuleCount	Integer	The number of rules in the permission group.
AccessGroup.MountPointCount	Integer	The number of mount entries associated with the permission group.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=GetAccessGroup
&InputRegionId=cn-hangzhou
&AccessGroupId=c5ffd6-bf99****
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "AccessGroup": {
    "Description": "Special permission group for the test cluster",
    "RegionId": "cn-shanghai",
    "AccessGroupName": "test-cluster-policy",
    "RuleCount": 3,
    "NetworkType": "VPC",
    "CreateTime": "2018-01-05 12:30:15",
    "AccessGroupId": "c5ffd6-bf99****",
    "MountPointCount": 1
  },
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```


2.7.1.5.5. ListAccessGroups

You can call this operation to query the detailed information about multiple permission groups.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
StartOffset	Integer	FALSE	The position from which to start listing permission groups. Default value: 1.
Limit	Integer	FALSE	The maximum number of entries to return. Default value: 10.
OrderBy	String	FALSE	The field by which to sort permission groups. Valid values: AccessGroupName and CreateTime. Default value: CreateTime.
OrderType	String	FALSE	The ordering mode. Valid values: ASC and DESC. Default value: ASC.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of entries returned. Maximum value: the value of the Limit parameter.

Parameter	Type	Description
AccessGroups	Array(AccessGroup)	The list of detailed information about permission groups.
AccessGroup.RegionId	String	The ID of the zone.
AccessGroup.AccessGroupName	String	The name of the permission group.
AccessGroup.NetworkType	String	The type of the permission group.
AccessGroup.Description	String	The description of the permission group.
AccessGroup.AccessGroupId	String	The ID of the permission group.
AccessGroup.CreateTime	String	The time the permission group was created.
AccessGroup.RuleCount	Integer	The number of rules in the permission group.
AccessGroup.MountPointCount	Integer	The number of mount entries associated with the permission group.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=ListAccessGroups
&InputRegionId=cn-hangzhou
&StartOffset=10
&Limit=10
&OrderBy=CreateTime
&OrderType=ASC
&<Common request parameters>
```

Sample responses

- JSON format

```
{
 "TotalCount": 1,
 "AccessGroups": [
  {
   "Description": "Special permission group for the test cluster",
   "RegionId": "cn-shanghai",
   "AccessGroupName": "test-cluster-policy",
   "RuleCount": 3,
   "NetworkType": "VPC",
   "CreateTime": "2018-01-05 12:30:15",
   "AccessGroupId": "c5ffd6-bf99****",
   "MountPointCount": 1
  }
 ],
 "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```


2.7.1.5.6. CreateAccessRule

You can call this operation to create a permission rule.

Note Priority indicates the matching sequence of the rules in a permission group. The smaller the Priority value, the higher the priority is.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
AccessGroupId	String	TRUE	The ID of the permission group.
NetworkSegment	String	TRUE	The IP address or address range. For example, 192.168.1.220 indicates an IP address, and 10.10.3.0/24 indicates an IP address range from 10.10.3.0 to 10.10.3.255.

Parameter	Type	Required	Description
RWAccessType	String	TRUE	The access type. RDWR indicates read/write permissions, and RDONLY indicates read-only. Set this parameter to RDWR.
Priority	Integer	TRUE	The priority of the rule. The smaller the value, the higher the priority is. The rules are matched in the ascending order of the Priority value until a match is found. Valid values: 0 to 100.
Description	String	FALSE	The description of the rule. Maximum value: 100 bytes.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
AccessRuleId	String	The ID of the rule.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=CreateAccessRule
&InputRegionId=cn-hangzhou
&AccessGroupId=c5ffd6-bf9941bd
&NetworkSegment=10.10.3.0/24
&RWAccessType=RDWR
&Priority=2
"Description": "network segment of the server to which logs are uploaded",
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8",
  "AccessRuleId": "a0ws0****"
}
```

2.7.1.5.7. DeleteAccessRule

You can call this operation to delete a permission rule.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
AccessGroupId	String	TRUE	The ID of the permission group.
AccessRuleId	String	TRUE	The ID of the rule.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=DeleteAccessRule
&InputRegionId=cn-hangzhou
&AccessGroupId=c5ffd6-bf99****
&AccessRuleId=a0ws0****
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.5.8. ModifyAccessRule

You can call this operation to modify attributes about a rule.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
AccessGroupId	String	TRUE	The ID of the permission group.
AccessRuleId	String	TRUE	The ID of the rule.
RWAccessType	String	FALSE	The access type. RDWR indicates read/write permissions, and RDONLY indicates read-only. Set this parameter to RDWR.
Priority	Integer	FALSE	The priority of the rule. The smaller the value, the higher the priority is. The rules are matched in the ascending order of the Priority value until a match is found. Valid values: 0 to 100.
Description	String	FALSE	The description of the rule. Maximum value: 100 bytes.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=ModifyAccessRule
&InputRegionId=cn-hangzhou
&AccessGroupId=c5ffd6-bf99****
&AccessRuleId=a0ws0****
&RWAccessType=RDWR
&Priority=2
"Description": "network segment of the server to which logs are uploaded",
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.5.9. GetAccessRule

You can query this operation to query detailed information about a rule.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
AccessGroupId	String	TRUE	The ID of the permission group.
AccessRuleId	String	TRUE	The ID of the rule.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
AccessRule	Struct	The detailed information about the rule.
AccessRule.AccessRuleId	String	The ID of the rule.
AccessRule.AccessGroupId	String	The ID of the permission group.
AccessRule.RegionId	String	The ID of the zone.
AccessRule.NetworkSegment	String	The IP address or address range. For example, 192.168.1.220 indicates an IP address, and 10.10.3.0/24 indicates an IP address range from 10.10.3.0 to 10.10.3.255.
AccessRule.Description	String	The description of the rule.
AccessRule.Priority	Integer	The priority of the rule. The smaller the value, the higher the priority is. The rules are matched in the ascending order of the Priority value until a match is found.

Parameter	Type	Description
AccessRule.RWAccessType	String	The access type. RDWR indicates read/write permissions, and RDONLY indicates read-only. Set this parameter to RDWR.
AccessRule.CreateTime	String	The time the rule was created.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=GetAccessRule
&InputRegionId=cn-hangzhou
&AccessGroupId=c5ffd6-bf99****
&AccessRuleId=a0ws0****
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8",
  "AccessRule": {
    "NetworkSegment": "10.10.3.0/24",
    "Description": "Network segment of the server to which logs are uploaded",
    "RWAccessType": "RDWR",
    "RegionId": "cn-shanghai",
    "AccessRuleId": "a0ws0****",
    "Priority": 2,
    "CreateTime": "2018-01-05 12:30:15",
    "AccessGroupId": "c5ffd6-bf99****"
  }
}
```

2.7.1.5.10. ListAccessRules

You can call this operation to query the detailed information about multiple rules.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
AccessGroupId	String	TRUE	The ID of the permission group.
StartOffset	Integer	FALSE	The position from which to start listing access rules. Default value: 1.
Limit	Integer	FALSE	The maximum number of entries to return. Default value: 10.
OrderBy	String	FALSE	The field by which to sort access rules. Valid values: Priority and CreateTime. Default value: Priority.
OrderType	String	FALSE	The ordering mode. Valid values: ASC and DESC. Default value: ASC.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of entries returned. Maximum value: the value of the Limit parameter.
AccessRules	Array(AccessRule)	The list of detailed information about rules.
AccessRule.AccessRuleId	String	The ID of the rule.
AccessRule.AccessGroupId	String	The ID of the permission group.
AccessRule.RegionId	String	The ID of the zone.
AccessRule.NetworkSegment	String	The IP address or address range. For example, 192.168.1.220 indicates an IP address, and 10.10.3.0/24 indicates an IP address range from 10.10.3.0 to 10.10.3.255.
AccessRule.Description	String	The description of the rule.

Parameter	Type	Description
AccessRule.Priority	Integer	The priority of the rule. The smaller the value, the higher the priority is. The rules are matched in the ascending order of the Priority value until a match is found.
AccessRule.RWAccessType	String	The access type. RDWR indicates read/write permissions, and RDONLY indicates read-only. Set this parameter to RDWR.
AccessRule.CreateTime	String	The time the rule was created.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=ListAccessRules
&InputRegionId=cn-hangzhou
&AccessGroupId=c5ffd6-bf99****
&StartOffset=10
&Limit=10
&OrderBy=CreateTime
&OrderType=ASC
&<Common request parameters>
```

Sample responses

- JSON format

```
{
 "TotalCount": 1,
 "AccessRules": [
  {
   "NetworkSegment": "10.10.3.0/24",
   "Description": "Network segment of the server to which logs are uploaded",
   "RWAccessType": "RDWR",
   "RegionId": "cn-shanghai",
   "AccessRuleId": "a0ws0****",
   "Priority": 2,
   "CreateTime": "2018-01-05 12:30:15",
   "AccessGroupId": "c5ffd6-bf99****"
  }
 ],
 "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```


2.7.1.6. Mount points

2.7.1.6.1. CreateMountPoint

You can call this operation to create a mount point. You can attach a file system instance to a VPC and allow the IP addresses defined in the specified permission rules to access the file system instance.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
FileSystemId	String	TRUE	The ID of the specified file system instance.
AccessGroupId	String	TRUE	The ID of the permission group.
NetworkType	String	TRUE	The network type of the mount point. Set this parameter to VPC.
VpcId	String	TRUE	The ID of the VPC.
VSwitchId	String	TRUE	The ID of the VSwitch.

Parameter	Type	Required	Description
Description	String	FALSE	The description of the mount point. Maximum length: 100 bytes.

Response parameters

Parameter	Type	Description
MountPointId	String	The ID of the mount point.
RequestId	String	The ID of the request.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=CreateMountPoint
&InputRegionId=cn-hangzhou
&FileSystemId=037cb4****
&AccessGroupId=c5ffd6-bf99****
&NetworkType=VPC
&VpcId=vpc-bp1lfyerqlollad1e****
&VSwitchId=vsw-bp11990m3zf3hp867****
&Description=Attach the online file system instance to the VSwitch in the VPC log cluster
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "MountPointId": "037cb49e1d-c****",
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.6.2. DeleteMountPoint

You can call this operation to delete a mount point.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.

Parameter	Type	Required	Description
FileSystemId	String	TRUE	The ID of the specified file system instance.
MountPointId	String	TRUE	The ID of the mount point.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=DeleteMountPoint
&InputRegionId=cn-hangzhou
&FileSystemId=037cb4****
&MountPointId=037cb49e1d-c****
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.6.3. ModifyMountPoint

You can call this operation to enable or disable a mount point, or modify the description of a mount point.

Description

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
FileSystemId	String	TRUE	The ID of the specified file system instance.

Parameter	Type	Required	Description
MountPointId	String	TRUE	The ID of the mount point.
AccessGroupId	String	FALSE	The ID of the permission group.
Description	String	FALSE	The description of the mount point. Maximum length: 100 bytes.
Status	String	FALSE	The status of the mount point. Inactive indicates that the mount point is disabled. Active indicates that the mount point is enabled.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=ModifyMountPoint
&InputRegionId=cn-hangzhou
&FileSystemId=037cb4****
&MountPointId=037cb49e1d-c****
&AccessGroupId=c5ffd6-bf99****
&Description=Attach the online file system instance to the VSwitch in the VPC log cluster
&Status=Inactive
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.6.4. GetMountPoint

You can call this operation to query detailed information about a mount point.

Request parameters

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
FileSystemId	String	TRUE	The ID of the specified file system instance.
MountPointId	String	TRUE	The ID of the mount point.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
MountPoint	Struct	The detailed information about a mount point.
MountPoint.RegionId	String	The ID of the zone.
MountPoint.FileSystemId	String	The ID of the specified file system instance.
MountPoint.NetworkType	String	The network type of the mount point. Set this parameter to VPC.
MountPoint.VpcId	String	The ID of the VPC.
MountPoint.VSwitchId	String	The ID of the VSwitch.
MountPoint.AccessGroupId	String	The ID of the permission group.
MountPoint.Description	String	The description of the mount point.
MountPoint.Status	String	The status of the mount point. Inactive indicates that the mount point is disabled. Active indicates that the mount point is enabled.
MountPoint.MountPointId	String	The ID of the mount point.
MountPoint.MountPointDomain	String	The domain name of the mount point. Users within the mounted VPC network segment can use this domain name to access Apsara File Storage for HDFS.

Parameter	Type	Description
MountPoint.CreateTime	String	The time the mount point was created.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=GetMountPoint
&InputRegionId=cn-hangzhou
&FileSystemId=037cb4****
&MountPointId=037cb49e1d-c****
&<Common request parameters>
```

Sample responses

- JSON format

```
{
  "MountPoint": {
    "Status": "Inactive",
    "VpcId": "vpc-bp1lfyerqlollad1ee6k7",
    "Description": "Attach the online file system instance to the VSwitch in the VPC log cluster",
    "RegionId": "cn-shanghai",
    "CreateTime": "2018-01-05 12:30:15",
    "FileSystemId": "037cb4****",
    "VSwitchId": "vsw-bp11990m3zf3hp867****",
    "MountPointDomain": "037cb49e1d-cpu65.cn-hangzhou.dfs.aliyuncs.com",
    "MountPointId": "037cb49e1d-c****",
    "NetworkType": "VPC",
    "AccessGroupId": "c5ffd6-bf99****"
  },
  "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8"
}
```

2.7.1.6.5. ListMountPoints

You can call this operation to query the detailed information about multiple mount points.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
InputRegionId	String	TRUE	The ID of the specified region.
FileSystemId	String	TRUE	The ID of the specified file system instance.
StartOffset	Integer	FALSE	The position from which to start listing mount points. Default value: 1.
Limit	Integer	FALSE	The maximum number of entries to return. Default value: 10.
OrderBy	String	FALSE	The field by which to sort mount points. Set this parameter to CreateTime. Default value: CreateTime.
OrderType	String	FALSE	The ordering mode. Valid values: ASC and DESC. Default value: ASC.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of entries returned. Maximum value: the value of the Limit parameter.
MountPoints	Array(MountPoint)	The list of detailed information about mount points entries.
MountPoint.RegionId	String	The ID of the zone.
MountPoint.FileSystemId	String	The ID of the specified file system instance.
MountPoint.NetworkType	String	The network type of the mount point. Set this parameter to VPC.
MountPoint.VpcId	String	The ID of the VPC.
MountPoint.VSwitchId	String	The ID of the VSwitch.
MountPoint.AccessGroupId	String	The ID of the permission group.

Parameter	Type	Description
MountPoint.Description	String	The description of the mount point.
MountPoint.Status	String	The status of the mount point. Inactive indicates that the mount point is disabled. Active indicates that the mount point is enabled.
MountPoint.MountPointId	String	The ID of the mount point.
MountPoint.MountPointDomain	String	The domain name of the mount point. Users within the mounted VPC network segment can use this domain name to access Apsara File Storage for HDFS.
MountPoint.CreateTime	String	The time the mount point was created.

Examples

Sample requests

```
GET https://dfs.regionid.example.com/?Action=ListMountPoints
&InputRegionId=cn-hangzhou
&FileSystemId=037cb4****
&StartOffset=10
&Limit=10
&OrderBy=CreateTime
&OrderType=ASC
&<Common request parameters>
```

Sample responses

- JSON format

```
{
 "TotalCount": 1,
 "RequestId": "55C5FFD6-BF99-41BD-9C66-FFF39189F4F8",
 "MountPoints": [
  {
   "Status": "Inactive",
   "VpcId": "vpc-bp1lfyerqlollad1e****",
   "Description": "Attach the online file system instance to the VSwitch in the VPC log cluster",
   "RegionId": "cn-shanghai",
   "CreateTime": "2018-01-05 12:30:15",
   "FileSystemId": "037cb4****",
   "VSwitchId": "vsw-bp11990m3zf3hp867****",
   "MountPointDomain": "037cb49e1d-cpu65.cn-hangzhou.dfs.aliyuncs.com",
   "MountPointId": "037cb49e1d-c****",
   "NetworkType": "VPC",
   "AccessGroupId": "c5ffd6-bf99****"
  }
 ]
}
```


2.7.1.7. Appendix: Error codes

An error code consists of three components, as described in Error codes.

Error codes

Component	Description
HTTP status code	The HTTP response code that complies with HTTP syntax.
Code	The error code.
Message	The error message.

Error codes

HTTP status code	Error code	Error message	Description

HTTP status code	Error code	Error message	Description
500	InternalError	An internal error occurred, please try again later.	The error message returned because an unknown internal error has occurred. Try again later.
503	ServiceUnavailable	The service is unavailable, please try again later.	The error message returned because the service is unavailable. Try again later.
401	NoPermission	The user is not authorized to operate on the specified resource, please check the permission of the user.	The error message returned because the user is not authorized to operate this resource. Check the permissions of the user.
501	NotFoundAction	Cannot find this action, please check whether the action is valid.	The error message returned because this operation was not found. Check whether the operation is valid.
400	InvalidRequest	Invalid request, please check request parameters.	The error message returned because the request is invalid. Check whether the request parameters are correct.

HTTP status code	Error code	Error message	Description
400	InvalidUserStatus	Invalid user, please check the user status.	The error message returned because the user status is not valid. Check the user status.
400	InvalidFileSystemName	Invalid filesystem name, please check whether it is unique.	The error message returned because the file system instance name is invalid. Check whether the name is unique.
400	InvalidFileSystemId	Invalid filesystem id, please check it.	The error message returned because the file system instance ID is invalid. Check whether the instance ID is valid.
400	InvalidMountPointId	Invalid mountpoint id, please check it.	The error message returned because the mount point ID is invalid. Check whether the mount point ID is valid.
403	FileSystemCountExceedLimit	The filesystem number has exceed the limit, please check the number of the owned filesystems.	The error message returned because the number of file system instances exceeds the limit. Check the number of file system instances that you own.

HTTP status code	Error code	Error message	Description
403	FileSystemHasMountPoint	The filesystem has mount points, please delete them first.	The error message returned because there are still mount points in the file system instance. Delete the mount points first.
403	MountPointCountExceedLimit	The mount point number has exceeded the limit, please check the number of the owned mount points. mount points.	The error message returned because the number of mount points exceeds the limit. Check the number of mount points that you own.
410	ResourceAlreadyDelete	The resource has already been deleted, please refresh.	The error message returned because the resource has been deleted. Refresh the page.
400	InvalidSpaceCapacity	The value of SpaceCapacity is invalid, please check the input.	The error message returned because the SpaceCapacity value is invalid. Check whether the specified value is valid.
403	ResourceNotEnough	The storage resource is not enough, please contact the system administrator.	The error message returned because there are insufficient storage resources. Contact the system administrator.

HTTP status code	Error code	Error message	Description
403	ActionNotComplete	The preceding action is still running, please wait a moment.	The error message returned because the previous operation is still in progress. Wait until it is complete and try again.
403	RegionNotSupport	The specified region is not support.	The error message returned because the specified region does not support the operation.
400	MissingParameter	The parameter %s is required.	The error message returned because the %s parameter is not specified. Specify this parameter.
403	ResourceLimitExceed	The %s resource has exceeded the limit.	The error message returned because the %s resource has exceeded its limit.
403	DependencyFound	The %s resource is being depended, please remove it first.	The error message returned because the %s resource is in use. Remove it first.
400	InvalidParameter	Invalid parameter, name: %s value: %s	The error message returned because the %s parameter and %s value are invalid.

HTTP status code	Error code	Error message	Description
404	ResourceNotExist	Resource %s does not exist, id: %s	The error message returned because the %s resource with %s as its ID does not exist.
409	ResourceNameConflict	The name of resource %s conflicts with others.	The error message returned because the %s resource name conflicts with another resource name.
409	ResourceAlreadyCreate	Resource %s has already been created, id: %s	The error message returned because the resource of the %s type with %s as its ID has already been created.

2.7.2. SDK reference

2.7.2.1. Overview

Apsara File Storage for HDFS SDKs consist of the file system SDK and the management Java SDK.

- The file system SDK provides a Hadoop-compatible file system through the implementation of Hadoop FileSystem interfaces. It is a JAR file named *alicloud.dfs-1.0.0.jar*.

  With this SDK, Apache Hadoop computing and analysis applications such as MapReduce, Hive, and Spark can use Apsara File Storage for HDFS as the default file system for better features and performance over the original HDFS.
- You can use the management Java SDK to call the management APIs of Apsara File Storage for HDFS to implement the corresponding functions available in the Apsara Stack console. The management Java SDK is a JAR file named *aliyun-java-sdk-dfs-1.0.jar*.

2.7.2.2. File system SDK

This topic uses hadoop-mapreduce-examples to describe how to use the file system SDK. MapReduce runs in the pseudo-distributed mode. For more information about the pseudo-distributed mode of MapReduce, see Pseudo-Distributed Operation.

2.1 Check the environment

1. Run the `java -version` command to view the JDK version.

   If the JDK version is earlier than 1.8, install the latest JDK.

2. After the JDK is installed, set the environment variables as follows: (Assume that the installation path is */opt/install/java*.)

   ```
   JAVA_HOME=/opt/install/java
   ```

   ```
   PATH=/opt/install/java/bin:$PATH
   ```

2.2 Download the file system SDK

You can click here to download the JAR package of the file system SDK: *alicloud.dfs-1.0.0.jar*.

2.3 Configure Hadoop

1. Download the Hadoop 2.7.2 release package.
2. Run the `tar -zxvf hadoop-2.7.2.tar.gz` command to decompress the downloaded package.
3. Run the `export HADOOP_HOME=yourWorkingDir/hadoop-2.7.2` command to set the environment variables.
4. Run the `cd hadoop-2.7.2` command to access the hadoop directory.
5. Modify the *etc/hadoop/hadoop-env.sh* file. Add JAVA_HOME set in Section "2.1 Check the environment."

   ```
   # set to the root of your Java installation
   export JAVA_HOME=youJAVADirt
   ```

6. Modify the *etc/hadoop/core-site.xml* file and synchronize the *core-site.xml* file to all nodes that are dependent on hadoop-common. The following code shows the content to be modified in the *core-site.xml* file:

```
<property>
      <name>fs.defaultFS</name>
      <value>dfs://DfsInstanceID.RegionID.alidfs.aliyun.com:10290</value>
    </property>
    <property>
      <name>fs.dfs.impl</name>
      <value>com.alibaba.dfs.DistributedFileSystem</value>
   </property>
    <property>
      <name>fs.AbstractFileSystem.dfs.impl</name>
      <value>com.alibaba.dfs.DFS</value>
    </property>
    <property>
      <name>alidfs.usergroupservice.impl</name>
      <value>com.alibaba.dfs.security.LinuxUserGroupService.class</value>
</property>
```

Note

- Replace RegionID and DfsInstanceID with the actual region ID and Apsara File Storage for HDFS instance ID.
- You must synchronize the content from *core-site.xml* to all nodes dependent on hadoop-common.

2.4 Deploy dependencies

Copy the *alicloud.dfs-1.0.0.jar* package obtained in the preceding step to *CLASSPATH* of the Hadoop ecosystem component. We recommend that you deploy the package to the directory where *hadoop-common-X.YZ.jar* resides and copy this package to all Hadoop nodes. The directory of the MapReduce component is *$HADOOP_HOME/share/hadoop/hdfs*.

2.5 Verify installation

2.5.1 Prepare data

1. Run the following command to create a directory:

   ```
   $HADOOP_HOME/bin/hadoop fs -mkdir inputDir
   ```

2. Run the following command to upload the a.txt file to the directory:

   ```
   touch a.txt
   $HADOOP_HOME/bin/hadoop fs -put a.txt inputDir/
   ```

2.5.2 Run sample code

Run the following sample code in *$HADOOP_HOME*:

- wordcount:

  ```
  bin/hadoop jar ./share/hadoop/mapreduce/hadoop-mapreduce-examples-2.7.2.jar wordcount inputDir outputDir
  ```

- grep:

  ```
  bin/hadoop jar ./share/hadoop/mapreduce/hadoop-mapreduce-examples-2.7.2.jar grep inputDir/ outputDirGrep/ "the"
  ```

2.7.2.3. Management Java SDK

2.7.2.3.1. Java SDK

2.7.3. Obtain an AccessKey pair

You can obtain the AccessKey pair on the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

   > **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**.

   The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

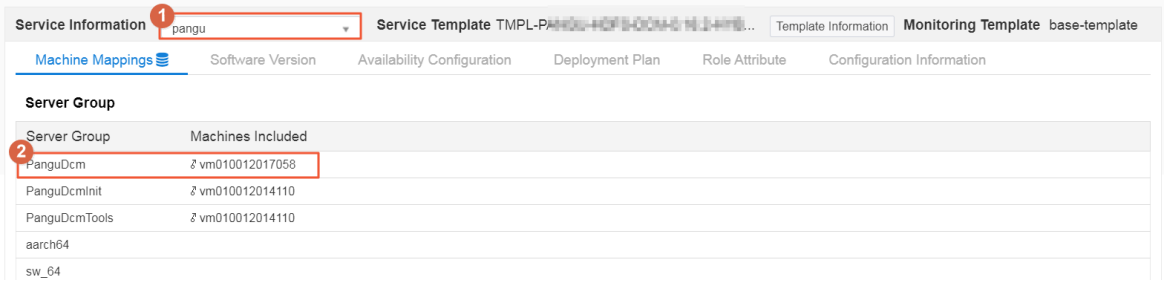
2.7.4. Obtain an endpoint

You can obtain the endpoint of a service in the Apsara Stack Operations console.

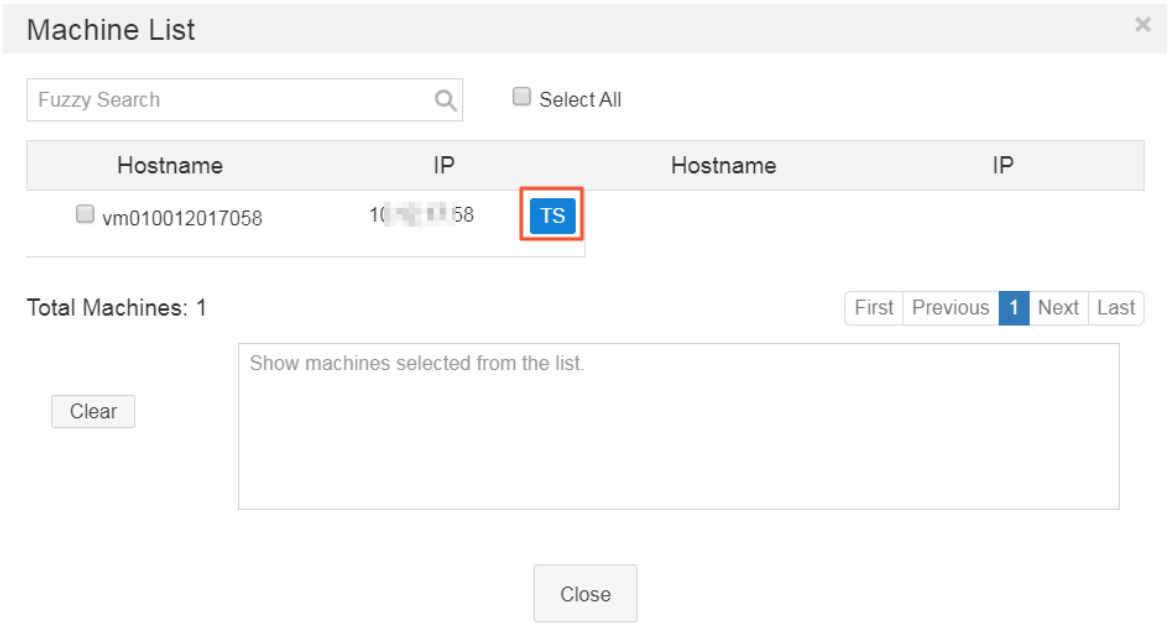
Procedure

1. Log on to the Apsara Stack Operations console. For more information about how to log on to Apsara Stack Operations, see **Operations of basic platforms** > **Apsara Stack Operations** > **Log on to Apsara Stack Operations** in *Operations Guide* .
2. In the left-side navigation pane, click **Products**.

3. Click **Apsara Infrastructure Management Framework** to go to the Apsara Infrastructure Management Framework console.
4. In the top navigation bar, choose **Operations** > **Cluster Operations**.
5. On the **Cluster Operations** page that appears, enter *PanguDcmCluster* in **Cluster**.
6. Click **Cluster Configuration** in the Actions column corresponding to the cluster.
7. On the **Cluster Configuration** page that appears, perform the following operations:



   - Select **pangu** from the **Service Information** drop-down list.
   - In **Server Group**, click the hostname corresponding to PanguDcm.
8. In the **Machine List** dialog box that appears, click **TS**.



9. On the **TerminalService** page that appears, run the following command:

```
grep -r internet-domain /apsara/pangu_dcm/conf.global/kv.json
```

10. Take the endpoint `"internet-domain": "example.site.com",` displayed in step 9 as an example. You can use the format `alidfs.${internet-domain}` to obtain `alidfs.example.site.com` .

2.8. ApsaraDB for RDS

2.8.1. API reference

2.8.1.1. List of operations by function

The following tables list API operations available for use in RDS.

RDS instance management

Operation	Description
CreateDBInstance	Creates an RDS instance.
DeleteDBInstance	Releases an RDS instance.
RestartDBInstance	Restarts an RDS instance.
DescribeDBInstanceAttribute	Queries the details of an RDS instance.
DescribeDBInstances	Queries the instance list.
ModifyDBInstanceSpec	Modifies the RDS instance type.
AllocateInstancePublicConnection	Applies for a public endpoint.
ReleaseInstancePublicConnection	Releases a public endpoint.
SwitchDBInstanceNetType	Applies for an internal endpoint.
DescribeDBInstanceNetInfo	Queries all endpoints.
ModifyDBInstanceConnectionString	Modifies an endpoint.
ModifyDBInstanceConnectionMode	Changes the RDS instance access mode.
ModifyDBInstanceNetworkType	Changes the RDS instance network type.
DescribeDBInstanceIPArrayList	Queries the IP whitelist of an RDS instance.
ModifySecurityIps	Modifies the IP whitelist of an RDS instance.
DescribeRegions	Queries the RDS region and zone information.
DescribeDBInstanceHAConfig	Queries the RDS zone information and data replication status.
MigrateToOtherZone	Migrates an RDS instance from one zone to another.
PurgeDBInstanceLog	Clears the logs of an RDS instance.
UpgradeDBInstanceEngineVersion	Upgrades the RDS instance version.
ModifyDBInstanceDescription	Modifies the description of an RDS instance.
ModifyDBInstanceMaintainTime	Modifies the maintenance window of an RDS instance.

Operation	Description
ModifyDBInstanceHAConfig	Modifies the data replication and high availability polices of an RDS instance.
SwitchDBInstanceHA	Switches between the primary and secondary RDS instances.
CreateReadonlyDBInstance	Creates a read-only RDS instance.
DescribeDBInstanceSSL	Queries the SSL link of an RDS instance.
ModifyDBInstanceSSL	Modifies the SSL link of an RDS instance.
DescribeDBInstanceTDE	Queries the TDE status of an RDS instance.
ModifyDBInstanceTDE	Modifies the TDE status of an RDS instance.

RDS database management

Operation	Description
CreateDatabase	Creates a database.
DeleteDatabase	Deletes a database.
DescribeDatabases	Queries the database list.
ModifyDBDescription	Modifies the description of a database.

RDS account management

Operation	Description
CreateAccount	Creates an account.
DeleteAccount	Deletes an account.
DescribeAccounts	Queries the account list.
GrantAccountPrivilege	Grants permissions to an account.
RevokeAccountPrivilege	Revokes permissions from an account.
ModifyAccountDescription	Modifies the description of an account.
ResetAccountPassword	Resets the password of an account.
ResetAccount	Resets an account.

RDS backup and restoration

Operation	Description
CreateBackup	Creates a backup.
CloneDBInstance	Clones an RDS instance.
DescribeBackups	Queries the backup instance list.
CreateTempDBInstance	Creates a temporary instance.
DescribeBackupPolicy	Queries a backup policy.
ModifyBackupPolicy	Modifies a backup policy.
RestoreDBInstance	Restores a backup set to an instance.
DeleteBackup	Deletes data backup files.

RDS monitoring management

Operation	Description
DescribeResourceUsage	Queries the resource usage of an instance.
DescribeDBInstancePerformance	Queries the performance data of an instance.
DescribeDBInstanceMonitor	Queries the monitoring behaviors of an instance.
ModifyDBInstanceMonitor	Modifies the monitoring behaviors of an instance.

RDS parameter management

Operation	Description
DescribeParameterTemplates	Queries a database parameter template.
DescribeParameters	Queries the running database parameter list of the current instance.
ModifyParameter	Modifies the database parameter list.

RDS log management

Operation	Description
DescribeSlowLogs	Queries the slow log list.
DescribeSlowLogRecords	Queries slow log details.
DescribeErrorLogs	Queries error logs.
DescribeBinlogFiles	Queries binlogs.

Operation	Description
DescribeSQLCollectorPolicy	Queries the SQL collection status.
ModifySQLCollectorPolicy	Changes the SQL collection status.
DescribeSQLLogRecords	Queries the SQL audit logs of an RDS instance.
DescribeSQLLogFiles	Queries the SQL audit file list.

RDS data migration

Operation	Description
ImportDatabaseBetweenInstances	Migrates data from other instances.
CancelImport	Cancels an import task.

RDS tag management

Operation	Description
AddTagsToResource	Binds a tag.
DescribeTags	Queries tags.
RemoveTagsFromResource	Unbinds a tag.

2.8.1.2. Make API requests

2.8.1.2.1. Request structure

This topic describes the request structure of RDS APIs.

Endpoints

The endpoint of the RDS API is rds.example.com. For more information about how to obtain a service endpoint, see Obtain an endpoint.

Protocols

You can send requests over HTTP or HTTPS. We recommend that you send requests over HTTPS to enhance security.

Methods

The HTTP GET method can be used to send requests. Request parameters must be included in the request URL.

Request parameters

Each request must specify the action to be performed in the Action parameter. Each operation request must include common request parameters and the specific request parameters of the operation called.

Encoding

Requests and responses are encoded in UTF-8.

2.8.1.2.2. Common parameters

2.8.1.2.2.1. Common request parameters

Common request parameters must be included in the request of each API.

Parameter	Type	Required	Description
Format	String	No	The format of the response. Valid values: JSON and XML. Default value: XML.
Version	String	Yes	The API version. It is in the YYYY-MM-DD format. The current version is 2014-08-15.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature result string. For more information about the signature calculation method, see Request signatures.
SignatureMethod	String	Yes	The algorithm used to create the request signature. Valid value: HMAC-SHA1.
Timestamp	String	Yes	The request timestamp. The timestamp follows the ISO 8601 standard and uses UTC. It is in the YYYY-MM-DDThh:mm:ssZ format. For example, 20:00:00, August 15, 2013, UTC+8 will be written as 2013-08-15T12:00:00Z.
SignatureVersion	String	Yes	The signature algorithm version. The current version is 1.0.
SignatureNonce	String	Yes	A unique, randomly generated number used to prevent network replay attacks. You must use a different random number for each request.

Example

```
https://rds.example.com/
? Format=xml
&Version=2014-08-15
&Signature=Pc5WB8gokVnxxxxx
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&OwnerId=12345678
&Timestamp=2014-10-10T12:00:00Z
```

2.8.1.2.2.2. Common response parameters

The system returns a unique RequestId for each API request, regardless of whether the API operation is successful.

Example

```
<? xml version="1.0" encoding="utf-8"? >
<!—Result root node-->
<API name + response>
   <!—Returned request tag-->
   <RequestId>4C4***38-****-****-****-*******6F216</RequestId>
   <!—Response data-->
</API name + response>
```

2.8.1.2.3. Responses

2.8.1.2.3.1. Success responses

The response data for API requests is displayed in a uniform format. In the response data, a 2xx HTTP status code indicates that the API operation is called.

The response data for called API operations is returned in either the XML or JSON format. You can add parameters to an API request to specify the format of the response data. Response data uses the XML format by default.

Sample responses in this topic are formatted with line breaks or indents for a clear view. The actual responses are not formatted in the same manner as these examples.

- Responses in the XML format include information about whether the call is successful, and details specific to the operation. Example:

```
<!—Result root node-->
<API name + response>
<!—Response request tag-->
<RequestId>4C467B38-****-447D-****-AC04*******16</RequestId>
<!—Response data-->
</API name + response>
```

- JSON format

```
{ "RequestId": "4C467B38-****-447D-****-AC04*******16", /* Response Data */}
```

2.8.1.2.3.2. Error responses

When an error occurs during an API call, no result data is returned. You can locate the cause of the error by referencing Error codes in Appendix.

When an error occurs on an HTTP request for an API operation, a 4xx or 5xx HTTP status code is returned.

The response body includes the error code and error message.

RequestId uniquely identifies the request and HostId indicates the ID of the site requested to be accessed. You can contact Alibaba Cloud customer service when the cause of the error cannot be found. We recommend that you provide HostId and RequestId to help us resolve the issue at the earliest opportunity.

XML format

```
<Error>
<RequestId>8906582E-****-****-A6C4-0E78*******5</RequestId>
<HostId>rds.example.com</HostId>
<Code>UnsupportedOperation</Code>
<Message>The specified action is not supported. </Message>
</Error>
```

JSON format

```
{ "RequestId": "7463B73D-****-4D19-****-6B8*******2EF",
"HostId": "rds.example.com",
"Code": "UnsupportedOperation",
"Message": "The specified action is not supported."
}
```

2.8.1.2.4. Request signatures

ApsaraDB for RDS authenticates each access request. Therefore, a request must contain signature information whether submitted using HTTP or HTTPS. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

RDS performs symmetric encryption using the AccessKey ID and AccessKey Secret to verify the identity of a request sender.

The AccessKey pair is issued by Alibaba Cloud and can be applied for and managed through the official Alibaba Cloud website.

- The AccessKey ID indicates the identity of the visitor.
- The AccessKey Secret is used to encrypt signature strings and verify signature strings on the server. You must keep your AccessKey Secret confidential.

Perform the following steps to sign an access request:

1. Use request parameters to construct a canonicalized query string.
   i. Sort all of the request parameters in alphabetic order.

      The request parameters include common request parameters and customized parameters for the API request, but exclude the Signature parameter in common request parameters.

      > Note When you use the GET method to submit a request, the request parameters are included as a part of the URI. The request parameters in the URI are placed after a question mark (?) and separated by ampersands (&).

   ii. Encode each parameter name and value.

      Parameter names and values are encoded into a URL based on the UTF-8 character set.

      The URL encoding rules are described as follows:

      - Uppercase and lowercase letters, numbers, hyphens (-), underscores (_), periods (.), and tildes (~) are not required to be encoded.
      - Other characters are encoded as %XY, where XY is the hexadecimal representation of the character in ASCII.

        For example, double quotation marks (") are encoded as %22.
      - Extended UTF-8 characters are encoded in the %XY%ZA... format.
      - A space is encoded as %20, rather than the plus sign (+).

        > Note Most libraries that support URL encoding, such as java.net.URLEncoder, comply with the encoding rules for the "application/x-www-form-urlencoded" MIME type.

        If this encoding method is used, replace the plus signs (+) in the encoded strings with %20, the asterisks (*) with %2A, and %7E with a tilde (~) to conform to the encoding rules.

   iii. Connect the encoded parameter names and values with equal signs (=).

   iv. Sort the equal sign-connected strings by their parameter names alphabetically and connect them with ampersands (&).

2. Use the created canonicalized query string to construct a string for signature calculation based on the following rule:

```
StringToSign=
HTTPMethod + “&” +
percentEncode( “/” ) + ” &” +
percentEncode(CanonicalizedQueryString)
```

- HTTPMethod: specifies to use the HTTP method to submit requests, such as GET.
- percentEncode("/"): specifies the encoded value for the forward slash (/) based on the URL encoding rules described in the preceding step, which is %2F.
- percentEncode(CanonicalizedQueryString): specifies the encoded canonicalized query string constructed in step 1, produced by following the URL encoding rules described in 1.b.

3. Use the previous signature string to calculate the HMAC value of the signature as defined in RFC 2104.

   Note The key used for signature calculation is your AccessKey Secret. An ampersand (&) is added to the end of the key (ASCII: 38). The SHA-1 hashing is used.

4. Encode the HMAC value into a string based on the Base64 encoding rules. This encoded string is the signature value.
5. Add the signature value as the Signature parameter value to the request parameters to complete the request signing process.

   Note The obtained signature value must use RFC 3986 URL encoding like other parameters before it can be submitted to the RDS server as the final request parameter value.

   DescribeCdnService is used here as an example. The request URL before signing is:

   ```
   http://rds.example.com/?TimeStamp=2013-06-01T10:33:56Z&Format=XML&AccessKeyId=testid&Action=DescribeDBInstances&SignatureMethod=HMAC-SHA1&RegionId=region1&SignatureNonce=NwDAxvLU6tFE0DVb&Version=2014-08-15&SignatureVersion=1.0
   ```

   After signing, the StringToSign is as follows:

   ```
   GET&%2F&AccessKeyId%3Dtestid%26Action%3DDescribeDBInstances%26Format%3DXML%26RegionId%3Dregion1%26SignatureMethod%3DHMAC-SHA1%26SignatureNonce%3DNwDAxvLU6tFE0DVb%26SignatureVersion%3D1.0%26TimeStamp%3D2013-06-01T10%253A33%253A56Z%26Version%3D2014-08-15
   ```

   Assume that the AccessKey ID is testid, the AccessKey Secret is testsecret, and the key used for HMAC calculation is testsecret&. The calculated signature value is as follows:

   ```
   BIPOMlu8LXBeZtLQkJTw6iFvw1E=
   ```

   In this example, the request URL after signing is as follows.

   The Signature parameter has been added to the URL.

```
http://rds.example.com/?TimeStamp=2013-06-01T10%3A33%3A56Z&Format=XML&AccessKeyId=testid&Action=DescribeDBInstances&SignatureMethod=HMAC-SH
```

2.8.1.3. Instance management

2.8.1.3.1. CreateDBInstance

Description

You can call this operation to create an RDS instance. For more information about the instance type, see Instance types in Appendix.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateDBInstance.
RegionId	String	Yes	The region ID of the instance. The region ID can be up to 50 characters in length. You can call the DescribeRegions operation to query available regions.
ZoneId	String	No	The zone ID of the instance. You can call the DescribeRegions operation to query available zones.
Engine	String	Yes	The type of the database. Valid values: MySQL, PostgreSQL, and PPAS.
EngineVersion	String	Yes	The version of the database engine. Valid values: MySQL: 5.6 and 5.7 PostgreSQL: 9.4 PPAS: 9.3 and 9.6
DBInstanceClass	String	Yes	The specifications of the instance.
DBInstanceStorage	Integer	Yes	The user-defined storage space. Valid values: MySQL HA edition: 5 to 2000 MySQL 5.7 basic edition: 20 to 1000 PostgreSQL or PPAS HA edition: 5 to 2000 This value must be a multiple of 5 GB. Unit: GB.
DBInstanceNetType	String	Yes	The network connection type of the instance. Valid values: Internet and Intranet.

Parameter	Type	Required	Description
DBInstanceDescription	String	No	The description of the instance. It can be up to 256 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with http:// or https://. It must start with a letter.
SecurityIPList	String	Yes	The IP addresses in an IP address whitelist. Separate multiple IP addresses with commas (,). You can add a maximum of 1,000 different IP addresses to a whitelist. Supported formats of IP addresses are IP addresses such as 0.0.0.0/0 and 10.23.12.24, or Classless Inter-Domain Routing (CIDR) blocks such as 10.23.12.24/24. /24 indicates the length of the IP address prefix. The IP address prefix can consist of 1 to 32 bits.
PayType	String	Yes	The billing method of the instance. Valid values: Postpaid and Prepaid. Postpaid indicates pay-as-you-go and Prepaid indicates subscription.
Period	String	No	The unit of the subscription period. It is required if PayType is set to Prepaid. Valid values: Year and Month.
UsedTime	String	No	The number of the subscription units. It is required if PayType is set to Prepaid. Valid values: positive integers such as 1, 2, and 3.
ClientToken	String	Yes	The client token that is used to ensure the idempotence of the request.
InstanceNetworkType	String	No	The network type of the instance. Valid values: VPC and Classic. Default value: Classic.
ConnectionMode	String	No	The access mode of the instance. Valid values: Performance and Safe. If no value is specified, the system automatically assigns an access mode.
VPCId	String	No	The ID of the VPC.
VSwitchId	String	No	The ID of the VSwitch.
PrivateIpAddress	String	No	The VPC IP address under the specified VSwitch. If no value is specified, the system automatically assigns a VPC IP address.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Parameter	Type	Description
DBInstanceId	String	The ID of the instance newly created.
OrderId	String	The ID of the order.
ConnectionString	String	The endpoint used to connect the database.
Port	String	The port used to connect the database.

Examples

Sample responses

- XML format

```
<CreateDBInstanceResponse>
<OrderId>100789370xxxxx</OrderId>
<ConnectionString>xxxxx.mysql.rds.aliyuncs.com </ConnectionString>
<DBInstanceId>rds-xxxxx</DBInstanceId>
<port>3306</port>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</CreateDBInstanceResponse>
```

- JSON format

```
{ "OrderId": "100789370230206",
"ConnectionString": "rds-xxxxx.mysql.rds.aliyuncs.com",
"DBInstanceId": "rds-xxxxx",
"Port": "3306",
"RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.3.2. DeleteDBInstance

Description

You can call this operation to release an RDS instance. Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The instance is not manually locked.
- The instance is a pay-as-you-go primary instance, read-only instance, disaster recovery instance, or temporary instance.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteDBInstance.
DBInstanceId	String	Yes	The ID of the instance to be released.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=DeleteDBInstance
&DBInstanceId=rds-xxxxx
&<[Common request parameters]>
```

Sample responses

- XML format

```
<DeleteDBInstanceResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</DeleteDBInstanceResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.3.3. RestartDBInstance

Description

You can call this operation to restart an RDS instance. The instance will be restarted in 10 seconds.

If there are a large number of transactions that must be submitted or rolled back, the restart process may be delayed for a minute.

Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The instance is not performing a backup task.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RestartDBInstance.
DBInstanceId	String	Yes	The ID of the instance to be restarted.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

- XML format

```
<RestartDBInstanceResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</RestartDBInstanceResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.3.4. DescribeDBInstanceAttribute

Description

You can call this operation to query the details of a specified instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceAttribute.
DBInstanceId	String	Yes	The ID of the instance to be queried. Up to 30 IDs can be entered at a time. Separate multiple ID with commas (,).

Response parameters

Parameter	Type	Example	Description
Items			The array that consists of DBInstanceAttribute data.

Parameter	Type	Example	Description
└DBInstanceId	String	rm-bpvxxxxx	The ID of the instance.
└PayType	String	Postpaid	The billing method of the instance. Valid values: • Postpaid: pay-as-you-go • Prepaid: subscription
└DBInstanceType	String	Primary	The role of the instance. Valid values: • Primary: primary instance • Readonly: read-only instance • Guard: disaster recovery instance • Temp: temporary instance
└Category	String	Basic	The category of the instance. Valid values: • Basic: basic edition • Standard: HA edition • Enterprise: finance edition
└InstanceNetworkType	String	Classic	The network type of the instance. Valid values: • Classic: classic network instance • VPC: VPC instance
└RegionId	String	cn-hangzhou	The region ID of the instance.
└ZoneId	String	cn-hangzhou-a	The zone ID of the instance.
└ConnectionString	String	rds-xxxxx.mysql.rds.aliyuncs.com	The endpoint used to connect the database.
└Port	String	3306	The port used to connect the instance.
└Engine	String	MySQL	The type of the database.
└EngineVersion	String	5.5	The version of the database.
└DBInstanceClassType	String	s	The family of the instance. Valid values: • s: shared instance • x: common instance • d: dedicated instance • h: dedicated host.
└DBInstanceClass	String	rds.mys2.small	The instance type.
└DBInstanceMemory	Long	240	The memory capacity of the instance. Unit: MB.

Parameter	Type	Example	Description
└DBInstanceStorage	Integer	10	The storage space of the instance. Unit: GB.
└DBInstanceNetType	String	Internet	The network connection type of the instance. Valid values: • Internet: public network • Intranet: internal network
└DBInstanceStatus	String	Running	The status of the instance. For more information, see Instance states in Appendix.
└DBInstanceDescription	String	Test instances	The description of the instance.
└LockMode	String	Unlock	The lock status of the instance. Valid values: • Unlock: normal • ManualLock: locked manually • LockByExpiration: locked automatically upon expiration • LockByRestoration: locked automatically before instance rollback • LockByDiskQuota: locked automatically for full disk space
└LockReason	String	None	The reason why the instance is locked.
└DBMaxQuantity	Integer	200	The maximum number of databases that can be created for an instance.
└AccountMaxQuantity	Integer	50	The maximum number of accounts that can be created for an instance.
└CreationTime	String	2011-05-30T12:11:4Z	The time when the instance was created. The time is in the yyyy-MM-ddThh:mmZ format. Example: 2011-05-30T12:11:4Z .
└ExpireTime	String	None	The expiration time of the instance. This parameter is not returned for pay-as-you-go instances.

Parameter	Type	Example	Description
└MaintainTime	String	00:00Z-02:00Z	The scheduled maintenance window of the instance. For example, `00:00Z-02:00Z` indicates that routine maintenance can be performed from 0:00 to 2:00.
└AvailabilityValue	String	100.0%	The availability status of the instance. Unit: %.
└MaxIOPS	Integer	150	The maximum number of I/O operations per second (IOPS).
└MaxConnections	Integer	60	The maximum number of concurrent connections to the instance.
└MasterInstanceId	String	null	The ID of the primary instance. If this parameter is not returned (null), the instance is a primary instance.
└IncrementSourceDBInstanceId	String	null	The instance ID of the incremental data source. For example, the incremental data source of a disaster recovery instance or read-only instance is the primary instance, and the incremental data source of the primary instance is null.
└GuardDBInstanceId	String	None	The ID of the disaster recovery instance attached to the instance.
└TempDBInstanceId	String	None	The ID of the temporary instance attached to the instance.
└ReadOnlyDBInstanceIds		rr-xxxxx	The IDs of the read-only instances attached to the instance.
└DBInstanceId	String	rm-bpxxxxx	The ID of the instance.
└VpcCloudInstanceId	String	vpc-xxxxx	The ID of the VPC instance.
└ResourceGroupId	String	3653788125	The ID of the resource group.
RequestId	String	1AD222E9-E606-4A42-BF6D-8A4442913CEF	The ID of the request.

DBInstanceAttribute parameters

Note You can call the DescribeDBInstanceHAConfig operation to query the primary and secondary node information of the instance.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeDBInstanceAttribute
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample success responses

JSON format

```
{ "Items":
  { "DBInstanceAttribute":
    [ { "LockMode": "Unlock",
      "ConnectionString": "rds-xxxxx.mysql.rds.aliyuncs.com",
      "CreationTime": "2014-10-10T10:28:48Z",
      "DBInstanceNetType": "Internet",
      "ReadOnlyDBInstanceIds": { "ReadOnlyDBInstanceId": [] },
      "MaxConnections": 60,
      "LockReason": "",
      "Engine": "MySQL",
      "AvailabilityValue": "100.0%",
      "AccountMaxQuantity": 50,
      "DBMaxQuantity": 200,
      "RegionId": "cn-hangzhou",
      "TempDBInstanceId": "",
      "DBInstanceMemory": 240,
      "MaxIOPS": 150,
      "DBInstanceType": "Primary",
      "DBInstanceStatus": "Running",
      "MasterInstanceId": "",
      "EngineVersion": "5.6",
      "IncrementSourceDBInstanceId": "",
      "GuardDBInstanceId": "",
      "DBInstanceStorage": 10,
      "DBInstanceDescription": "",
      "DBInstanceId": "rdsfnjfquxxxxx",
      "PayType": "Postpaid",
      "ExpireTime": "",
      "MaintainTime": "",
      "DBInstanceClass": "rds.mys2.small",
      "SecurityIPList": "11.11.11.11",
      "Port": "3306" } ] },
  "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```


Sample error responses

JSON format


```
{ "Code":"UnsupportedOperation",
"HostId":"rds.aliyuncs.com",
"Message":"The specified action is not supported.",
"RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.3.5. DescribeDBInstances

Description

You can call this operation to query instances and RAM-authorized instances.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeDBInstances	The operation that you want to perform. Set the valuer to DescribeDBInstances.
RegionId	String	Yes	cn-hangzhou	The region ID of the instance.
ConnectionMode	String	No	Performance	The access mode of the instance. Valid values: • Performance: standard access mode • Safe: safe access mode • If no value is specified, instances in both access modes are returned.

Parameter	Type	Required	Example	Description
DBInstanceType	String	No	Primary	The role of the instance. Valid values: • Primary: primary instance • Readonly: read-only instance • Guard: disaster recovery instance • Temp: temporary instance • If no value is specified, instance of all roles are returned.
InstanceNetworkType	String	No	Classic	The network type of the instance. Valid values: • VPC: VPC instance • Classic: classic network instance • If no value is specified, instance of both network types are returned.
PageNumber	Integer	No	1	The number of the page to return. Pages start from page 1 but must be equal to or smaller than the maximum Integer value. Default value: 1.

Parameter	Type	Required	Example	Description
PageSize	Integer	No	30	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30.
Tags	String	No	{ “key1” :” value 1” }	The tag of the instance, in the JSON format. The tag includes a key-value pair of TagKey and TagValue. TagValue can be left empty, but TagValue cannot. Example: { “key1” :” value 1” }.

Response parameters

Parameter	Type	Example	Description
PageNumber	Integer	1	The number of the page returned.
TotalRecordCount	Integer	1	The total number of entries.
PageRecordCount	Integer	1	The number of instances on the current page.
Items			The array that consists of instance data.
└DBInstanceId	String	rm-xxxxx	The ID of the instance.
└DBInstanceDescription	String	testforRemarks	The description of the instance.
└PayType	String	Postpaid	The billing method of the instance. Valid values: • Postpaid: pay-as-you-go • Prepaid: subscription

Parameter	Type	Example	Description
└DBInstanceType	String	Primary	The role of the instance. Valid values: • Primary: primary instance • ReadOnly: read-only instance • Guard: disaster recovery instance • Temp: temporary instance
└InstanceNetworkType	String	Classic	The network type of the instance. Valid values: • Classic: classic network instance • VPC: VPC instance
└ConnectionMode	String	Performance	The access mode of the instance. Valid values: • Performance: standard access mode • Safe: safe access mode
└RegionId	String	cn-hangzhou	The region ID of the instance.
└ExpireTime	String	None	The expiration time of the instance. This parameter is not returned for pay-as-you-go instances.
└DBInstanceStatus	String	Intranet	The status of the instance. For more information, see Instance states in Appendix.
└Engine	String	MySQL	The type of the database.

Parameter	Type	Example	Description
└DBInstanceNetType	String	Internet	The network connection type of the instance. Valid values: • Internet: public network • Intranet: internal network
└LockMode	String	Unlock	The lock status of the instance. Valid values: • Unlock: normal • ManualLock: locked manually • LockByExpiration: locked automatically upon expiration • LockByRestoration: locked automatically before instance rollback • LockByDiskQuota: locked automatically for full disk space
└LockReason	String	None	The reason why the instance is locked.
└MasterInstanceId	String	null	The ID of the primary instance. If this parameter is not returned (null), the instance is a primary instance.
└GuardDBInstanceId	String	None	The ID of the disaster recovery instance attached to the instance.
└TempDBInstanceId	String	None	The ID of the temporary instance attached to the instance.
└VpcCloudInstanceId	String	vpc-xxxxx	The ID of the VPC instance.
└ReadOnlyDBInstanceIds			None
└DBInstanceId	String	rm-xxxxx	The ID of the instance.

Parameter	Type	Example	Description
RequestId	String	1AD222E9-E606-4A42-BF6D-8A4442913CEF	The ID of the request.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeDBInstances
&RegionId=cn-hangzhou
&Engine=MySQL
&<Common request parameters>
```

Sample success responses

- XML format

```
<DescribeDBInstancesResponse>
<PageRecordCount>2</PageRecordCount>
<Items>
<DBInstance>
<DBInstanceDescription>testforRemarks</DBInstanceDescription>
<ExpireTime>2014-10-10T16:00:00Z</ExpireTime>
<DBInstanceId>rdsmjfirxxxxx</DBInstanceId>
<DBInstanceNetType>Internet</DBInstanceNetType>
<PayType>Prepaid</PayType>
<DBInstanceStatus>Running</DBInstanceStatus>
<DBInstanceType>Primary</DBInstanceType>
<Engine>MySQL</Engine>
<LockMode>Unlock</LockMode>
<LockReason/>
<RegionId>cn-hangzhou</RegionId>
<ZoneId>cn-hangzhou-a</ZoneId>
<MasterInstanceId/>
<GuardDBInstanceId/>
<TempDBInstanceId/>
<ReadOnlyDBInstanceIds>
<ReadOnlyDBInstanceId/> </ReadOnlyDBInstanceIds>
</DBInstance>
</Items>
<PageNumber>1</PageNumber>
<TotalRecordCount>2</TotalRecordCount>
<RequestId>2553A660-E4EB-4AF4-A402-8AFF70A49143</RequestId>
</DescribeDBInstancesResponse>
```

- JSON format

```
{ "Items":
  { "DBInstance":
    [ { "DBInstanceDescription":"testforRemarks",
      "DBInstanceId":"rdsmjfirxxxxx",
      "DBInstanceNetType":"Internet",
      "DBInstanceStatus":"Running",
      "DBInstanceType":"Primary",
      "Engine":"MySQL",
      "ExpireTime":"2014-10-10T16:00:00Z",
      "GuardDBInstanceId ":"",
      "LockMode":"Unlock",
      "LockReason":"",
      "MasterInstanceId":"",
      "PayType":"Prepaid",
      "ReadOnlyDBInstanceIds":{ "ReadOnlyDBInstanceId":[] },
      "RegionId":"cn-hangzhou",
      "TempDBInstanceId":"",
      "ZoneId":"cn-hangzhou-a" },
    ] },
  "PageNumber":1,
  "PageRecordCount":2,
  "RequestId":"2553A660-E4EB-4AF4-A402-8AFF70A49143",
  "TotalRecordCount":2
}
```


- **Sample error responses**

  JSON format


```
{ "Code":"UnsupportedOperation",
"HostId":"rds.aliyuncs.com",
"Message":"The specified action is not supported.",
"RequestId":"7463B73D-35CC-4D19-A010-6B8D65D242EF"}
```


2.8.1.3.6. ModifyDBInstanceSpec

Description

You can call this operation to change the type or storage space of instances. Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The instance is not performing a backup task.
- Either the instance type (DBInstanceClass) or storage space (DBInstanceStorage) parameter must be specified in the request.

- When reducing the amount of disk space, ensure that the target amount of disk space is no less than 1.1 times the actual space used.
- Only common and read-only instances allow configuration changes. Configurations of disaster recovery and temporary instances cannot be modified.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyDBInstanceSpec	The operation that you want to perform. Set the value to ModifyDBInstanceSpec.
DBInstanceId	String	Yes	rm-bpxxxx	The ID of the instance whose type or storage space is modified.
PayType	String	Yes	Postpaid	The billing method of the instance. Valid values: • Postpaid: pay-as-you-go • Prepaid: subscription
AccessKeyId	String	No	LTAIKw8gqxxxxx	The AccessKey ID provided by Alibaba Cloud.
ClientToken	String	No	ETnLKlblzczshOTUbOCziJZNwHlYBQ	The client token that is used to ensure the idempotence of the request.
DBInstanceClass	String	No	rds.mys2.small	The type of the instance. For more information, see Appendix Instance types.

Parameter	Type	Required	Example	Description
DBInstanceStorage	Integer	No	20	The user-defined storage space. This value must be a multiple of 5 GB. Unit: GB. Valid values: • MySQL, PostgreSQL, or PPAS HA edition: 5 to 2000 • MySQL 5.7 basic edition: 20 to 1000
EffectiveTime	String	No	Immediate	The time when the changes take effect. Valid values: Immediate and MaintainTime. Default value: Immediate
OwnerAccount	String	No	testuser@aliyun.com	The Apsara Stack tenant account.

Response parameters

Parameter	Type	Example	Description
RequestId	String	1AD222E9-E606-4A42-BF6D-8A4442913CEF	The ID of the request.

Examples

Sample requests

```
https://rds.example.com/?Action=ModifyDBInstanceSpec
&DBInstanceId=rds-xxxxx
&PayType=Postpaid
&DBInstanceStorage=10
&<Common request parameters>
```

Sample success responses

- XML format

```
<ModifyDBInstanceSpecResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ModifyDBInstanceSpecResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

Sample error responses

JSON format

```
{ "Code":"UnsupportedOperation",
"HostId":"rds.aliyuncs.com",
"Message":"The specified action is not supported.",
"RequestId":"7463B73D-35CC-4D19-A010-6B8D65D242EF"}
```

2.8.1.3.7. AllocateInstancePublicConnection

Description

You can call this operation to apply for a public endpoint for a specified instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AllocateInstancePublicConnection.
DBInstanceId	String	Yes	The ID of the instance for which the public endpoint is applied.
ConnectionStringPrefix	String	Yes	The endpoint to be used by the instance.
Port	String	Yes	The external port to be used by the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=AllocateInstancePublicConnection
&DBInstanceId=rds-xxxxx
&ConnectionStringPrefix=test0001
&Port=3306
&<Common request parameters>
```

Sample responses

- XML format

```
<AllocateInstancePublicConnectionResponse>
<RequestId>65BDA532-28AF-4122-AA39-B382721EEE64</RequestId>
</AllocateInstancePublicConnectionResponse>
```

- JSON format

```
{ "RequestId": "65BDA532-28AF-4122-AA39-B382721EEE64"}
```

2.8.1.3.8. ReleaseInstancePublicConnection

Description

You can call this operation to release the public endpoint of an instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ReleaseInstancePublicConnection.
DBInstanceId	String	Yes	The ID of the instance whose public endpoint is released.
CurrentConnectionString	String	Yes	The public endpoint.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=ReleaseInstancePublicConnection
&DBInstanceId=rds-xxxxx
&CurrentConnectionString=test0001.mysql.rds.example.com
&<Common request parameters>
```

Sample responses

- XML format

```
<ReleaseInstancePublicConnectionResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ReleaseInstancePublicConnectionResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.3.9. SwitchDBInstanceNetType

Description

You can call this operation to switch the network type of an instance between internal and public networks. After switching, the endpoint of the instance changes. You must modify the endpoint in the code and restart the application.

Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- There have been less than 20 switching operations performed within the last 24 hours.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to SwitchDBInstanceNetType.
DBInstanceId	String	Yes	The ID of the instance for which the network connection type is modified.
ConnectionString Prefix	String	Yes	The unique endpoint to be used. It can be up to 30 characters in length and can contains lowercase letters, digits, and hyphens (-). It must start with a letter.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

2.8.1.3.10. DescribeDBInstanceNetInfo

Description

You can call this operation to query the connection information of a specified instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceNetInfo.
DBInstanceId	String	Yes	The ID of the instance whose connection information is queried.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
DBInstanceNetInfos	List<DBInstanceAttribute>	The array that consists of DBInstanceAttribute data.
InstanceNetworkType	String	VPC: VPC instance Classic: classic network instance

DBInstanceNetInfo parameters

Parameter	Type	Description
ConnectionString	String	The DNS connection string.
IPAddress	String	The IP address.
IPType	String	Valid values for classic network instances: Inner and Public. Valid values for VPC instances: Private and Public.
Port	String	The port information.
VPCId	String	The ID of the VPC.
VSwitchId	String	The ID of the VSwitch.

2.8.1.3.11. ModifyDBInstanceConnectionString

Description

You can call this operation to modify the endpoint and port of a connection string.

RDS provides the internal and public endpoints and allows both types to coexist in a specific access mode.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceConnectionString.
DBInstanceId	String	Yes	The ID of the instance whose connection string is modified.
CurrentConnectionString	String	Yes	The endpoint used by the instance.
ConnectionStringPrefix	String	No	The endpoint to be used by the instance.
Port	String	No	The port to be used by the instance.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

2.8.1.3.12. ModifyDBInstanceConnectionMode

Description

You can call this operation to modify the access mode of RDS instances. Two access modes are available for RDS:

- Standard access mode
- Safe access mode

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceConnectionMode.
DBInstanceId	String	Yes	The ID of the instance for which the access mode is modified.
ConnectionMode	String	Yes	The access mode of the instance. Performance: standard access mode. Safe: safe access mode.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

2.8.1.3.13. ModifyDBInstanceNetworkType

Description

You can call this operation to switch the network type of an RDS instance between VPC and classic network.

> Note Only the classic network instances with the ConnectionMode set to Safe can have their network type switched to VPC.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceNetworkType.
DBInstanceId	String	Yes	The ID of the instance for which the network type is modified.
InstanceNetworkType	String	Yes	The network type of the instance. VPC: VPC instance. Classic: classic network instance.
VPCId	String	No	The ID of the VPC.
VSwitchId	String	No	The ID of the VSwitch. This parameter is required if the value of VPCId is specified.
PrivateIpAddress	String	No	The VPC IP address that belongs to the specified VSwitch. If no value is specified, the system automatically assigns a VPC IP address based on VPCId and VSwitchId.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

2.8.1.3.14. DescribeDBInstanceIPArrayList

Description

You can call this operation to query the IP whitelist of an instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceIPArrayList.
DBInstanceId	String	Yes	The ID of the instance whose IP whitelist is queried.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
Items	List<DBInstanceIPArray>	The array that consists of DBInstanceIPArray data.

DBInstanceIPArray parameters

Parameter	Type	Description
DBInstanceIPArrayName	String	The name of the IP whitelist.
DBInstanceIPArrayAttribute	String	The attribute of the IP whitelist. Default value: null. Whitelists tagged with "hidden" are not displayed in the console.
SecurityIPList	String	The IP addresses in an IP address whitelist. Separate multiple IP addresses with commas (,). You can add a maximum of 1,000 different IP addresses to a whitelist. Supported formats of IP addresses are IP addresses such as 0.0.0.0/0 and 10.23.12.24, or Classless Inter-Domain Routing (CIDR) blocks such as 10.23.12.24/24. /24 indicates the length of the IP address prefix. The IP address prefix can consist of 1 to 32 bits.

2.8.1.3.15. ModifySecurityIps

Description

You can call this operation to modify the IP whitelist of an instance.

Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The instance is not locked by the system.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifySecurityIps.
DBInstanceId	String	Yes	The ID of the instance whose IP whitelist is modified.
SecurityIps	String	No	The IP addresses in an IP address whitelist. Separate multiple IP addresses with commas (,). You can add a maximum of 1,000 different IP addresses to a whitelist. Supported formats of IP addresses are IP addresses such as 0.0.0.0/0 and 10.23.12.24, or Classless Inter-Domain Routing (CIDR) blocks such as 10.23.12.24/24. /24 indicates the length of the IP address prefix. The IP address prefix can consist of 1 to 32 bits.
DBInstanceIPArrayName	String	No	The name of the IP whitelist. If no value is specified, the whitelist named Default will be modified.
DBInstanceIPArrayAttribute	String	No	The attribute of the IP whitelist. Default value: null. Whitelists tagged with "hidden" are not displayed in the console.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=ModifySecurityIps
&DBInstanceId=rds-xxxxx
&SecurityIps=192.168.1.2
&<Common request parameters>
```

Sample responses

- XML format

```
<ModifySecurityIpsResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ModifySecurityIpsResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.3.16. DescribeRegions

Description

You can call this operation to query the available RDS regions and zones.

Before you call the CreateInstance operation, call this operation to query region IDs.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeRegions.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Regions	List<RDSRegion>	The array that consists of RDSRegion data.

RDSRegion parameters

Parameter	Type	Description
RegionId	String	The region ID.
ZoneId	String	The zone ID.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeRegions
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeRegionsResponse>
<Regions>
<RDSRegion>
<RegionId>cn-hangzhou</RegionId>
<ZoneId>cn-hangzhou-a</RegionId>
</RDSRegion>
<RDSRegion>
<RegionId>cn-hangzhou</RegionId
><ZoneId>cn-hangzhou-b</ZoneId>
</RDSRegion>
</Regions>
<RequestId>A36D9720-7902-42A4-B8B9-014A2135E6C3</RequestId>
</DescribeRegionsResponse>
```

- JSON format

```
{ "Regions":
   { "RDSRegion":
      [ {"RegionId": "cn-hangzhou",
         "ZoneId":"cn-hangzhou-a"},
        {"RegionId": "cn-hangzhou",
         "ZoneId":"cn-hangzhou-b"},
         ]},
   "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"
}
```

2.8.1.3.17. DescribeDBInstanceHAConfig

Description

You can call this operation to query the zone information and data replication status of instances.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceHAConfig.
DBInstanceId	String	Yes	The ID of the instance for which the zone information and data replication status are queried.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
DBInstanceId	String	The ID of the instance for which the zone information and data replication status were queried.
SyncMode	String	The synchronization mode. Valid values: Sync, Semi-sync, and Async.
HAMode	String	The high availability mode. RPO: Data persistence is preferred. RTO: Instance availability is preferred.
HostInstanceInfos	List<NodeInfo>	The array that consists of NodeInfo data.

NodeInfo parameters

Parameter	Type	Description
NodeId	String	The unique ID of the primary or secondary node.
NodeType	String	The type of the node. Master: primary node. Slave: secondary node.
RegionId	String	The region ID of the instance.
ZoneId	String	The zone ID of the instance.
SyncStatus	String	The synchronization status of the instance. NotAvailable: A failure has occurred and synchronization is unavailable. Syncing: Synchronization is in process, with a probability of data loss during failovers. Synchronized: Synchronization is completed. NotSupport: Synchronization is not supported by the engine type or version.
LogSyncTime	String	The time when the secondary database receives logs.
DataSyncTime	String	The time when the secondary database receives data.

2.8.1.3.18. MigrateToOtherZone

Description

You can call this operation to migrate an instance from one zone to another.

For example, if instance 1 is located in the Hangzhou Zone A zone of the China (Hangzhou) region, you can call this operation to migrate the instance to the Hangzhou Zone B zone of the China (Hangzhou) region.

Note In cross-zone migration, instances must be migrated within the same region. For example, instances in a zone of the China (Hangzhou) region cannot be migrated to a zone of the China (Qingdao) region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to MigrateToOtherZone.
DBInstanceId	String	Yes	The ID of the instance to be migrated.
ZoneId	String	Yes	The zone ID of the instance. You can call the DescribeRegions operation to query available zones.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=MigrateToOtherZone
&DBInstanceId=rds-xxxxx
&ZoneId=cn-hangzhou-b
&<Common request parameters>
```

Sample responses

- XML format

```
<MigrateToOtherZoneResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</MigrateToOtherZoneResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.3.19. PurgeDBInstanceLog

Description

You can call this operation to clear all binlogs for a MySQL instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to PurgeDBInstanceLog.
DBInstanceId	String	Yes	The ID of the instance for which all binlogs are cleared.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=PurgeDBInstanceLog
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<PurgeDBInstanceLogResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</PurgeDBInstanceLogResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.3.20. UpgradeDBInstanceEngineVersion

Description

You can call this operation to upgrade the database version of an instance. For example, you can upgrade the database version from MySQL 5.1 to MySQL 5.5.

If a read-only or disaster recovery instance is attached to the primary instance, you must first upgrade the database version of the attached instance.

Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The specified database version must be later than the current database version of the target instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to UpgradeDBInstanceEngineVersion.
DBInstanceId	String	Yes	The instance to be upgraded.
EngineVersion	String	Yes	The database version to be upgraded to.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
TaskId	Integer	The ID of the task.

Examples

Request parameters

```
https://rds.example.com/?Action=UpgradeDBInstanceEngineVersion
&DBInstanceId=rds-xxxxx
&EngineVersion=5.6
&<Common request parameters>
```

Response parameters

- XML format

```
<UpgradeDBInstanceEngineVersionResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<TaskId>124378</Taskid>
</UpgradeDBInstanceEngineVersionResponse>
```

- JSON format

```
{"RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC",
"TaskId":" 124378" }
```

2.8.1.3.21. ModifyDBInstanceDescription

Description

You can call this operation to modify the description of an instance to identify the instance easily. For example, you can modify the description of an instance to *Alibaba Cloud testing environment instance*.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceDescription.
DBInstanceId	String	Yes	The ID of the instance whose description is modified.
DBInstanceDescription	Sting	Yes	The description of the instance.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=ModifyDBInstanceDescription
&DBInstanceId=rds-xxxxx
&DBInstanceDescription=testdescribe
&<Common request parameters>
```

Sample responses

- XML format

```
<ModifyDBInstanceDescriptionResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ModifyDBInstanceDescriptionResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.3.22. ModifyDBInstanceMaintainTime

Description

You can call this operation to modify the scheduled period for routine maintenance. You can set the maintenance window to an off-peak period.

Alibaba Cloud performs routine maintenance during the maintenance window to minimize the impact on your services.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceMaintainTime.
DBInstanceId	String	Yes	The ID of the instance whose maintenance window is modified.
MaintainTime	String	Yes	The maintenance window of the instance. Valid values: 22:00Z-02:00Z 02:00Z-06:00Z 06:00Z-10:00Z 10:00Z-14:00Z 14:00Z-18:00Z 18:00Z-22:00Z

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=ModifyDBInstanceMaintainTime
&DBInstanceId=rds-xxxxx
&MaintainTime=22:00Z-02:00Z
&<Common request parameters>
```

Sample responses

- XML format

```
<ModifyDBInstanceMaintainTimeResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ModifyDBInstanceMaintainTimeResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.3.23. ModifyDBInstanceHAConfig

Description

You can call this operation to modify the instance data replication mode and high availability switching rules.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceHAConfig.
DBInstanceId	String	Yes	The ID of the instance for which the data replication mode and high availability switching rules are modified.
SyncMode	String	Yes	The synchronization mode of the instance. Valid values: Sync, Semi-sync, and Async.
HAMode	String	Yes	The HA mode of the instance. RPO: Data persistence is preferred. RTO: Instance availability is preferred.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

2.8.1.3.24. SwitchDBInstanceHA

Description

You can call this operation to change the database used as the primary database. RDS instances are composed of primary and secondary databases distributed across different servers. The new primary database bears the service traffic.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to SwitchDBInstanceHA.
DBInstanceId	String	Yes	The ID of the primary instance.
NodeId	String	Yes	The unique ID of the node. You can call the DescribeDBInstanceHAConfig operation to query the value of this parameter.

Parameter	Type	Required	Description
Force	String	Yes	Yes: forced. No: unforced. Default value: No.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

2.8.1.3.25. CreateReadOnlyDBInstance

Description

You can call this operation to create a read-only instance for a primary RDS instance. Before you call this operation, ensure that the following requirements are met:

- The instance is in the running but not failover state.
- The read-only instance must be in the same region as the primary instance.
- The database version of the read-only instance must be the same as or later than that of the primary instance. The primary instance must be a MySQL 5.6 or later instance.
- The read-only instance must be a MySQL 5.6 or later instance.
- A primary RDS instance can have up to five read-only instances.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateReadOnlyDBInstance.
RegionId	String	Yes	The region ID of the instance. It can be up to 50 characters in length. You can call the DescribeRegions operation to query available regions.
ZoneId	String	Yes	The zone ID of the instance. You can call the DescribeRegions operation to query available zones.
DBInstanceId	String	Yes	The ID of the primary instance.
EngineVersion	String	Yes	The database version of the instance. Set the value to 5.6.
DBInstanceClass	String	Yes	The type of the instance. For more information, see Instance types in Appendix.
DBInstanceStorage	Integer	Yes	The user-defined storage space. Valid values: 5 to 1000. This value must be a multiple of 5 GB. Unit: GB.

Parameter	Type	Required	Description
DBInstanceDescription	String	No	The description of the instance. It can be up to 256 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with http:// or https://. It must start with a letter.
PayType	String	Yes	The billing method. Set the value to Postpaid.
ClientToken	String	Yes	The client token that is used to ensure the idempotence of the request.
InstanceNetworkType	String	No	The network type of the instance. Valid values: VPC and Classic. Default value: Classic.
VPCId	String	No	The ID of the VPC.
VSwitchId	String	No	The ID of the VSwitch.
PrivateIpAddress	String	No	The IP address of the VPC that belongs to VSwitchId. If no value is specified, the system automatically allocates a VPC IP address based on VPCId and VSwitchId.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
DBInstanceId	String	The ID of the instance added.
OrderId	String	The ID of the order.
ConnectionString	String	The endpoint used to connect the database.
Port	String	The port used to connect the database.

Examples

Sample requests

```
https://rds.example.com/?Action=CreateReadOnlyDBInstance
&RegionId=cn-hangzhou
&ZoneId=cn-hangzhou-b
&DBInstanceId=rds-xxxxx
&EngineVersion=5.6
&DBInstanceClass=rds.mys2.small
&DBInstanceStorage=10
&PayType=Postpaid
&ClientToken=ETnLKxxxxx
&<[Common request parameters]>
```

Sample responses

- XML format

```
<CreateDBInstanceResponse>
<OrderId>10078937xxxxx</OrderId>
<ConnectionString>rds-xxxxx.mysql.rds.aliyuncs.com </ConnectionString>
<DBInstanceId>rds-xxxxx</DBInstanceId>
<port>3306</port>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</CreateDBInstanceResponse>
```

- JSON format

```
{ "OrderId": "100789370230206",
"ConnectionString": "rds-xxxxx.mysql.rds.aliyuncs.com",
"DBInstanceId": "rds-xxxxx",
"Port": "3306",
"RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.3.26. DescribeDBInstanceSSL

Description

You can call this operation to query the SSL link of the instance. This operation is only supported on MySQL 5.6 and MySQL 5.7.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceSSL.

Parameter	Type	Required	Description
DBInstanceId	String	Yes	The ID of the instance for which the SSL link is queried.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
ConnectionString	String	The connection string protected by the SSL certificate.
SSLExpireTime	String	The expiration time of the SSL certificate. The time is in the yyyy-MM-ddThh:mmZ format.
RequireUpdate	String	Specifies whether an immediate upgrade is required. Valid values: Yes and No.
RequireUpdateReason	String	The reasons why an upgrade is recommended.

2.8.1.3.27. ModifyDBInstanceSSL

Description

You can call this operation to modify the SSL link of the instance. This operation is only supported on MySQL 5.6 and MySQL 5.7.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceSSL.
DBInstanceId	String	Yes	The ID of the instance for which the SSL link is modified.
ConnectionString	String	Yes	Each instance can only have one connection string protected by the SSL certificate. The SSL certificate can be created or updated for the connection string.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
SSLExpireTime	String	The expiration time of the SSL certificate. The time is in the yyyy-MM-ddThh:mmZ format.

2.8.1.3.28. DescribeDBInstanceTDE

Description

You can call this operation to query the TDE status of the instance. This operation is only supported on MySQL 5.6 and MySQL 5.7.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceTDE.
DBInstanceId	String	Yes	The ID of the instance for which TDE is enabled or disabled.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
TDEStatus	String	The TDE status of the instance. Valid values: Enabled and Disabled.
Databases	List<DataBase>	The array that consists of Database data.

DataBase parameters:

Parameter	Type	Description
DBName	String	The name of the database.
TDEStatus	String	The TDE status of the database. Valid values: Enabled and Disabled.

2.8.1.3.29. ModifyDBInstanceTDE

Description

You can call this operation to modify TDE status of the instance. This operation is only supported on MySQL 5.6 and MySQL 5.7. TDE can only be enabled on instances and cannot be disabled. The DBName value cannot be accepted either.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceTDE.
DBInstanceId	String	Yes	The ID of the instance for which TDE is enabled or disabled.
TDEStatus	String	Yes	The TDE status of the instance. Valid values: Enabled and Disabled.
DBName	String	No	The name of the database. Up to 50 names can be entered in a single request. Separated multiple names with commas (,).

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

2.8.1.4. Database management

2.8.1.4.1. CreateDatabase

Description

You can call this operation to create a new database in an instance. Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The instance is not locked by the system.
- The maximum number of databases in the instance is not reached.
- The instance is a primary instance.

Note This operation is not supported on PostgreSQL or PPAS. Users of PostgreSQL and PPAS instances can perform the CREATE DATABASE operation through SQL instead.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateDatabase.
DBInstanceId	String	Yes	The ID of the instance to which the database is added.

Parameter	Type	Required	Description
DBName	String	Yes	The unique name of the database. The name can be up to 64 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a letter. For more information about invalid characters, see Forbidden keywords.
CharacterSetName	String	Yes	The character set. Valid values: MySQL: utf8, gbk, latin1, and utf8mb4
DBDescription	String	No	The description of the database. It can be up to 256 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with http:// or https://. It must start with a letter.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=CreateDatabase
&CharacterSetName=gbk
&DBName=testDB
&DBInstanceId=rds-xxxxx
&<[Common request parameters]>
```

Sample responses

- XML format

```
<CreateDatabaseResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</CreateDatabaseResponse>
```

- JSON format

```
{ "RequestID":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.4.2. DeleteDatabase

Description

You can call this operation to delete a database from an instance.

Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The instance is a primary instance.

> Note This operation is not supported on PostgreSQL or PPAS. Users of PostgreSQL and PPAS instances are permitted to perform the DROP DATABASE operation through SQL.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteDatabase.
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.
DBName	String	Yes	The name of the database.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=DeleteDatabase
&DBName=testDB
&DBInstanceId=rds-xxxxx
&<[Common request parameters]>
```

Sample responses

- XML format

```
<DeleteDatabaseResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</DeleteDatabaseResponse>
```

- JSON format

```
{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.4.3. DescribeDatabases

Description

You can call this operation to query the database list information for a specified instance and database. If the search parameters are entered incorrectly, an error prompt is returned and the returned data is empty.

> Note This operation is not supported on PostgreSQL or PPAS.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDatabases.
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.
DBName	String	No	The name of the database.
DBStatus	String	No	The status of the database. Valid values: Creating, Running, and Deleting.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Databases	List<Database>	The array that consists of Database data.

Database parameters

Parameter	Type	Description
DBName	String	The name of the database.
DBInstanceId	String	The ID of the instance to which the database belongs.
Engine	String	The role of the database instance.
DBStatus	String	The status of the database. Valid values: Creating, Running, and Deleting.

Parameter	Type	Description
CharacterSetName	String	The character set.
DBDescription	String	The description of the database.
Accounts	List<AccountPrivilegeInfo>	The array that consists of AccountPrivilegeInfo data.
Account	String	The name of the account used to access the database.
AccountPrivilege	String	The permissions of the account on the database.

AccountPrivilegeInfo parameters

Parameter	Type	Description
Account	String	The name of the account used to access the database.
AccountPrivilege	String	The permissions of the account on the database.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeDatabases
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeDatabasesResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<Databases>
<Database>
<Engine>MySQL</Engine>
<DBName>testdb</DBName>
<CharacterSetName>utf8</CharacterSetName>
<DBStatus>Creating</DBStatus>
<DBInstanceId>rds-xxxxx</DBInstanceId>
<Accounts>
<AccountPrivilegeInfo></AccountPrivilegeInfo>
<Accounts>
</Database>
</Databases>
</DescribeDatabasesResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC",
"Databases":
 { "Database":
  [ { "Engine": "MySQL",
   "CharacterSetName": "utf8",
   "DBStatus": "Creating",
   "DBDescription": "",
   "DBInstanceId": "rds-xxxxx",
   "Accounts": { " AccountPrivilegeInfo": [] },
   "DBName": "testdb" }] }
   }
```

2.8.1.4.4. ModifyDBDescription

Description

You can call this operation to modify the description of a database to facilitate user records. For example, you can modify the description of a database to Instance database A for Alibaba Cloud testing environment.

> **Note** This operation is not supported on PostgreSQL or PPAS.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBDescription.
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.
DBName	String	Yes	The name of the database.
DBDescription	String	Yes	The description of the database.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=ModifyDBDescription
&DBInstanceId=rds-xxxxx
&DBInstanceDescription=testDBdescribe
&<Common request parameters>
```

Sample responses

- XML format

```
<ModifyDBDescriptionResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ModifyDBDescriptionResponse>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.5. Account management

2.8.1.5.1. CreateAccount

Description

> **Note**
>
> In the same instance, one account can manage multiple databases with different permissions.

You can call this operation to create an account for a database. Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The database is in the running state.
- The instance is not locked by the system.
- The maximum number of accounts for a single instance is not reached.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateAccount.
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.
AccountName	String	Yes	The unique name of the account. The name can be up to 16 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a letter. For more information about invalid characters, see Forbidden keywords.
AccountPassword	String	Yes	The password for the account. It must be 6 to 32 characters in length and can contain letters, digits, and underscores (_).
AccountType	String	No	The type of the account. Valid values: Normal and Super. Default value: Normal. This parameter is only valid for MySQL 5.6 and MySQL 5.7. PostgreSQL and PPAS can each have only a single initial account. Other accounts must be created by the initial account when it is logged on to the database.
AccountDescription	String	No	The description of the account. It can be up to 256 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with http:// or https://. It must start with a letter.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=CreateAccount
&AccountName=testacc02
&AccountPassword=pwxxxxx
&DBInstanceId=rds-xxxxx
&<[Common request parameters]>
```

Sample responses

- XML format

```
<CreateAccountResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</CreateAccountResponse>
```

- JSON format

```
{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.5.2. DeleteAccount

Description

You can call this operation to delete a database account.

The instance must be in the running state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteAccount.
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.
AccountName	String	Yes	The unique name of the account. The name can be up to 16 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a letter. For more information about invalid characters, see Forbidden keywords.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=DeleteAccount
&DBInstanceId=rds-xxxxx
&AccountName=testacc01
&<[Common request parameters]>
```

Sample responses

- XML format

```
<DeleteAccountResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</DeleteAccountResponse>
```

- JSON format

```
{ "RequestID":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.5.3. DescribeAccounts

Description

You can call this operation to query the account list information for a specified instance and database and the information of its associated accounts.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeAccounts.
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.
AccountName	String	Yes	The name of the account.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
Accounts	List<DBInstanceAccount>	The array that consists of DBInstanceAccount data.

DBInstanceAccount parameters

Parameter	Type	Description
DBInstanceId	String	The ID of the instance to which the account belongs.
AccountName	String	The name of the database account.
AccountStatus	String	The account status. Valid values: Unavailable and Available.
AccountDescription	String	The description of the account.
DatabasePrivileges	List<DatabasePrivilege>	The array that consists of DatabasePrivileges data.
AccountType	String	The type of the account. Valid values: Normal and Super.

DatabasePrivilege parameters

Parameter	Type	Description
DBName	String	The name of the database.
AccountPrivilege	String	The name of the database account.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeAccounts
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeAccountsResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<Accounts>
<DBInstanceAccount>
<AccountName>MySQL</AccountName>
<DBInstanceId>testdb</DBInstanceId>
<AccountStatus>utf8</AccountStatus>
<AccountDescription>
</AccountDescription>
<DatabasePrivileges>
<DatabasePrivilege></DatabasePrivilege>
</DatabasePrivileges>
<DBInstanceAccount>
</Accounts>
</DescribeAccountsResponse>
```

- JSON format

```
{ "Accounts":
  { "DBInstanceAccount":
    [ { "AccountDescription": "",
      "DBInstanceId": "rds-xxxxx",
      "DatabasePrivileges": { "DatabasePrivilege": [] },
      "AccountStatus": "Unavailable",
      "AccountName": "testaccount" } ] },
  "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.5.4. GrantAccountPrivilege

Description

You can call this operation to grant database access permissions to accounts. A single account can be associated with one or more databases.

If the specified account already has access permissions on the specified database, the operation directly returns a successful response.

The instance must be in the running state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to GrantAccountPrivilege.

Parameter	Type	Required	Description
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.
AccountName	String	Yes	The name of the account.
DBName	String	Yes	The name of the database associated with the account.
AccountPrivilege	String	Yes	The permissions of the account. Valid values: ReadOnly and ReadWrite.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=GrantAccountPrivilege
&AccountName=testacc02
&AccountPrivilege=readwrite
&DBName=testdb03
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<GrantAccountPrivilegeResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</GrantAccountPrivilegeResponse>
```

- JSON format

```
{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.5.5. RevokeAccountPrivilege

Description

You can call this operation to revoke database access permissions from an account. Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The database is in the running state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RevokeAccountPrivilege.
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.
AccountName	String	Yes	The name of the account.
DBName	String	Yes	The name of the database.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=RevokeAccountPrivilege
&AccountName=testacc02
&DBName=testdb03
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<RevokeAccountPrivilegeResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</RevokeAccountPrivilegeResponse>
```

- JSON format

```
{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.5.6. ModifyAccountDescription

Description

You can call this operation to modify the description of an account to facilitate user records. For example, you can modify the description of an account to Account A for Alibaba Cloud testing environment.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyAccountDescription.
DBInstanceId	String	Yes	The ID of the instance for which the account description is modified.
AccountName	String	Yes	The unique name of the account. The name can be up to 16 characters in length and can contain lowercase letters, digits, and underscores (_). It must start with a letter. For more information about invalid characters, see Forbidden keywords.
AccountDescription	String	Yes	The description of the account. It can be up to 256 characters in length and can contain letters, digits, underscores (_), and hyphens (-). It cannot start with http:// or https://. It must start with a letter.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=ModifyAccountDescription
&DBInstanceId=rds-xxxxx
&AccountName=testacc01
&AccountDescription=testAccoutdescribe
&<Common request parameters>
```

Sample responses

- XML format

```
<ModifyAccountDescription>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ModifyAccountDescription>
```

- JSON format

```
{ "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.5.7. ResetAccountPassword

Description

You can call this operation to reset the account password. Before you call this operation, ensure that the following requirements are met:

The instance is in the running state and not locked by the system.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ResetAccountPassword.
DBInstanceId	String	Yes	The ID of the instance for which the account password is reset.
AccountName	String	Yes	The name of the account.
AccountPassword	String	Yes	The new password. It must be 6 to 32 characters in length and can contain letters, digits, and underscores (_).

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=ResetAccountPassword
&AccountName=testacc02
&AccountPassword=pwxxxxx
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<ResetAccountPasswordResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ResetAccountPasswordResponse>
```

- JSON format

```
{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.5.8. ResetAccount

Description

You can call this operation to reset the initial account of an instance.

This operation is not applicable to MySQL 5.6 or MySQL 5.7 instances that do not have privileged accounts.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ResetAccount.
DBInstanceId	String	Yes	The ID of the instance for which the initial account is reset.
AccountName	String	Yes	The name of the account.
AccountPassword	String	Yes	The password for the account.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

2.8.1.6. Backup and restoration

2.8.1.6.1. CreateBackup

Description

You can call this operation to manually create a backup. Up to 10 backups can be created for an instance in a single day.

Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The most recent backup has been completed.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateBackup.
DBInstanceId	String	Yes	The ID of the instance for which the backup is created.
BackupMethod	String	No	The backup method. Valid values: Logical and Physical. Default value: Physical. Logical backup cannot be used for instances without databases.
BackupStrategy	String	No	The logical backup range. db: single-database backup. instance: instance backup. This parameter is valid only when BackupMethod is set to Logical.
DBName	String	No	The name of the database for logical single-database backup. This parameter is valid only when BackupMethod is set to Logical and BackupStrategy is set to db.
BackupType	String	No	The backup type. Auto: specifies whether it is a full backup or an incremental backup through automatic calculation. FullBackup: specifies a full backup. Default value: Auto

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action= CreateBackup
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<CreateBackupResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</CreateBackupResponse>
```

- JSON format

{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}

2.8.1.6.2. CloneDBInstance

Description

You can call this operation to clone a new instance with historical data based on the backup file of an existing instance or a specified time.

The new instance will have the same whitelist, SQL audit, alarm threshold, backup, and parameter settings as the existing instance.

The data in the new instance is the same as historical data in the backup file. The clone feature can only be used with MySQL engines.

Database account information is cloned differently for different account types:

- If a privileged account is used as the primary instance, instances that are cloned from it will also carry the same privileged account information.
- If a standard account is used as the primary instance, instances that are cloned from it will also carry the information of the account used when the backup file is generated or at the specified time.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CloneDBInstance.
DBInstanceId	String	Yes	The ID of the instance to be cloned.
BackupId	String	No	The ID of the backup set. You can call the DescribeBackups operation to query backup set IDs.
RestoreTime	String	No	A point in time within the backup retention period to obtain a backup set from. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-06-11T16:00:00Z. Either BackupId or RestoreTime is required.
PayType	String	Yes	The billing method of the instance. Valid values: Postpaid and Prepaid. Postpaid indicates pay-as-you-go and Prepaid indicates subscription.
Period	String	No	The unit of the subscription period. It is required if PayType is set to Prepaid. Valid values: Year and Month.
UsedTime	String	No	The number of the subscription units. It is required if PayType is set to Prepaid. Valid values: positive integers such as 1, 2, and 3.

Parameter	Type	Required	Description
DBInstanceClass	String	No	The specifications of the instance. For more information, see Instance types in Appendix. This parameter is optional. If it is not specified, the new instance is of the same type as the primary instance.
DBInstanceStorage	String	No	The disk space. Unit: GB. This value must be a multiple of 5 GB. RDS instances of the dedicated host type: 3000 to 3000. RDS instances of other types: 5 to 2000.
InstanceNetworkType	String	No	The network type of the instance. Valid values: Classic and VPC. This value is the same as that of the primary instance by default.
VPCId	String	No	The ID of the VPC.
VSwitch ID	String	No	The ID of the VSwitich.
PrivateIpAddress	String	No	The IP address of the VPC under VSwitchId. If no value is specified, the system automatically assigns a VPC IP address.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
DBInstanceId		The ID of the instance cloned.
OrderId		The ID of the order.

2.8.1.6.3. DescribeBackups

Description

You can call this operation to search for a set of instance backups. The set of backups must be in the Success state, indicating that they can be used to restore an instance.

RDS provides backup files for you to download.

- When DownloadLink is NULL, RDS does not provide a download URL.
- When DownloadLink is not NULL, you can use this URL to download the backup file through Wget (with double quotation marks), a browser, or a user program. The expiration time for this URL is specified by LinkExpiredTime. Use it before the expiration time.

  If the BackupSet has expired, the following error code is displayed:

```
<? xml version="1.0" encoding="UTF-8" ? ><Error><Code>AccessDenied</Code><Message>Request has expired. </Message><Expires>2012-12-25T09:47:52.000Z</Expires><ServerTime>2012-12-25T09:49:00.000Z</ServerTime><RequestId>50D9768CA801C2F102005C70</RequestId><HostId>oss-test.aliyun-inc.com</HostId></Error>
```

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeBackups.
DBInstanceId	String	Yes	The ID of the instance for which the backup set is queried.
BackupId	Integer	No	The ID of the backup set.
BackupStatus	String	No	The status of the backup set. Valid values: Success and Failed.
BackupMode	String	No	The backup mode. Valid values: Automated and Manual.
StartTime	String	Yes	The beginning of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-06-11T15:00Z.
EndTime	String	Yes	The end of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-06-11T16:00Z. The end time must be later than the start time.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1 but must be equal to or smaller than the maximum Integer value. Default value: 1.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
TotalRecordCount	Interger	The total number of entries.
PageNumber	Integer	The number of the page returned.
PageRecordCount	Integer	The number of backup sets on the current page.
Items	List<Backup>	The array that consists of Backup data.

2.8.1.6.4. CreateTempDBInstance

Description

Note You can create a temporary instance based on a backup set or a point in time within the past seven days. When a temporary instance is created, accounts and databases inherit the backup set data.

You can call this operation to create a temporary instance. Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The instance is not undergoing any migration tasks.
- The instance is not locked by the system.
- The current status of the instance backup set is Success.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateTempDBInstance.
DBInstanceId	String	Yes	The ID of the instance to be created.
BackupId	Integer	No	The ID of the backup set.
RestoreTime	String	No	The restoration time of the backup set. It can be any time within the past seven days that is more than 30 minutes before the current time. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. The time must be in UTC. Example: 2011-06-11T16:00:00Z.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
TempDBInstanceId	String	The ID of the temporary instance.

Examples

Sample requests

```
https://rds.example.com/?Action=CreateTempDBInstance
&BackupId=90262
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<CreateTempDBInstanceResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<TempDBInstanceId>sub-xxxxx</TempDBInstanceId>
</CreateTempDBInstanceResponse>
```

- JSON format

```
{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC",
"TempDBInstanceId":"sub-xxxxx"}
```

2.8.1.6.5. DescribeBackupPolicy

Description

You can call this operation to query the backup policy configured for the system. RDS periodically backs up an instance based on the user-defined system configuration.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeBackupPolicy.
DBInstanceId	String	Yes	The ID of the instance for which the backup policy is queried.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
BackupRetentionPeriod	String	The data backup retention period. Unit: days. Valid values: 1 to 30.
PreferredBackupTime	String	The backup time. The time is in the HH:mmZ to HH:mmZ format.

Parameter	Type	Description
PreferredBackupPeriod	String	The backup day. Valid values: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.
BackupLog	String	The log backup status. Valid values: Enable and Disabled.
LogBackupRetentionPeriod	String	The log backup retention period. Unit: days. Valid values: 1 to 30.

2.8.1.6.6. ModifyBackupPolicy

Description

You can call this operation to modify a backup policy. RDS periodically backs up instances based on the user-defined system configuration.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyBackupPolicy.
DBInstanceId	String	Yes	The ID of the instance for which the backup policy is modified.
PreferredBackupTime	String	Yes	The backup time. Format: HH:mmZ to HH:mmZ.
PreferredBackupPeriod	String	Yes	The backup day. Valid values: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.
BackupRetentionPeriod	String	No	The data backup retention period. Unit: days. Valid values: 1 to 30. Default value: 7.
BackupLog	String	No	The log backup status. Valid values: Enable and Disabled. Default value: Enable.
LogBackupRetentionPeriod	String	No	The log backup retention period. It cannot exceed BackupRetentionPeriod. Unit: days. Valid values: 1 to 30. When you enable log backup, you can configure the log backup retention period. This operation is only supported on MySQL, PostgreSQL, and PPAS.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=ModifyBackupPolicy
&DBInstanceId=rds-xxxxx
&PreferredBackupTime=00:00Z—01:00Z
&PreferredBackupPeriod=Monday
&<Common request parameters>
```

Sample responses

- XML format

```
<ModifyBackupPolicyResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ModifyBackupPolicyResponse>
```

- JSON format

```
{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.6.7. RestoreDBInstance

Description

You can call this operation to overwrite the contents of an instance and restore a backup set to that instance.

Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The instance is not undergoing any migration tasks.
- The instance is not locked by the system.
- The current status of the instance backup set is Success.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RestoreDBInstance.

Parameter	Type	Required	Description
DBInstanceId	String	Yes	The ID of the instance to which the backup set is restored.
BackupId	Integer	Yes	The ID of the backup set.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=RestoreDBInstance
&BackupId=103312
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<RestoreDBInstanceResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</RestoreDBInstanceResponse>
```

- JSON format

```
{"RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.6.8. DeleteBackup

Description

You can call this operation to delete data backup files that have been stored for longer than seven days or longer than the log backup retention period.

This operation only deletes the specified backup sets for the target instance. It does not delete the backup sets for associated instances, such as read-only, disaster recovery, or cloned instances.

Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.

- This operation is applicable only to MySQL, PostgreSQL, and PPAS instances.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteBackup.
DBInstanceId	String	Yes	The ID of the instance for which data backup files are deleted.
BackupId	String	Yes	The ID of the backup set. Backup set IDs can be obtained through DescribeBackups. You can enter up to 100 backup set IDs in a single request. Separate multiple IDs with commas (,). Only backup sets that are in the Enabled status can be deleted when you call the DescribeBackups operation.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

2.8.1.7. Monitoring management

2.8.1.7.1. DescribeResourceUsage

Description

You can call this operation to query the resource usage information of an instance. When this operation is called, the system returns the amount of space occupied by the specified instance.

DBInstanceId is used to obtain instance resource usage information.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeResourceUsage.
DBInstanceId	String	Yes	The ID of the instance for which the resource usage information is queried.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
DBInstanceId	String	The ID of the instance for which the resource usage information was queried.

Parameter	Type	Description
Engine	String	The type of the database.
DiskUsed	Integer	The total space occupied by both data files and log files. Unit: Byte. -1 indicates no data.
DataSize	Integer	The disk space that is used to store user data. Unit: Byte. -1 indicates no data.
LogSize	Integer	The disk space that is used to store log files. Unit: Byte. -1 indicates no data.
BackupSize	Integer	The total space occupied by backup data. Unit: Byte. -1 indicates no data.
ColdBackupSize	Integer	The total space occupied by cold backup data. Unit: Byte. -1 indicates no data.
SQLSize	Integer	The total space occupied by SQL data. Unit: Byte. -1 indicates no data.

2.8.1.7.2. DescribeDBInstancePerformance

Description

You can call this operation to query the performance metrics of an instance over a specified period of time based on the performance parameters.

There are three output formats based on different query time ranges:

- When the query time range is less than or equal to one day, performance metrics are displayed at one-minute intervals.
- Queries with the time range from one to seven days are not supported.
- When the query time range is greater than seven days but less than or equal to 15 days, performance metrics are displayed at one-hour intervals.
- Queries with the time range greater than 15 days but less than 30 days are not supported.
- When the query time range is greater than or equal to 30 days but less than or equal to one year, performance metrics are displayed at one-day intervals.

> **Note** When the instance space usage key is MySQL_SpaceUsage, performance metric data can be queried only when the time range is less than or equal to one day.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstancePerformance.

Parameter	Type	Required	Description
DBInstanceId	String	Yes	The ID of the instance for which performance metrics are queried.
Key	Integer	Yes	The performance metrics. Separate performance metrics with commas (,). For more information, see Performance parameters.
StartTime	String	Yes	The beginning of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2012-06-11T15:00Z.
EndTime	String	Yes	The end of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2012-06-11T15:00Z.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
DBInstanceId	String	The ID of the instance for which performance metrics were queried.
Engine	String	The type of the database.
StartTime	String	The beginning of the time range where the query was executed. The time is in the yyyy-MM-ddThh:mmZ format. Example: 2011-05-30T03:29Z.
EndTime	String	The end of the time range where the query was executed. The time is in the yyyy-MM-ddThh:mmZ format. Example: 2011-05-30T03:29Z. The end time must be later than the start time.
PerformanceKeys	List<PerformanceKey>	The array that consists of PerformanceKey data. Example: {perf1, perf2, perf3, ...}.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeDBInstancePerformance
&DBInstanceId=rds-xxxxx
&key= MySQL_xxxxx
&StartTime=2013-01-11T15:00:00Z
&EndTime=2013-06-05T15:00:00Z
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeDBInstancePerformanceResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<DBInstanceID>rds-xxxxx</DBInstanceID>
<StartTime>2013-01-11T15:00:00Z</StartTime>
<EndTime>2013-10-17T15:00Z</EndTime>
<Engine>MySQL</Engine>
<PerformanceKeys>
<PerformanceKey>
<Key>MySQL_xxxxx</Key>
<Unit>KB</Unit>
<ValueFormat>recv_k&amp;sent_k</ValueFormat>
<Values><Values/>
</PerformanceKey>
</PerformanceKeys>
</DescribeDBInstancePerformanceResponse>
```

- JSON format

```
{"RequestId" 1e3d5a1e0-67ca-4336624bc-eaf2d5a1e4dc,
"DBInstanceID": rds-xxxxx,
"StartTime": "2012-06-11T15:00Z",
"EndTime": "2013-10-17T15:00Z",
"Engine": "MySQL",
"PerformanceKeys":
  { PerformanceKey[ {
    "Key": "MySQL_xxxxx",
    "Unit": "KB",
    "ValueFormat": "recv_k&sent_k",
    "Values": { "PerformanceValue":[] } } ] }}
```

2.8.1.7.3. DescribeDBInstanceMonitor

Description

You can call this operation to query the monitoring behavior of an instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceMonitor.

Parameter	Type	Required	Description
DBInstanceId	String	Yes	The ID of the instance for which the monitoring behavior is queried.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Period	String	The monitoring period. Unit: seconds.

2.8.1.7.4. ModifyDBInstanceMonitor

Description

You can call this operation to modify the monitoring behavior of an instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceMonitor.
DBInstanceId	String	Yes	The ID of the instance for which the monitoring behavior is modified.
Period	String	Yes	The monitoring period. Unit: seconds. Valid values: 60 and 300. Default value: 300.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

2.8.1.8. Parameter management

2.8.1.8.1. DescribeParameterTemplates

Description

You can call this operation to query the parameter template list. The list includes parameter names, default parameter values, whether they can be modified, whether the database must be restarted for them to take effect, and regular expressions acting as parameter validation rules.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeParameterTemplates.
Engine	String	Yes	The type of the database. Valid value: MySQL.
EngineVersion	String	Yes	The version of the database. MySQL database: 5.6 or 5.7.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Engine	String	The type of the database.
EngineVersion	String	The version of the database.
ParameterCount	Integer	The number of parameters.
Parameters	List<TemplateRecord>	The array that consists of TemplateRecord data. Format: {parameter1, parameter2, parameter3, ...}.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeParameterTemplates
&Engine=MySQL
&EngineVersion=5.6
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeParameterTemplatesResponse>
<Engine>mysql</Engine>
<EngineVersion>5.6</EngineVersion>
<ParameterCount>1</ParameterCount>
<Parameters>
<TemplateRecord>
<CheckingCode>[0-100]</CheckingCode>
<ForceRestart>True</ForceRestart>
<Factor>1</Factor>
<ParameterDescription>test</ParameterDescription>
<ParameterName>fill factor</ParameterName>
<ParameterValue>0</ParameterValue>
<ForceModify>True</ForceModify>
<Unit>INT</Unit>
</TemplateRecord>
</Parameters>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</DescribeParameterTemplatesResponse>
```

- JSON format

```
{"Engine": "mysql",
"EngineVersion": "5.6",
"ParameterCount":1,
"Parameters":
  { "TemplateRecord": [ {
     "ParameterDescription": "test",
     "ForceRestart": "True",
     "CheckingCode": "[0-100]"
     "Factor":"1",
     "ParameterName":"fill factor",
     "ParameterValue":"0",
     "ForceModify":"True",
     "Unit":"INT" } ] },
"RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.8.2. DescribeParameters

Description

You can call this operation to query the current instance parameter configuration.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeParameters.
DBInstanceId	String	Yes	The ID of the instance for which parameters are queried.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Engine	String	The type of the database.
EngineVersion	String	The version of the database.
RunningParameters	List<DBInstanceParameter>	The array that consists of running DBInstanceParameter data. Format: {parameter1,parameter2,parameter3, ...}.
ConfigParameters	List<DBInstanceParameter>	The array that consists of synchronizing DBInstanceParameter data. Format: {parameter1,parameter2,parameter3,...}.

DBInstanceParameter parameters

Parameter	Type	Description
ParameterName	String	The name of the parameter.
ParameterValue	String	The value of the parameter.
ParameterDescription	String	The description of the parameter.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeParameters
&DBInstanceId=rds-xxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeParametersResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<Engine>mysql</Engine >
<EngineVersion>5.6</EngineVersion>
<RunningParameters>
<DBInstanceParameter>
<ParameterDescription>test</ParameterDescription>
<ParameterName>fill factor</ParameterName>
<ParameterValue>0</ParameterValue>
</DBInstanceParameter>
</RunningParameters>
<ConfigParameters>
<DBInstanceParameter>
<ParameterDescription>test1</ParameterDescription>
<ParameterName>fill factor</ParameterName>
<ParameterValue>50</ParameterValue>
</DBInstanceParameter>
</ConfigParameters>
</DescribeParametersResponse>
```

- JSON format

```
{ "ConfigParameters": {
   "DBInstanceParameter": [ {
      "ParameterDescription": "test",
      "ParameterName": "fill factor",
      "ParameterValue": "50" } ] },
   "Engine": "mysql",
   "EngineVersion": "5.6",
   "RunningParameters": {
      "DBInstanceParameter": [ {
         "ParameterDescription": "test1",
         "ParameterName": "fill factor",
         "ParameterValue": "0" } ] },
   "RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.8.3. ModifyParameter

Description

You can call this operation to modify instance parameters. After you submit a request, RDS assigns a task to apply new parameters to the instance. If there are any parameter modifications that require the database to be restarted, RDS restarts the database.

Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The instance is not locked by the system.

There are three types of parameter values:

- 1 to 65,535: indicates a numerical range. Regular identification is used to extract the minimum and maximum values. The input parameter is then verified based on the extracted minimum and maximum values. The parameter must be a multiple of a divisible factor.
- utf8 | gbk | latin1: indicates a set value determination rule. Regular identification is used to extract the fixed value. The input parameter is then verified based on these fixed values.
- Others: These must be implemented with regular expressions.

Before assigning the task, RDS checks the parameter as follows:

1. Whether the parameter exist.
2. Whether the parameter can be modified.
3. Whether the parameter is valid.

   If the parameter is invalid, RDS returns the 400 HTTP status code and information about the invalid parameter. Example:

```
{"HttpStatusCode":400,
"Code":"InvalidParameter.Format",
"Message":"Specified parameter is not valid.[auto_increment_increment:a,character_set_client:41]"}
```

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyParameter.
DBInstanceId	String	Yes	The ID of the instance for which parameters are modified.
Parameters	String	Yes	The JSON string for the parameter and its value. The parameter value must be of the string type. {"auto_increment_increment":"1", "character_set_client":"utf8"}.
Forcerestart	String	No	Specifies whether to forcibly restart the database. Valid values: true and false. If a parameter can take effect only after database restart, Forcerestart must be set to true. Otherwise, the parameter modification will not take effect. Default value: false.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=ModifyeParameter
&DBInstanceId=rds-xxxxx
&Parameters={"key_buffer_size":"456","character_set_client":"gbk"}
&<Common request parameters>
```

Sample responses

- XML format

```
<ModifyeParameterResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</ModifyeParameterResponse>
```

- JSON format

```
{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC",}
```

2.8.1.9. Log management

2.8.1.9.1. DescribeSlowLogs

Description

You can call this operation to query the slow log summary of the databases in a specified instance over a specified period of time.

This operation supports querying by page.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSlowLogs.
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.

Parameter	Type	Required	Description
StartTime	String	Yes	The beginning of the date range where the query is performed. Specify the date in the YYYY-MM-DDZ format. Example: 2011-05-30Z.
EndTime	String	Yes	The end of the date range where the query is performed. The end date must be later than the start date. Specify the date in the YYYY-MM-DDZ format. Example: 2011-05-30Z.
DBName	String	No	The name of the database.
SortKey	String	No	The basis by which query results are sorted. Valid values: TotalExecutionCounts: in the descending order of execution times. TotalQueryTimes: in the descending order of the total execution duration. TotalLogicalReads: in the descending order of the total number of logical reads.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1 but must be equal to or smaller than the maximum Integer value. Default value: 1.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
Engine	String	The type of the database.
StartTime	String	The beginning of the date range where the query is performed. The date is in the YYYY-MM-DDZ format. Example: 2011-05-30Z.
EndTime	String	The end of the date range where the query is performed. The date is in the YYYY-MM-DDZ format. Example: 2011-05-30Z.
TotalRecordCount	Integer	The total number of entries.
PageNumber	Integer	The number of the page returned.

Parameter	Type	Description
PageRecordCount	Integer	The number of SQL slow queries on the current page.
Items	List<SQLSlowLog>	The list of slow log statements.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeSlowLogs
&DBInstanceId=rds-xxxxx
&StartTime=2011-06-11Z
&EndTime=2011-12-11Z
&SortKey= Totaxxxxx
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeSlowLogsResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<DBInstanceID>rds-xxxxx</DBInstanceID>
<Engine>MySQL</Engine>
<StartTime>2011-06-11Z</StartTime>
<EndTime>2011-12-11Z</EndTime>
<TotalRecordCount>1</TotalRecordCount>
<PageNumber>1</PageNumber>
<PageRecordCount>1</PageRecordCount>
<Items>
<SQLSlowLog>
<SQLText>update test.zxb set id=0 limit 1</SQLText>
<MySQLTotalExecutionCounts>178</MySQLTotalExecutionCounts>
<MySQLTotalExecutionTimes>189</MySQLTotalExecutionTimes>
<TotalLogicalReadcounts>89</TotalLogicalReadcounts>
<TotalPhysicalReadcounts>90</TotalPhysicalReadcounts>
<ReportTime>2013-11-12Z</ReportTime>
</SQLSlowLog>
</Items>
</DescribeSlowLogsResponse>
```

- JSON format

```
{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC",
"StartTime":"2011-06-11Z ",
"EndTime":"2011-12-11Z ",
"Engine":"MySQL",
"PageNumber":1,
"PageRecordCount":1,
"TotalRecordCount":  1,
"Items":{
  "SQLSlowLog":[{
    "SQLText":" update test.zxb set id=0 limit 1" ,
    "MySQLTotalExecutionCounts":178,
    "MySQLTotalExecutionTimes":189,
    "TotalLogicalReadcounts":89,
    "TotalPhysicalReadcounts":90,
    "ReportTime":"2013-11-12Z " }]}}
```


2.8.1.9.2. DescribeSlowLogRecords

Description

You can call this operation to query the slow log details of the databases in a specified instance over a specified period of time. This operation is only supported on MySQL instances.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSlowLogRecords.
DBInstanceId	String	Yes	The ID of the instance to which the database belongs.
StartTime	String	Yes	The beginning of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-06-11T15:00Z.
EndTime	String	Yes	The end of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-06-11T16:00Z.
DBName	String	No	The name of the database.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30.

Parameter	Type	Required	Description
PageNumber	Integer	No	The number of the page to return. Pages start from page 1 but must be equal to or smaller than the maximum Integer value. Default value: 1.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
Engine	String	The type of the database.
TotalRecordCount	Integer	The total number of entries.
PageNumber	Integer	The number of the page returned.
PageRecordCount	Integer	The number of SQL slow queries on the current page.
Items	List<SQLSlowRecord>	-

SQLSlowLog parameters

Parameter	Type	Description
HostAddress	String	The host address to connect the database.
DBName	String	The name of the database.
SQLText	String	The query statement.
QueryTimes	Long	The execution time of the slow query. Unit: seconds.
LockTimes	Long	The lock time of the slow query. Unit: seconds.
ParseRowCounts	Long	The number of entries parsed.
ReturnRowCounts	Long	The number of entries returned.
ExecutionStartTime	String	The beginning of the time range where the query was executed. The time is in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-06-11T15:00:08Z.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeSlowLogRecords
&DBInstanceId=rds-xxxxx
&StartTime=2011-06-11T15:00Z
&EndTime=2011-06-11T16:00Z
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeSlowLogRecordsResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<DBInstanceID>rds-xxxxx</DBInstanceID>
<Engine>MySQL</Engine>
<TotalRecordCount>1</TotalRecordCount>
<PageNumber>1</PageNumber>
<PageRecordCount>1</PageRecordCount>
<Items>
<SQLSlowRecord>
<HostAddress>192.168.0.123</HostAddress>
<DBName>test</DBName>
<SQLText>update test.zxb set id=0 limit 1</SQLText>
<QueryTimes>123</QueryTimes>
<LockTimes>12</LockTimes>
<ParseRowCounts>125</ParseRowCounts>
<ReturnRowCounts>1</ReturnRowCounts>
<ExecutionStartTime>2011-06-11T15:00:08Z</ExecutionStartTime>
</SQLSlowRecord>
</Items>
</DescribeSlowLogRecordsResponse>
```

- JSON format

{ "RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC",
"Engine":"MySQL",
"PageNumber":1,
"PageRecordCount":1,
"TotalRecordCount":1,
"Items":{
"SQLSlowRecord":[{
HostAddress:" 192.168.0.123" ,
DBName:" test" ,
SQLText:" update test.zxb set id=0 limit 1" ,
QueryTimes:" 123" ,
LockTimes:" 12" ,
ParseRowCounts:" 125" ,
ReturnRowCounts:" 1" ,
ExecutionStartTime:" 2011-06-11T15:00:08Z" }]}}

2.8.1.9.3. DescribeErrorLogs

Description

You can call this operation to query the error logs generated for an instance over a specified period of time.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeErrorLogs.
DBInstanceId	String	Yes	The ID of the instance for which error logs are queried.
StartTime	String	Yes	The beginning of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-05-30T12:10Z.
EndTime	String	Yes	The end of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-05-30T20:10Z.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1 but must be equal to or smaller than the maximum Integer value. Default value: 1.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
TotalRecordCount	Integer	The total number of entries.
PageNumber	Integer	The number of the page returned.
PageRecordCount	Integer	The number of error logs on the current page.
Items	List<ErrorLogs>	-

ErrorLogs parameters

Parameter	Type	Description
ErrorInfo	String	The error log information.
CreateTime	String	The time when the error log was generated. The time is in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-05-30T12:11:4Z.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeErrorLogs.
&DBInstanceId=rds-xxxxx
&StartTime=2011-06-11T15:00Z
&EndTime=2011-06-11T20:00Z
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeErrorLogsResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<TotalRecordCount>1</TotalRecordCount>
<PageNumber>1</PageNumber>
<PageRecordCount>1<PageRecordCount>
<Items>
<ErrorLog>
<ErrorInfo>spid52 DBCC TRACEON 3499, server process ID (SPID) 52. This is an informational message only; no user action is required</ErrorInfo>
<CreateTime>2013-06-04T15:00:00</CreateTime>
</ErrorLog>
</Items>
</DescribeErrorLogsResponse>
```

- JSON format

```
{"RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC",
"PageNumber":1,
"TotalRecordCount":1,
"PageRecordCount":1,
"Items":{
 "ErrorLog":[{
  ErrorInfo:" spid52 DBCC TRACEON 3499, server process ID (SPID) 52. This is an informational message only; no user action is required" ,
  CreateTime:" 2013-06-04T15:00:00" }]}}
```

2.8.1.9.4. DescribeBinlogFiles

Description

You can call this operation to query binlogs of a MySQL instance. This operation supports querying by page. RDS provides binlog files for you to download.

- When the DownloadLink is NULL, RDS does not provide a download URL.
- When DownloadLink is not NULL, you can use this URL to download the backup file through Wget (with double quotation marks), a browser, or a user program. The expiration time for this URL is specified by LinkExpiredTime. Use it before the expiration time.

  If the BackupSet has expired, the following error code is displayed:

```
<Error>
<Code>AccessDenied</Code>
<Message>Request has expired. </Message>
<Expires>2012-12-25T09:47:52.000Z</Expires>
<ServerTime>2012-12-25T09:49:00.000Z</ServerTime>
<RequestId>50D9768CA801C2F102005C70</RequestId>
<HostId>oss-test.aliyun-inc.com</HostId>
</Error>
```

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeBinlogFiles.
DBInstanceId	String	Yes	The ID of the instance for which binlogs are queried.
StartTime	String	Yes	The beginning of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format.
EndTime	String	Yes	The end of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. The end time must be later than the start time.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1 but must be equal to or smaller than the maximum Integer value. Default value: 1.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
TotalRecordCount	Integer	The total number of binlog files.
PageNumber	Integer	The number of the page returned.
PageRecordCount	Integer	The number of binlog files on the current page.
Items	List<BinLogFile>	-

BinLogFile parameters

Parameter	Type	Description
FileSize	Long	The size of a binlog file. Unit: Byte.
LogBeginTime	String	The beginning of the time range where the binlog was executed.
LogEndTime	String	The end of the time range where the binlog was executed.
DownloadLink	String	The HTTP-compliant download URL. If this parameter is set to NULL, no download URL exists.
HostInstanceID	String	The ID of the instance to which the binlog belongs. This parameter indicates whether the binlog is from the primary or secondary instance.
LinkExpiredTime	String	The URL expiration time. The time is in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-06-11T15:00:00Z.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeBinlogFiles
&DBInstanceId=rds-xxxxx
&StartTime=2011-06-11T15:00:00Z
&EndTime=2013-06-05T15:00:00Z
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeBinlogFilesResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
<TotalRecordCount>1</TotalRecordCount>
<PageNumber>1</PageNumber>
<PageRecordCount>1<PageRecordCount>
<Items>
<BinLogFile>
<FileSize>123</FileSize>
<LogBeginTime>2013-06-01T15:00:00Z</LogBeginTime>
<LogEndTime>2013-06-02T18:00:00Z</LogEndTime>
<DownloadLink>http://rdslog-real.oss.aliyuncs.com/custins47742/hostins46770/mysql-bin. 000120.zip
?spm=0.0.0.0.eMQKjs&OSSAccessKeyId=c9gzsqpauxxxxx&Expires=1384916927&Signature=07TMgM3xxx
xx</DownloadLink>
<LinkExpiredTime>2013-06-09T18:00:00Z</LinkExpiredTime>
</BinLogFile>
</Items>
</DescribeBinlogFilesResponse>
```

- JSON format

```
{ "RequestId":"66816822-CEC1-4C8D-AB26-2530A7D4DCA5",
"PageNumber":1,
"TotalRecordCount":1,
"PageRecordCount":1,
"Items":{
 "BinLogFile":[{
  FileSize:” 123” ,
  LogBeginTime:” 2013-06-01T15:00:00Z” ,
  LogEndTime:” 2013-06-02T18:00:00Z” ,
  DownloadLink:” http://rdslog-real.oss.aliyuncs.com/custinsxxxxx/hostinsxxxxx/mysql-bin. 000120.zi
p?spm=0.0.0.0.eMQKjs&OSSAccessKeyId=c9gzsqpauxxxxx&Expires=1384916927&Signature=07TMgM3xx
xxx” ,
  LinkExpiredTime” 2013-06-09T18:00:00Z” }]}}
```

2.8.1.9.5. DescribeSQLCollectorPolicy

Description

You can call this operation to check whether SQL collection is enabled for a specified RDS instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSQLCollectorPolicy.
DBInstanceId	String	Yes	The ID of the instance for which SQL collection is enabled or disabled.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
SQLCollectorStatus	String	Indicates whether SQL collection is enabled. Valid values: Enable and Disabled.

2.8.1.9.6. ModifySQLCollectorPolicy

Description

You can call this operation to enable or disable SQL collection for the specified RDS instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifySQLCollectorPolicy.
DBInstanceId	String	Yes	The ID of the instance for which SQL collection is enabled or disabled.
SQLCollectorStatus	String	Yes	Specifies whether to enable SQL collection. Valid values: Enable and Disabled.

Response parameters

This operation returns only common response parameters. For more information, see Common response parameters.

2.8.1.9.7. DescribeSQLLogRecords

Description

You can call this operation to query the SQL audit logs generated for an instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSQLLogRecords.
DBInstanceId	String	Yes	The ID of the instance for which SQL audit logs are queried.
Database	String	No	The name of the database. All databases are selected by default.
User	String	No	The name of the user. All users are selected by default.
Form	String	No	The file generation form for audit logs. Valid values: File and Stream. If this parameter is set to File, only common parameters are returned, and you must call the DescribeSQLLogFiles operation to obtain the final download file address. If this parameter is set to Stream, data streams are returned. Default value: Stream.
QueryKeywords	String	No	The keywords used for query. Up to 10 keywords can be entered at a time. Separate multiple keywords with spaces.
StartTime	String	Yes	The beginning of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format.
EndTime	String	Yes	The end of the time range where the query is performed. Specify the time in the yyyy-MM-ddTHH:mm:ssZ format. The end time must be later than the start time.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, 100, and 200. Default value: 100.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1 but must be equal to or smaller than the maximum Integer value. Default value: 1.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
TotalRecordCount	Integer	The total number of entries.
PageNumber	Integer	The number of the page returned.
PageRecordCount	Integer	The number of SQL logs on the current page.
Items	List<SQLRecord>	The array that consists of SQLRecord data.

SQLRecord parameters

Parameter	Type	Description
DBName	String	The name of the database.
AccountName	String	The name of the account.
HostAddress	String	The IP address of the client.
SQLText	String	The SQL statement.
TotalExecutionTimes	Long	The amount of time taken to execute the operation. Unit: microseconds.
ReturnRowCounts	Long	The number of entries returned.
ThreadID	String	The thread ID.
ExecuteTime	String	The execution time. The time is in the yyyy-MM-ddTHH:mm:ssZ format. Example: 2011-05-30T12:11:20Z.

Examples

Sample requests

```
https://rds.example.com/?Action=DescribeSQLLogRecords
&DBInstanceId=rds-xxxxx
&StartTime=2011-06-11T15:00:00Z
&EndTime=2013-06-05T15:00:00Z
&<Common request parameters>
```

Sample responses

- XML format

```
<DescribeSQLLogRecordsResponse>
<PageNumber>1</PageNumber>
  <RequestId>08A3B71B-FE08-4B03-974F-CC7EA6DB1828</RequestId>
  <TotalRecordCounts>1</TotalRecordCounts>
  <SQLItems>
    <SQLItem>
      <ReturnRowCounts>34</ReturnRowCounts>
      <TotalExecutionTimes>12</TotalExecutionTimes>
      <HostAddress>192.168.xx.xx</HostAddress>
      <ExecuteTime>2011-06-11T15:00:23Z</ExecuteTime>
      <SQLText>update test.zxb set id=0 limit 1</SQLText>
      <AccountName>accounttest</AccountName>
      <DBName>test</DBName>
    </SQLItem>
  </SQLItems>
  <ItemsCounts>1</ItemsCounts>
</DescribeSQLLogRecordsResponse>
```

- JSON format

```
{"PageNumber":1,
  "RequestId":"08A3B71B-FE08-4B03-974F-CC7EA6DB1828",
  "TotalRecordCounts":1,
  "SQLItems":{
    "SQLItem":[
      {
        "ReturnRowCounts":34,
        "TotalExecutionTimes":12,
        "HostAddress":"192.168.xx.xx",
        "ExecuteTime":"2011-06-11T15:00:23Z",
        "SQLText":"update test.zxb set id=0 limit 1",
        "AccountName":"accounttest",
        "DBName":"test"
      }
    ]
  },
  "ItemsCounts":1
}
```

2.8.1.9.8. DescribeSQLLogFiles

Description

You can call this operation to query SQL audit files.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSQLLogFiles.
DBInstanceId	String	Yes	The ID of the instance for which SQL audit files are queried.

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
TotalRecordCount	Integer	The total number of entries.
PageNumber	Integer	The number of the page returned.
PageRecordCount	Integer	The number of entries on the current page.
Items	List<LogFile>	The array that consists of audit file data.

LogFile parameters

Parameter	Type	Description
FileID	Integer	The ID of an audit log file.
DBInstanceId	String	The ID of the instance for which SQL audit files were queried.
LogStatus	String	The status of SQL audit files. Valid values: • Success • Failed • Generating
LogStartTime	String	The beginning of the time range where the audit log was executed.
LogEndTime	String	The end of the time range where the audit log was executed.
LogDownloadURL	String	The file download URL. If the download URL is unavailable, this parameter will be empty.
LogSize	Long	The size of an audit log file. Unit: Byte.

2.8.1.10. Data migration

2.8.1.10.1. ImportDatabaseBetweenInstances

Description

You can call this operation to migrate data from one RDS instance to another. This operation is only supported on MySQL instances of the dedicated type.

MySQL instances support batch database migration. During migration, the source instance status changes to Migrating and the destination instance status changes to Importing data.

Database migration is performed between different instances that belong to the same user. Before you call this operation, ensure that the following requirements are met:

- The instance is in the running state.
- The database is in the running state.
- The destination instance is not locked by the system.
- Destination instance storage space > Space occupied by the destination instance - Destination instance database space + Source instance database space.
- Databases to be migrated exist in both the source and destination instances and are activated.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ImportDatabaseBetweenInstances.
DBInstanceId	String	Yes	The ID of the destination instance.
SourceDBInstanceId	String	Yes	The ID of the source instance, which cannot be the same as that of the destination instance.
DBInfo	String	Yes	The database information to be migrated, in the JSON format. For MySQL instances, the parameter value is an array. Example: {"DBNames":["mydb","mydb2"]}. For MySQL instances, the names of the source and destination databases must be the same. In this example, data is migrated from the two databases mydb and mydb2. These databases must exist in both the source and destination instances.

DBInfo parameters

Parameter	Type	Required	Description
DBNames	List	Yes	The names of databases to be migrated. Example: ["mydb","mydb2"].

Response parameters

Parameter	Type	Description
<Common response parameters>		For more information, see Common response parameters.
ImportId	Integer	The ID of the destination instance.

Examples

Sample requests

```
https://rds.example.com/?Action=ImportDatabaseBetweenInstances
&DBInstanceId=rds-xxxxx
&SourceDBInstanceId=rds-xxxxx
&{"DBNames":["mydb","mydb2"]}
&<Common request parameter>
```

Sample responses

- XML format

```
<ImportDatabaseBetweenInstancesResponse>
 <ImportId>2122321</ImportId>
 <RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
 </ImportDatabaseBetweenInstancesResponse>
```

- JSON format

```
{"ImportId":2122321",
 RequestId":"1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC"}
```

2.8.1.10.2. CancelImport

Description

You can call this operation to cancel migration tasks from other RDS instances of the MySQL type.

Migration tasks from MySQL instances can be canceled.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CancelImport.
DBInstanceId	String	Yes	The ID of the instance for which migration tasks are canceled.
ImportId	Integer	Yes	The migration task ID.

Parameter	Type	Required	Description

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Examples

Sample requests

```
https://rds.example.com/?Action=CancelImport
&DBInstanceId=rds-xxxxx
&ImportId=127562
&<Common request parameter>
```

Sample responses

- XML format

```
<CancelImportResponse>
<RequestId>1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC</RequestId>
</CancelImportResponse>
```

- JSON format

```
{"RequestId": "1E3D5A1E0-67CA-43DA-24BC-EAF2D5A1E4DC" }
```

2.8.1.11. Tag management

2.8.1.11.1. AddTagsToResource

Description

You can call this operation to bind existing or newly created tags to instances. Before you call this operation, ensure that the following requirements are met:

Each tag is composed of a TagKey and a TagValue. The TagKey cannot be blank, but the TagValue can.

- The values of TagKey and TagValue cannot start with aliyun.
- The values of TagKey and TagValue are not case sensitive.
- The maximum length of TagKey is 64 characters and the maximum length of TagValue is 128 characters.
- Each instance can only be bound to a maximum of 10 tags. Each tag bound to the same instance

must have a unique TagKey. If tags with duplicate TagKeys are bound to the same instance, the tag bound last overwrites the existing tag.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to AddTagsToResource.
RegionId	String	Yes	The region ID of the instance for which a tag is be bound.
DBInstanceId	String	Yes	The ID of the instance for which a tag is be bound. Up to 30 IDs can be entered in a single request. Separate multiple IDs with commas (,) Format: instance1,instance2,instance3.
Tags	JSON string	Yes	The tag pair to be bound. This parameter must include a TagKey, but does not need to include a corresponding TagValue. Up to five tag pairs can be entered in a single request. The TagKey is required, and TagValue is optional. Format: { “key1” :” value1” , “key2” :” ” }.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

2.8.1.11.2. DescribeTags

Description

You can call this operation to view the bound tag information of an RDS instance belonging to the current account. This operation must meet the following requirements:

If a specified instance ID is provided, all tags bound to this instance are queried and the other filter criteria are ignored.

- If the TagKey of a key is provided without a TagValue, the results of all tags matching the TagKey criteria are returned.
- If both TagKey and TagValue are provided, only the results that match both parameters are returned.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeTags.
RegionId	String	Yes	The region ID of the instance.
DBInstanceId	String	No	The name of the instance. If this parameter is provided, all the other filter criteria are ignored.
Tags	Json string	No	The tag pair. This parameter must include a TagKey, but does not need to include a corresponding TagValue. The TagKey cannot be blank, but the TagValue can. Format: {"key1":"value1 "}.

Response parameters

Name	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Items	List<TagInfos>	The array that consists of tag data.

TagInfos parameters

Name	Type	Description
TagKey	String	The TagKey.
TagValue	String	The TagValue.
DBInstanceIds	List<DBInstanceId>	The IDs of instances bound to this tag.

DBInstanceIds parameters

Name	Type	Description
DBInstanceId	String	The name of the instance.

2.8.1.11.3. RemoveTagsFromResource

Description

You can call this operation to unbind tags from an instance. This operation must meet the following requirements:

A maximum of 10 tags can be unbound in a single request.

If a tag is unbound from all of its bound instances, the tag itself is automatically deleted.

If the TagKey of a key is provided without a TagValue, all tags matching the TagKey criteria are unbound.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RemoveTagsFromResource.
RegionId	String	Yes	The region ID of the instance.
DBInstanceId	String	Yes	The name of the instance.
Tags	Json string	Yes	The tag pair to be unbound. This parameter must include a TagKey, but does not need to include a corresponding TagValue. The TagKey cannot be blank, but the TagValue can. Format: {"key1":"value1 "}.

Response parameters

Name	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

2.8.1.12. RAM authorization

Use RAM for RDS resource authorization

All RDS instances created through an Apsara Stack tenant account are resources owned by that account. Apsara Stack tenant accounts have full operation permissions on their own resources by default.

Resource Access Management (RAM) allows you to grant RAM users the access and management permissions on RDS resources owned by an Apsara Stack tenant account.

If you do not need to use RAM, ignore this topic.

Resource types in RAM

The only type of RDS resources that can be authorized through RAM is dbinstance. The following table lists the resource description method when the resources are authorized through RAM.

Resource type	Resource description in authorization policy
Instance	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid acs:rds:$regionid:$accountid:dbinstance/ *acs:rds::dbinstance/*

All $regionids must be the ID of a region or an asterisk (*). All $instanceids must be the ID of an instance or an asterisk (*). Similarly, $account-id is the numerical ID of your Apsara Stack tenant account, which can be replaced by an asterisk (*).

Authorization actions in RAM

In RAM, the following actions can be authorized to an RDS resource.

Action1	Action2
CreateDBInstance	ModifyDBInstanceSpec
DeleteDBInstance	CreateReadonlyDBInstance
DescribeDBInstances	DescribeDBInstanceAttribute
SwitchDBInstanceNetType	RestartDBInstance
ModifyDBInstanceDescription	ModifySecurityIps
ModifyDBInstanceMaintainTime	UpgradeDBInstanceEngineVersion
PurgeDBInstanceLog	CreateDatabase
DeleteDatabase	DescribeDatabases
ModifyDBDescription	ModifyeParameter
DescribeParameters	DescribeOptimizeAdviceByDBA
DescribeOptimizeAdviceOnMissIndex	ImportDataBaseBetweenInstances
CancelImport	CreateAccount
ResetAccountPassword	GrantAccountPrivilege
RevokeAccountPrivilege	DescribeAccounts
DeleteAccount	ModifyAccountDescription
CreateBackup	DescribeBackups
CreateTempDBInstance	DescribeBackupPolicy
ModifyBackupPolicy	DescribeResourceUsage
DescribeDBInstancePerformance	DescribeSlowLogs
DescribeSlowLogRecords	DescribeErrorLogs
DescribeBinlogFiles	DescribeSQLLogReports
DescribeSQLLogRecords	DescribeOptimizeAdviceOnStorage
DescribeOptimizeAdviceOnMissPK	DescribeOptimizeAdviceOnExcessIndex

Note All APIs except DescribeRegions and DescribeParameterTemplates can be authorized.

RAM authentication rules of APIs

When a RAM user accesses resources through an API, the RDS back end checks the permissions of the caller on RAM to ensure they are authorized to access the resources. Each API determines the resources to undergo permission checks by determining the resources mentioned in the API statement. The following table lists the authentication rules for each API.

Action	Authentication rule
CreateDBInstance	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DeleteDBInstance	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeDBInstances	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
SwitchDBInstanceNetType	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyDBInstanceDescription	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyDBInstanceMaintainTime	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
PurgeDBInstanceLog	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DeleteDatabase	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyDBDescription	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
CancelImport	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ResetAccountPassword	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
RevokeAccountPrivilege	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DeleteAccount	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
CreateBackup	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
CreateTempDBInstance	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyBackupPolicy	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeDBInstancePerformance	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeSlowLogRecords	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeBinlogFiles	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeSQLLogRecords	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeOptimizeAdviceOnMissPK	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid

Action	Authentication rule
DescribeOptimizeAdviceOnMissIndex	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeParameters	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
CreatePrepaidDBInstanceForChannel	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyPrepaidDBInstanceSpec	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
CreatePostpaidDBInstanceForChannel	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyPostpaidDBInstanceSpec	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeDBInstanceAttribute	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
RestartDBInstance	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ModifySecurityIps	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
UpgradeDBInstanceEngineVersion	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
CreateDatabase	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeDatabases	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ImportDataBaseBetweenInstances	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
CreateAccount	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
GrantAccountPrivilege	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeAccounts	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyAccountDescription	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeBackups	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeBackupPolicy	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeResourceUsage	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeSlowLogs	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeErrorLogs	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeSQLLogReports	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeOptimizeAdviceOnStorage	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeOptimizeAdviceOnExcessIndex	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeOptimizeAdviceByDBA	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyeParameter	acs:rds:$regionid:$accountid:dbinstance/$dbinstanceid

2.8.1.13. Appendix

2.8.1.13.1. Error codes on the client

2.8.1.13.1.1. Common errors

Error code	Error message	HTTP status code
MissingParameter	The input parameter "parameter name" that is mandatory for processing this request is not supplied.	400
InvalidParameter	The specified parameter "Action or Version" is not valid.	400
InvalidAccessKeyId.NotFound	The Access Key ID provided does not exist in our records.	404
IncompleteSignature	The request signature does not conform to Aliyun standards.	400
IllegalTimestamp	The input parameter "Timestamp" that is mandatory for processing this request is not supplied.	400
InvalidOwnerId	The specified OwnerId is not valid.	400
InvalidOwnerAccount	The specified OwnerAccount is not valid.	400
InvalidOwner	OwnerId and OwnerAccount can't be used at one API access.	400
Throttling	Request was denied due to request throttling.	400
InvalidAction	The specified action is not valid.	403
ActionUnauthorized	The specified action is not available for you	403
UnsupportedHTTPMethod	This http method not supported.	403
UnsupportedParameter	The parameter "<parameter name>" is not supported.	400
Forbidden.InstanceNotFound	The specified Instance is not found.	404
Forbidden.RAM	User not authorized to operate on the specified resource, or this API doesn't support RAM.	403
Forbedden.NotSupportRAM	This action does not support accessed by RAM mode.	403
Forbidden.RiskControl	This operation is forbidden by Aliyun Risk Control system.	403
InsufficientBalance	Your account does not have enough balance.	400

Error code	Error message	HTTP status code
Forbidden.Authentication	This operation is forbidden by Aliyun Realname Authentication system.	403
Invalid<parameter name>. ValueNotSupported	The specified parameter “parameter name” is not valid.	400
Invalid<parameter name>. Malformed	The specified parameter "parameter name n" is not valid.	400
InvalidParameter	The specified parameter " parameter name n " is not valid.	400

2.8.1.13.1.2. Specific errors

Error code	Error message	HTTP status code
InvalidRegionId.NotFound	The DBInstanceId provided does not exist in our records.	404
InvalidSecurityIPList.Duplicate	The Security IP address is not in the available range or occupied.	400
InvalidSecurityIPListLength.Malformed	The quota of security ip exceeds.	400
InvalidEngineVersionInRegion.NotAvailable	The EngineVersion in the Region is not available.	403
InvaildEngineInRegion.NotAvailable	The Engine in the Region is not available.	403
InvaildDBInstanceClassInRegion.NotAvailable	The DBInstanceClass in the Region is not available.	403
OperationDenied	The resource is out of usage.	403
RegionUnauthorized	There is no authority to create instance in the specified region.	403
QuotaExceeded.CreateInstance	The quota of create instance exceeds.	403
InvalidDBInstanceId.NotFound	The DBInstanceId provided does not exist in our records.	404
MissingParameter	The input parameters "DBInstanceClass" and "DBInstanceStorage" all blank or no change.	400
OperationDenied.DBInstanceType	The operation is not permitted due to type of instance.	400

Error code	Error message	HTTP status code
OperationDenied.DBInstanceStorageReduce	The operation is not permitted due to reduce storage.	403
OperationDenied.DBInstanceStatus	The operation is not permitted due to instance status.	403
DependencyViolation	The operation is not permitted due to instance mount read only or guard instance.	403
InvalidConnectionStringPrefix.Duplicate	The connection string is not in the available range or occupied.	400
QuotaExceeded.SwitchTime	The quota of switch time exceed.	400
OperationDenied.LockMode	The operation is not permitted due to lock of instance.	403
InvalidSecurityIps.Duplicate	The quota of security ip exceeds.	400
OperationDenied.CurrentEngineVersion	The operation is not permitted due to specified current version.	400
OperationDenied.ReadOnlyDBInstanceLower	The operation is not permitted due to higher read only instance version.	403
OperationDenied.GuardDBInstanceLower	The operation is not permitted due to higher guard instance version.	403
OperationDenied.MasterDBInstanceState	The operation is not permitted due to status of master instance.	403
QuotaExceeded.DBName	The quota of db exceeds.	400
InvalidDBName.Duplicate	The Security db Name is not in the available range or occupied.	400
InvalidParameter.Keyword	The specified parameter "DBName" is keyword	400
OperationDenied.DBStatus	The operation is not permitted due to status of database.	403
OperationDenied.DBInstanceEngine	The operation is not permitted due to engine of instance.	403
FTPServiceUnavailable	The request has failed due to a temporary failure of the FTP server.	403
QuotaExceeded.Upload	The quota of file exceeds.	403
InvalidFileName.NotCompleted	The specified "FileName" is not completed.	404

Error code	Error message	HTTP status code
InvalidFileName.NotAvailable	The specified "FileName" is not Available.	404
QuotaExceeded.FileSize	The quota of file size exceeds.	403
QuotaExceeded.DBInstanceStorage	The quota of instance storage exceeds.	403
InvalidDBInfo.Malformed	The specified parameter "DBInfo" is not valid or db not exist.	400
OperationDenied.Region	The operation is not permitted due to different region.	403
OperationDenied.Engine	The operation is not permitted due to different engine.	403
OperationDenied.DBInstanceId	The operation is not permitted due to DBInstanceId and SourceDBInstanceId is same.	403
InvalidTaskId.NotFound	The ImportId provided does not exist in our records.	400
OperationDenied.IncorrectTaskStatus	The operation is not permitted due to status of import.	403
InvalidAccountName.keyword	The specified parameter "AccountName" is a keyword.	400
InvalidAccountName.Duplicate	The Security db Name is not in the available range or occupied.	400
QuotaExceeded.AccountName	The quota of account exceeds.	403
OperationDenied.AccountStatus	The operation is not permitted due to status of account.	403
InvalidDBName.NotFound	The DBName provided does not exist in our records.	404
OperationDenied.AccountType	The operation is not permitted due to type of account.	403
OperationDenied.BackupJobExists	The operation is not permitted due to backup job exist.	403
OperationDenied.NoDatabase	The operation is not permitted due to no database.	403
InvalidStartTimeAndEndTime.Malformed	The end time must be greater than the start time	400

Error code	Error message	HTTP status code
OperationDenied.BackupJobExists	The operation is not permitted due to backup job exist.	403
InvalidBackupId.NotFound	The BackupId provided does not exist in our records.	404
OperationDenied.NotFoundBackup	The operation is not permitted due to no backup.	403
OperationDenied.BackupStatus	The operation is not permitted due to type of backup.	403
OperationDenied.BackupMethod	The operation is not permitted method of backup.	403
OperationDenied.TempDBInstanceExists	The operation is not permitted due to temp instance exist.	403
Forbidden.Authentication	The operation is forbidden by Aliyun Realname Authentication System.	403
IncorrectDBInstanceConnType	Current DB instance conn type does not support this operation.	404
IncorrecttVpcId.Mismatch	The specified parameter "VpcId" is not valid.	400
IntranetNetTypeNotExists	Current DB instance net type does not support this operation.	404
InvalidDBInstanceName.NotFound	The DBInstanceId provided does not exist in our records.	403
InvalidConnectionMode.ValueNotSupported	The specified parameter "ConnectionMode" is not valid.	400
InvalidConnectionString.DuplicateSpecified	connection string already exists in the Aliyun RDS.	403
InvalidConnectionString.DuplicateSpecified	connection string or port want to be modified is the same with current net type.	400
InvalidConnectionStringPrefix.Duplicated	Specified connection string already exists in the Aliyun RDS.	403
InvalidCurrentConnectionString.NotFound	Specified current connection string doesn't exist.	400
InvalidDBInstanceId.NotFound	The DBInstanceId provided does not exist in our records.	400
InvalidDBInstanceId.QuotaExceeded	The quota of instance id exceeds.	400

Error code	Error message	HTTP status code
InvalidDBInstanceNetType.NotFound	The Specified DB instance net type is not found.	404
InvalidDBinstanceNetType.ValueNotSupport	The specified parameter "DBinstanceNetType" is not valid.	400
InvalidDBInstanceType.ValueNotSupport	The specified parameter "DBInstanceType" is not valid.	400
InvalidEngineVersion.Malformed	The specified parameter "EngineVersion" is not valid.	400
InvalidInstanceNetworkType.ValueNotSupported	The specified parameter "InstanceNetworkType" is not valid.	400
InvalidParameter	The specified parameter "dbInstanceId" is not valid.	400
InvalidPort.Malformed	Specified port is not valid.	400
InvalidPrivateIpAddress.Duplicated	Specified private IP address is duplicated.	400
InvalidPrivateIpAddress.Mismatch	Specified private IP address is not in the CIDR block of virtual switch.	400
InvalidVPCId.NotFound	Specified virtual vpc is not found.	400
InvalidVSwitchId.Mismatch	Specified instance and virtual switch are not in the same zone.	400
InvalidVSwitchId.NotFound	Specified virtual switch is not found in specified VPC.	400
NetTypeExists	Specified net type already existed.	400
NetTypeExists	Specified public net type already existed.	403
OperationDenied.DBInstanceNetType	The operation is not permitted due to net type of instance.	403
OperationDenied.DBInstanceStatus	The operation is not permitted due to status of instance.	403
OperationDenied.DBInstanceType	The operation is not permitted due to type of instance.	403
OperationDenied.LockMode	The operation is not permitted due to lock of instance.	403
OperationDenied.Switch	Specified instance cannot be switched.	400
OperationDenied.Switch	Specified instance cannot be switched to VPC.	403

Error code	Error message	HTTP status code
OperationDenied.SwitchToVPC	Specified instance cannot be switched to VPC.	403
OperationDenied	The resource is out of usage.	403
OperationDenied	The vpc cloudinstanceIp is use, please check params.	406
OperationDenied	The vpc service is error, please check params.	400
PARAMETER_ERROR	The vpc request parameter may not be null.	406
PARAMETER_MUST_NOT_NULL	The parameter must not be null.	406
PublicConnectionExists	PublicConnection exists.	403
bpcIzNoNotEqualsRdsMultIzNo	Specified vpc IzNo not equal rds IzNo.	400
OperationDenied.DBInstanceStatus	The operation is not permitted due to status of instance.	403
OperationDenied.DBInstanceType	The operation is not permitted due to type of instance.	403
OperationDenied.LockMode	The operation is not permitted due to lock of instance.	403
OperationDenied.Switch	Specified instance cannot be switched.	400
OperationDenied.SwitchToVPC	Specified instance cannot be switched to VPC.	403
OperationDenied	The resource is out of usage.	403
OperationDenied	The vpc cloudinstanceIp is use, please check params.	406
OperationDenied	The vpc service is error, please check params.	400
PARAMETER_ERROR	The vpc request parameter may not be null.	406
PARAMETER_MUST_NOT_NULL	The parameter must not be null.	406
PublicConnectionExists	PublicConnection exists.	403
bpcIzNoNotEqualsRdsMultIzNo	Specified vpc IzNo not equal rds IzNo.	400

2.8.1.13.2. Error codes on the server

Error code	Error message	HTTP status code
ServiceUnavailable	The request has failed due to a temporary failure of the server.	503
InternalError	The request processing has failed due to some unknown error, exception or failure.	500

2.8.1.13.3. Instance states

State	Description
Creating	An instance is being created.
Running	An instance is in the running state.
Deleting	An instance is being deleted.
Rebooting	An instance is being restarted.
DBInstanceClassChanging	An instance is being upgraded or downgraded.
TRANSING	Data is being migrated.
EngineVersionUpgrading	Engine version is being upgraded.
TransingToOthers	Data is being migrated to other RDS instances.
GuardDBInstanceCreating	A disaster recovery instance is being created.
Restoring	A backup is being restored.
Importing	Data is being imported.
ImportingFromOthers	Data is being imported from other RDS instances.
DBInstanceNetTypeChanging	The network type is being switched between Intranet and Internet.
GuardSwitching	The instance is undergoing disaster recover failover.
INS_CLONING	The instance is being cloned.

2.8.1.13.4. Performance parameters

ApsaraDB RDS for MySQL

API parameter	Description
MySQL_NetworkTraffic	The average inbound traffic to a MySQL instance per second and average outbound traffic from a MySQL instance per second. Unit: KB.
MySQL_QPSTPS	The average number of SQL statements executed per second and average number of transactions per second.
MySQL_Sessions	The number of active connections and total number of current connections.
MySQL_InnoDBBufferRatio	The read hit rate of the InnoDB buffer pool, utilization of the InnoDB buffer pool, and percentage of dirty data blocks in the InnoDB buffer pool.
MySQL_InnoDBDataReadWriten	The average volume of data that InnoDB reads per second and average volume of data that InnoDB writes per second. Unit: KB.
MySQL_InnoDBLogRequests	The average number of read operations performed from the InnoDB buffer pool per second and average number of write operations performed on the InnoDB buffer pool per second.
MySQL_InnoDBLogWrites	The average number of log write requests per second, average number of physical writes performed on log files per second, and average number of fsync() writes completed on log files per second.
MySQL_TempDiskTableCreates	The number of temporary tables automatically created in the hard drive during MySQL statement execution.
MySQL_MyISAMKeyBufferRatio	The average Key Buffer utilization of MyISAM per second, average Key Buffer read hit rate of MyISAM per second, and average Key Buffer write hit rate of MyISAM per second.
MySQL_MyISAMKeyReadWrites	The average number of data reads from the buffer pool by MyISAM per second, average number of data writes to the buffer pool by MyISAM per second, average number of data reads from the hard disk by MyISAM per second, and average number of data writes to the hard disk by MyISAM per second.
MySQL_COMDML	The average number of DELETE statements executed per second, average number of INSERT statements executed per second, average number of INSERT_SELECT statements execute per second, average number of REPLACE statements executed per second, average number of REPLACE_SELECT statements executed per second, average number of SELECT statements executed per second, and average number of UPDATE statements executed per second.
MySQL_RowDML	The average number of rows read from the InnoDB table per second, average number of rows updated in the InnoDB table per second, average number of rows deleted from the InnoDB table per second, average number of rows inserted into the InnoDB table per second, and average number of physical writes to log files per second.
MySQL_MemCpuUsage	The CPU utilization and memory usage of a MySQL Instance within the entire operating system.

API parameter	Description
MySQL_IOPS	The IOPS of a MySQL instance.
MySQL_DetailedSpaceUsage	The disk space occupied by a MySQL instance, including ins_size (total space), data_size (data space), log_size (log space), tmp_size (temporary space), and other_size (system space).
slavestat	The latency of read-only instances.

2.8.1.13.5. Forbidden keywords

RDS for MySQL

Parameter field	Keyword description
DBName/ AccountName	admin, aurora, replicator, xtrabak, root(MySQL5.5/5.6), mysql, test, eagleye, information_schema, guest, add, analyze, asc, between, blob, call, change, check, condition, continue, cross, current_timestamp, database, day_microsecond, dec, default, desc, distinct, double, each, enclosed, exit, fetch, float8, foreign, goto, having, hour_minute, ignore, infile, insensitive, int1, int4, interval, iterate, keys, leading, like, lines, localtimestamp, longblob, low_priority, mediumint, minute_microsecond, modifies, no_write_to_binlog, on, optionally, out, precision, purge, read, references, rename, require, revoke, schema, select, set, spatial, sqlexception, sql_big_result, ssl, table, tinyblob, to, true, unique, update, using, utc_timestamp, varchar, when, with, xor, all, and, asensitive, bigint, both, cascade, char, collate, connection, convert, current_date, current_user, databases, day_minute, decimal, delayed, describe, distinctrow, drop, else, escaped, explain, float, for, from, grant, high_priority, hour_second, in, inner, insert, int2, int8, into, join, kill, leave, limit, load, lock, longtext, match, mediumtext, minute_second, natural, null, optimize, or, outer, primary, raid0, reads, regexp, repeat, restrict, right, schemas, sensitive, show, specific, sqlstate, sql_calc_found_rows, starting, terminated, tinyint, trailing, undo, unlock, usage, utc_date, values, varcharacter, where, write, year_month, alter, as, before, binary, by, case, character, column, constraint, create, current_time, cursor, day_hour, day_second, declare, delete, deterministic, div, dual, elseif, exists, false, float4, force, fulltext, group, hour_microsecond, if, index, inout, int, int3, integer, is, key, label, left, linear, localtime, long, loop, mediumblob, middleint, mod, not, numeric, option, order, outfile, procedure, range, real, release, replace, return, rlike, second_microsecond, separator, smallint, sql, sqlwarning, sql_small_result, straight_join, then, tinytext, trigger, union, unsigned, use, utc_time, varbinary, varying, while, x509, zerofill, galaxy

2.8.1.13.6. Instance types

Instances of different editions, versions, and types each perform differently from one another.

ApsaraDB RDS for MySQL instance types

Edition	Version	Instance family	Instance type	CPU and memory	Maximum connections	Maximum IOPS	Disk capacity	Zone-disaster recovery deployment
High-availability Edition	5.6 or 5.7	Dedicated instance (X8)	mysql.x8.medium.2	2 cores, 16 GB	2,500	4,500	250 GB	Single-data center deployment Dual-data center deployment
			mysql.x8.large.2	4 cores, 32 GB	5,000	9,000	500 GB	
			mysql.x8.xlarge.2	8 cores, 64 GB	10,000	18,000	1 TB	
			mysql.x8.2xlarge.2	16 cores, 128 GB	20,000	36,000	2 TB	
		Dedicated instance (X4)	mysql.x4.large.2	4 cores, 16 GB	2,500	4,500	250 GB	
			mysql.x4.xlarge.2	8 cores, 32 GB	5,000	9,000	500 GB	
			mysql.x4.2xlarge.2	16 cores, 64 GB	10,000	18,000	1 TB	
			mysql.x4.4xlarge.2	32 cores, 128 GB	20,000	36,000	2 TB	
		Dedicated host	rds.mysql.st.d13	30 cores, 220 GB	64,000	20,000	3 TB	
MySQL Finance Edition (three-node)	5.6	Dedicated instance (high memory)	mysql.x8.medium.4	2 cores, 16 GB	2,500	4,500	250 GB	Dual-data center deployment
			mysql.x8.large.4	4 cores, 32 GB	5,000	9,000	500 GB	
			mysql.x8.xlarge.4	8 cores, 64 GB	10,000	18,000	1 TB	
			mysql.x8.2xlarge.4	16 cores, 128 GB	20,000	36,000	2 TB	
			mysql.x8.4xlarge.4	32 cores, 256 GB	40,000	72,000	3 TB	

Edition	Version	Instance family	Instance type	CPU and memory	Maximum connections	Maximum IOPS	Disk capacity	Zone-disaster recovery deployment
Read-only instance	5.6 or 5.7	Dedicated instance (X8)	mysqlro.x8.medium.1	2 cores, 16 GB	2,500	4,500	250 GB	Single-data center deployment Dual-data center deployment
			mysqlro.x8.large.1	4 cores, 32 GB	5,000	9,000	500 GB	
			mysqlro.x8.xlarge.1	8 cores, 64 GB	10,000	18,000	1 TB	
			mysqlro.x8.2xlarge.1	16 cores, 128 GB	20,000	36,000	2 TB	
		Dedicated instance (X4)	mysqlro.x4.large.1	4 cores, 16 GB	2,500	4,500	250 GB	
			mysqlro.x4.xlarge.1	8 cores, 32 GB	5,000	9,000	500 GB	
			mysqlro.x4.2xlarge.1	16 cores, 64 GB	10,000	18,000	1 TB	
			mysqlro.x4.4xlarge.1	32 cores, 128 GB	20,000	36,000	2 TB	
		Dedicated host	rds.mysql.st.d13	30 cores, 220 GB	64,000	20,000	3 TB	

ApsaraDB RDS for PostgreSQL instance types

Edition	Version	Instance family	Instance type	CPU and memory	Maximum connections	Maximum IOPS	Disk capacity	Zone-disaster recovery deployment

Edition	Version	Instance family	Instance type	CPU and memory	Maximum connections	Maximum IOPS	Disk capacity	Zone-disaster recovery deployment
High-availability Edition	9.4	Dedicated instance (high memory)	pg.x8.medium.2	2 cores, 16 GB	2,500	4,500	250 GB	Single-data center deployment Dual-data center deployment
			pg.x8.large.2	4 cores, 32 GB	5,000	9,000	500 GB	
			pg.x8.xlarge.2	8 cores, 64 GB	10,000	18,000	1 TB	
			pg.x8.2xlarge.2	16 cores, 128 GB	12,000	36,000	2 TB	
		Dedicated instance (high CPU)	pg.x4.large.2	4 cores, 16 GB	2,500	4,500	250 GB or 500 GB	
			pg.x4.xlarge.2	8 cores, 32 GB	5,000	9,000	500 GB or 1 TB	
			pg.x4.2xlarge.2	16 cores, 64 GB	10,000	18,000	1 TB or 2 TB	
			pg.x4.4xlarge.2	32 cores, 128 GB	12,000	36,000	2 TB or 3 TB	
		Dedicated host	rds.pg.st.d13	30 cores, 220 GB	4,000	20,000	3 TB	

ApsaraDB RDS for PPAS instance types

Edition	Version	Instance family	Instance type	CPU and memory	Maximum connections	Maximum IOPS	Disk capacity	Zone-disaster recovery deployment

Edition	Version	Instance family	Instance type	CPU and memory	Maximum connections	Maximum IOPS	Disk capacity	Zone-disaster recovery deployment
High-availability Edition	9.3 or 9.6	Dedicated instance	ppas.x4.small.2	1 core, 4 GB	200	5,000	250 GB	Single-data center deployment Dual-data center deployment
			ppas.x4.medium.2	2 cores, 8 GB	400	10,000	250 GB	
			ppas.x8.medium.2	2 cores, 16 GB	2,500	15,000	250 GB	
			ppas.x4.large.2	4 cores, 16 GB	2,500	20,000	250 GB or 500 GB	
			ppas.x8.large.2	4 cores, 32 GB	5,000	30,000	250 GB or 500 GB	
			ppas.x4.xlarge.2	8 cores, 32 GB	5,000	40,000	500 GB or 1 TB	
			ppas.x8.xlarge.2	8 cores, 64 GB	10,000	60,000	500 GB or 1 TB	
			ppas.x4.2xlarge.2	16 cores, 64 GB	10,000	80,000	1 TB or 2 TB	
			ppas.x8.2xlarge.2	16 cores, 128 GB	12,000	120,000	1 TB or 2 TB	
			ppas.x4.4xlarge.2	32 cores, 128 GB	12,000	160,000	2 TB or 3 TB	
			ppas.x8.4xlarge.2	32 cores, 256 GB	12,000	240,000	2 TB or 3 TB	
		Dedicated host	rds.ppas.st.d13	30 cores, 220 GB	4,000	20,000	3 TB	

2.8.2. SDK reference

2.8.2.1. Java SDK

2.8.2.1.1. Quick start

This topic describes how to obtain and use the RDS Java SDK.

Prerequisites

- You must have a RAM user account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the Java SDK. For more information about how to view and obtain your AccessKey pair in the Apsara Stack Operations console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.
- Apsara Stack Java SDK supports JDK 1.6 and later.

Install the Java SDK

If you use Apache Maven to manage Java projects, you only need to import the JAR file to the *pom.xml* file of the project.

To use the SDK of a service, you must install the service SDK and the SDK core library.

The SDK core library is V3.7.1. The SDK is *V2.1.4*.

```
<dependencies>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-sdk-core</artifactId>
      <version>3.7.1</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-core-3.7.1.jar</systemPath>
    </dependency>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-rds</artifactId>
      <version>2.1.4</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-rds-2.1.4.jar</systemPath>
    </dependency>
  </dependencies>
```

Use the Java SDK

To call the Java SDK, perform the following operations:

1. Create a DefaultAcsClient instance and initialize it.
2. Create an API request and configure its parameters.
3. Initiate the request and handle its response or exception.

```
package com.testprogram;
 import com.aliyuncs.profile.DefaultProfile;
 import com.aliyuncs.DefaultAcsClient;
 import com.aliyuncs.IAcsClient;
 import com.aliyuncs.exceptions.ClientException;
 import com.aliyuncs.exceptions.ServerException;
 import com.aliyuncs.ecs.model.v20140526.*;
 public class Main {
    public static void main(String[] args) {
       // Create a DefaultAcsClient instance and initialize it.
       DefaultProfile profile = DefaultProfile.getProfile(
          "<your-region-id>",         // Your region ID.
          "<your-access-key-id>",     // Your AccessKey ID.
          "<your-access-key-secret>"); // Your AccessKey Secret.
       // Set the endpoint of the current service.
      profile.addEndpoint("your-region-id", "your-region-id", "product", "endpoint");
       IAcsClient client = new DefaultAcsClient(profile);
       // Create an API request and configure its parameters.
       DescribeInstancesRequest request = new DescribeInstancesRequest();
       request.setPageSize(10);
       // Initiate the request and handle the response or exception.
       DescribeInstancesResponse response;
       try {
          response = client.getAcsResponse(request);
          for (DescribeInstancesResponse.Instance instance:response.getInstances()) {
             System.out.println(instance.getPublicIpAddress());
          }
       } catch (ServerException e) {
          e.printStackTrace();
       } catch (ClientException e) {
          e.printStackTrace();
       }
    }
 } Enter your actual service information
```

2.8.2.1.2. Use the SDK

2.8.2.1.2.1. Install the Java SDK

This topic describes how to install and use the RDS Java SDK.

The RDS Java SDK supports JDK 1.6 and later. You can import the JAR file to install the JDK.

You can click Here to download the JAR file for VPC.

You can import the JAR file to install the VPC Java SDK regardless of the IDE (Eclipse or IntelliJ).

The installation method is as follows:

- Use Eclipse

  To install the RDS Java SDK in an Eclipse project, perform the following operations:

  i. Copy the downloaded `aliyun-java-sdk-rds.jar` file to your project folder.

  ii. Open your project in Eclipse, right-click the project, and choose **Properties** from the shortcut menu.

  iii. In the dialog box that appears, choose **Java Build Path** > **Libraries** > **Add JARs** to add the downloaded JAR file.

  iv. Click **Apply and Close**.

- Use IntelliJ

  To install the RDS Java SDK in an IntelliJ project, perform the following operations:

  i. Copy the downloaded `aliyun-java-sdk-rds.jar` file to your project folder.

  ii. Open your project in IntelliJ. In the menu bar, choose **File** > **Project Structure**.

  iii. Click **Apply**, and then **OK**.

2.8.2.1.2.2. Configure identity verification credentials

When using SDKs to access Apsara Stack services, you must provide an authorized Apsara Stack tenant account for identity verification.

The Java SDK supports the use of AccessKey pairs for identity verification. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

To use AccessKey pairs as credentials, you must configure your credentials when initializing the client.

> **Notice** Ensure that code containing your AccessKey pair is kept confidential and is not disclosed, such as being uploaded to a public GitHub project. Otherwise, the information security of your Apsara Stack account may become compromised.

```
DefaultProfile profile = DefaultProfile.getProfile(
  "<your-region-id>",        // Your region ID.
  "<your-access-key-id>", // Your AccessKey ID.
  "<your-access-key-secret>"); // Your AccessKey Secret.
```

2.8.2.1.2.3. Initiate a request

This topic describes how to use the RDS Java SDK to initiate a request.

Procedure

1. Create an AcsClient instance.

```
IAcsClient client = new DefaultAcsClient(profile);
```

2. Create a request.

   The naming convention for requests is `${apiName}Request`. ${apiName} is the API name, such as *DescribeDBInstanceAttribute*.

   When multiple SDKs are used, different requests may have the same name. Differentiate the requests based on the PageSize value.

```
DescribeDBInstanceAttributeRequest request = new DescribeDBInstanceAttributeRequest();
request.setPageSize(10);
```

3. Initiate the request and handle the response.

```
DescribeDBInstanceAttributeResponse response;
try {
   response = client.getAcsResponse(request);
   for (DescribeDBInstanceAttributeResponse.Instance instance:response.getInstances()) {
      System.out.println(instance.getPublicIpAddress());
   }
} catch (ServerException e) {
   e.printStackTrace();
} catch (ClientException e) {
   e.printStackTrace();
}
```

   All returned fields are deserialized into the response. You can call `response.getXXX()` to obtain the response fields.

```
instanceStatus := response.getStatus()
```

   However, if an exception occurs or you want to obtain the original HTTP response, use `doAction()` to obtain the original response.

```
HttpResponse response = client.doAction(request);
```

2.8.2.1.2.4. Troubleshooting

The Java SDK returns corresponding errors when errors occur on the server side or the SDK side. These errors contain detailed error information, including the error code and the error message.

You do not need to handle the errors returned from the Java SDK. You only need to handle the errors returned by the server.

- `ServerException` indicates the error message generated on the server side.
- `ClientException` indicates the error message generated on the SDK side.

For example, if the following error occurs, you can modify the AccessKey ID based on the error message.

```
com.aliyuncs.exceptions.ClientException: InvalidAccessKeyId.NotFound : Specified access key is not foun
d.
```

If you need to handle the client errors returned from the SDK side, see the following sample code:

```
try {
    FooResponse response = client.getAcsResponse(request);
    // Handle the response.
    // ...
}catch (ServerException e){
    // You can add your own exception handling logic here.
    // For example, view the error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
    // If the problem persists, you can submit a ticket with the request ID included.
    System.out.println("ResponseId=" + e.getRequestId());
}catch (ClientException e){
    // You can add your own exception handling logic here.
    // For example, view the error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
}
```

2.8.2.1.2.5. Call an API through CommonRequest

If no SDKs are provided for specific service APIs, you can use the generic calling method CommonRequest to call the service APIs. You can use CommonRequest to call any APIs.

Characteristics of CommonRequest calling

The CommonRequest calling method has the following characteristics:

- Light weight: You only need the core package to initiate the call, without downloading or installing the SDK of each product.
- Easy and convenient: You can call the latest API without updating the SDK.
- Fast iteration

Use CommonRequest

To initiate a CommonRequest request, you must obtain the values of the following parameters. You can obtain the values of these parameters from the API document of each product.

- Domain: the service address of a product
- Version: the version of the API, which is in the format of YYYY-MM-DD

You can obtain the API version from the common parameters in the API document of each product.

- API information: the name of the API to be called.

  You must obtain the value of the Action parameter and use `request.ApiName = "<Action>"` to specify the API name.

  Take the RunInstances API as an example. You must use `request.ApiName = "RunInstances"` to specify the API name when initiating a CommonRequest request.

  You must obtain the value of the PathPattern parameter and use `request.PathPattern = "<PathPattern>"` to specify the RESTful path.

  For example, if the PathPattern value of the GetClusterList API is `/clusters`, you must use `request.PathPattern = "/clusters"` to specify the RESTful path when initiating a CommonRequest request.

Example: Call an RPC API

The following sample code shows how to use the CommonRequest method to call DescribeDBInstanceAttribute:

```
import com.aliyuncs.CommonRequest;
import com.aliyuncs.CommonResponse;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
public class Sample {
  public static void main(String[] args) {
    // Create a DefaultAcsClient instance and initialize it.
    DefaultProfile profile = DefaultProfile.getProfile(
      "<your-region-id>", // Your region ID.
      "<your-access-key-id>", // Your AccessKey ID.
      "<your-access-key-secret>"); // Your AccessKey Secret.
    IAcsClient client = new DefaultAcsClient(profile);
    // Create an API request and configure its parameters.
    CommonRequest request = new CommonRequest();
    request.setDomain("rds.aliyuncs.com");
    request.setVersion("2014-05-26");
    request.setAction("DescribeDBInstanceAttribute");
    request.putQueryParameter("PageNumber", "1");
    request.putQueryParameter("PageSize", "30");
    try {
      CommonResponse response = client.getCommonResponse(request);
      System.out.println(response.getData());
    } catch (ServerException e) {
      // TODO Auto-generated catch block
      e.printStackTrace();
    } catch (ClientException e) {
      // TODO Auto-generated catch block
      e.printStackTrace();
    }
  }
}
```

Example: Call a RESTful API

The following sample code shows how to use the CommonRequest method to call the API to list all cluster instances:

```
import com.aliyuncs.CommonRequest;
import com.aliyuncs.CommonResponse;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
public class Sample {
    public static void main(String[] args) {
        // Create a DefaultAcsClient instance and initialize it.
        DefaultProfile profile = DefaultProfile.getProfile(
            "<your-region-id>", // Your region ID.
            "<your-access-key-id>", // Your AccessKey ID.
            "<your-access-key-secret>"); // Your AccessKey Secret.
        IAcsClient client = new DefaultAcsClient(profile);
        // Create an API request and configure its parameters.
        CommonRequest request = new CommonRequest();
        request.setDomain("rds.aliyuncs.com");
        request.setVersion("2015-12-15");
        request.setUriPattern("/clusters");
        try {
            CommonResponse response = client.getCommonResponse(request);
            System.out.println(response.getData());
        } catch (ServerException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        } catch (ClientException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        }
    }
}
```

2.8.2.1.2.6. Common errors

This topic describes how to troubleshoot common errors you may encounter during the use of SDKs.

Error code	Error message	Cause	Solution
SDK.CanNotResolveEndpoint	Can not resolve endpoint, please check the user guide	The SDK cannot obtain the region endpoint of the called service.	Check whether the specified region ID and endpoint are correct. After obtaining the correct endpoint, run the following code to set the endpoint: `DefaultProfile.addEndpoint("your-region-id", "your-region-id", "product", "endpoint"");`
SDK.JsonUnmarshalError	Failed to unmarshal response	The SDK response fails to be deserialized. In most cases, it is because the structure of the response received by the SDK does not conform to the API metadata, such as mismatched fields or incorrect formatting.	You can use the `client.doAction(request)` method to obtain the original HTTP response.
SDK.TimeoutError	*The request timed out 4 times(3 for retry), perhaps we should have the threshold raised a little?*	The request has timed out and all retry attempts have failed.	In scenarios such as poor network quality, we recommend that you prolong the timeout period or increase the maximum number of retries.
SDK.ServerError: InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The API only accepts HTTPS requests. It does not accept HTTP requests.	You can add the following code to the request before it is sent: `request.setProtocol(ProtocolType.HTTPS)`

2.8.2.2. Python SDK

2.8.2.2.1. Quick start

This topic describes how to obtain and use the RDS Python SDK.

Prerequisites

- You must have a RAM user account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the Python SDK. For more information about how to view and obtain your AccessKey pair in the Apsara Stack Operations console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.

Install the Python SDK

To install the Python SDK, perform the following operations:

1. Install the SDK core library.
   - If you are using Python V2.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core
     ```

   - If you are using Python V3.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core-v3
     ```

2. Install the SDK.

   Run the following command to install the RDS Python SDK:

   ```
   pip install aliyun-python-sdk-rds
   ```

Use the Python SDK

To call the Python SDK, perform the following operations:

1. Create a client instance. When creating the client instance, you must obtain the Region ID, AccessKey ID, and AccessKey Secret.
2. Create an API request and configure its parameters.
3. Initiate the request and handle its response or exception.

```
#! /usr/bin/env python
#coding=utf-8

from aliyunsdkcore import client
from aliyunsdkcore.profile import region_provider
from aliyunsdkrds.request.v20140526 import DescribeDBInstanceAttributeRequest

# global config
region_id = 'xxxxx'
secret_id = 'xxxxx'
secret_key = 'xxxxx'

# product config
product_name = 'Rds'
endpoint = 'rds.example.com'

# create client
client.region_provider.modify_point(product_name, region_id, endpoint)
clt = client.AcsClient(secret_id, secret_key, region_id)

# setup request
request = DescribeDBInstanceAttributeRequest.DescribeDBInstanceAttributeRequest()
request.set_accept_format('json')

# get response
response = clt.do_action_with_exception(request)

print response
```

2.8.2.2.2. Use the SDK

2.8.2.2.2.1. Install the Python SDK

This topic describes how to install and use the RDS Python SDK.

The Python SDK supports Python V2.6.x, V2.7.x, V3.x, and later. You can use the following installation methods:

- Use pip (recommended)

  Run the following commands to install the Python SDK through pip:

```
pip install aliyun-python-sdk-core # Install the SDK core library.
pip install aliyun-python-sdk-rds # Install the RDS management library.
```

> **Note** If you are using Python V3.x, use the `pip install aliyun-python-sdk-core-v3` command instead of the `pip install aliyun-python-sdk-core` command.

- Download the Python SDK source code from Apsara Stack official website.

```
# Install the SDK core library.
cd aliyun-python-sdk-core
python setup.py install
# Installing the RDS Python SDK.
cd aliyun-python-sdk-rds
python setup.py install
```

- Use the source code
  i. Download the SDK package and extract it.
  ii. You can use one of the following methods to install the SDK package:
    - Modify the sys.path variable, and add the directory that you want to search for. It is the directory where the SDK package has been extracted to. Example:

```
>>> import sys
>>> sys.path.append('/Users/michael/my_py_scripts')
```

> **Note** This modification takes effect only when the RDS instance is running.

    - Configure the PYTHONPATH environment variable, and add the directory where you want to extract the SDK package to. The content of this environment variable is automatically added to the module search directory.

      You can configure the PYTHONPATH environment variable similar to how you configure the Path environment variable.
    - Place the extracted SDK package into the project. You can then use the Python SDK in the project.

2.8.2.2.2.2. Configure identity verification credentials

When using SDKs to access Apsara Stack services, you must provide an authorized Apsara Stack tenant account for identity verification.

The Python SDK supports the use of AccessKey pairs for identity verification. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

To use AccessKey pairs as credentials, you must configure your credentials when initializing the client.

> **Notice** Ensure that code containing your AccessKey pair is kept confidential and is not exposed (such as being uploaded to a public GitHub project). Otherwise, the information security of your Apsara Stack tenant account may become compromised.

```
clt = client.AcsClient(secret_id, secret_key, region_id)
```

2.8.2.2.2.3. Initiate a request

This topic describes how to use the RDS Python SDK to initiate a request.

Procedure

1. Import the SDK of the RDS service.

   ```
   from aliyunsdkcore import client
   from aliyunsdkcore.profile import region_provider
   from aliyunsdkrds.request.v20140526 import DescribeDBInstanceAttributeRequest
   ```

2. Create an AcsClient instance.

   ```
   client.region_provider.modify_point(product_name, region_id, endpoint)
   clt = client.AcsClient(secret_id, secret_key, region_id)
   ```

3. Create a Request object.

   ```
   request = DescribeDBInstanceAttributeRequest.DescribeDBInstanceAttributeRequest()
   request.set_accept_format('json')
   ```

4. Initiate the request and handle the response.

   ```
   response = clt.do_action_with_exception(request)


   print response
   ```

2.8.2.2.2.4. Set HTTPS requests

The Python SDK allows you to send API requests through HTTP and HTTPS.

When using the Python SDK, you can specify a default protocol (HTTP or HTTPS) for requests to different services, or set a global protocol for all requests.

> **Note** The default protocol for each service takes precedence over the global protocol.

Add OpenSSL support

OpenSSL support is required to send HTTPS requests by using Python SDK. To send HTTPS requests through the Python SDK, you must add OpenSSL support in Python.

Run the `python -c "import ssl"` command to check whether your Python environment supports OpenSSL. If error message `ImportError: No module named ssl` does not appear, OpenSSL is already supported.

If OpenSSL is not supported, run the following command to install it:

```
pip install pyopenssl
```

Set the protocol to HTTP or HTTPS for a request

The following code shows how to set HTTPS as the protocol for a request.

```
request = CreateInstanceRequest.CreateInstanceRequest()
request.set_protocol_type("https")
# Valid values: https and http.
```

Set a global protocol for all service requests

The following code shows how to set a global protocol for all service requests:

```
import aliyunsdkcore.request
aliyunsdkcore.request.set_default_protocol_type("https")
# Create a request and call client.do_action_with_exception() to send the request.
```

2.8.2.2.2.5. Troubleshooting

The Python SDK returns corresponding errors when errors occur on the server side or the SDK side. These errors contain detailed error information, including the error code and the error message.

You do not need to handle the errors returned from the Python SDK. You only need to handle the errors returned by the server.

- `ServerException` indicates the error message generated on the server side.
- `ClientException` indicates the error message generated on the SDK side.

For example, if the following error occurs, you can modify the AccessKey ID based on the error message.

```
aliyunsdkcore.acs\_exception.exceptions.ServerException: HTTP Status: 404 Error:InvalidAccessKeyId.N
otFound Specified access key is not found.
```

If you need to handle the client errors returned from the SDK side, see the following sample code:

```
try:
    response = client.do_action_with_exception(request)
except ServerException as e:
    // You can add your own exception handling logic here.
    // For example, view the error message.
    print e.get_http_status()
    print e.get_error_code()
    print e.get_error_msg()
```

2.8.2.2.2.6. Call an API through CommonRequest

If no SDKs are provided for specific service APIs, you can use the generic calling method CommonRequest to call the service APIs. You can use CommonRequest to call any APIs.

Characteristics of CommonRequest calling

The CommonRequest calling method has the following characteristics:

- Light weight: You only need the core package to initiate the call, without downloading or installing the SDK of each product.
- Easy and convenient: You can call the latest API without updating the SDK.
- Fast iteration

Use CommonRequest

To initiate a CommonRequest request, you must obtain the values of the following parameters. You can obtain the values of these parameters from the API document of each product.

- Domain: the service address of a product
- Version: the version of the API, which is in the format of YYYY-MM-DD

  You can obtain the API version from the common parameters in the API document of each product.
- API information: the name of the API to be called.

  You must obtain the value of the Action parameter and use `request.ApiName = "<Action>"` to specify the API name.

  Take the RunInstances API as an example. You must use `request.ApiName = "RunInstances"` to specify the API name when initiating a CommonRequest request.

  You must obtain the value of the PathPattern parameter and use `request.PathPattern = "<PathPattern>"` to specify the RESTful path.

  For example, if the PathPattern value of the GetClusterList API is `/clusters`, you must use `request.PathPattern = "/clusters"` to specify the RESTful path when initiating a CommonRequest request.

Example: Call an RPC API

The following sample code shows how Python V2.x uses the CommonRequest method to call DescribeDBInstanceAttribute:

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.request import CommonRequest
client = AcsClient('{your_access_key_id}', '{your_access_key_secret}', '{your_region_id}')
request = CommonRequest()
request.set_domain('rds.aliyuncs.com')
request.set_version('2014-05-26')
request.set_action_name('DescribeDBInstanceAttribute')
# or:
# request = CommonRequest(domain='rds.aliyuncs.com', version='2014-05-26', action_name='DescribeDBI
nstanceAttribute')
request.add_query_param('PageNumber', '1')
request.add_query_param('PageSize', '30')
response = client.do_action_with_exception(request)
```

Example: Call a RESTful API

The following sample code shows how Python V2.x uses the CommonRequest method to call the API to list all cluster instances:

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.request import CommonRequest
client = AcsClient('{your_access_key_id}', '{your_access_key_secret}', '{your_region_id}')
request = CommonRequest()
request.set_domain('cs.aliyuncs.com')
request.set_version('2015-12-15')
request.set_uri_pattern('/clusters')
# or:
# request = CommonRequest(domain='rds.aliyuncs.com', version='2014-05-26', uri_pattern='/clusters')
response = client.do_action_with_exception(request)
```

2.8.2.2.2.7. Common errors

This topic describes how to troubleshoot common errors you may encounter during the use of SDKs.

Error code	Error message	Cause	Solution

Error code	Error message	Cause	Solution

SDK.InvalidRegionId	Can not find endpoint to access.	The SDK cannot obtain the region endpoint of the called service.	Check whether the specified region ID and endpoint are correct. After you have obtained the endpoint, you can run the following code to set the endpoint:
			`from aliyunsdkcore.profile import region_provider`
			`region_provider.modify_point('product_name', 'region_id', 'endpoint')`

SDK.TimeoutError	-	The request has timed out and all retry attempts have failed.	In scenarios such as poor network quality, we recommend that you prolong the timeout period or increase the maximum number of retries.
SDK.ServerError: InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The API only accepts HTTPS requests. It does not accept HTTP requests.	You can add the following code to the request before it is sent: `request.set_protocol_type('https')`

2.8.2.3. PHP SDK

2.8.2.3.1. Quick start

Apsara Stack PHP SDK allows you to access RDS without performing complex programming operations. This topic describes how to obtain and use the RDS PHP SDK.

Prerequisites

- You must have a RAM user account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the Python SDK. For more information about how to view and obtain your AccessKey pair in the Apsara Stack Operations console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.
- Apsara Stack PHP SDK applies to PHP V5.3, V5.4, V5.5, V5.6, V7.0, and V7.1. You can run the **php -v** command to obtain the current PHP version number.

Install the PHP SDK

To install the PHP SDK, perform the following operations:

1. Download the PHP SDK source code from Apsara Stack official website.
2. Add the PHP SDK reference to your code.

   For example, if the PHP SDK is downloaded to `/path/to/aliyun-openapi-php-sdk`, run the following command:

```
require_once '/path/to/aliyun-openapi-php-sdk/aliyun-php-sdk-core/Config.php';
```

Use the PHP SDK

To call the PHP SDK, perform the following operations:

1. Create a DefaultAcsClient instance and initialize it.

   When you create and initialize a DefaultAcsClient instance, you must provide the values of Region ID, AccessKey ID, and AccessKey Secret.
2. Create an API request and configure its parameters.
3. Initiate the request and handle its response or exception.

```
<? php
use Rds\Request\V20140526\DescribeDBInstanceAttributeRequest;
# Create a DefaultAcsClient instance and initialize it.
$clientProfile = DefaultProfile::getProfile(
   "<your-region-id>",              # Your region ID.
   "<your-access-key-id>",          #  Your AccessKey ID.
   "<your-access-key-secret>"       # Your AccessKey Secret.
);
$client = new DefaultAcsClient($clientProfile);
# Set the endpoint of the current service.
$profile->endpoint ="your-region-id", "your-region-id", "product", "endpoint";
# Create an API request and configure its parameters.
$request = new DescribeDBInstanceAttributeRequest();
$request->setPageSize(10);
# Initiate the request and handle the response.
try {
   $response = $client->getAcsResponse($request);
   print_r($response);
} catch(ServerException $e) {
   print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
} catch(ClientException $e) {
   print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
}
? >
```

2.8.2.4. C# SDK

Prerequisites

Framework 2.0+

Download the SDK

Download the C# SDK source code from GitHub at https://github.com/aliyun/aliyun-openapi-net-sdk.

Install the SDK

1. Compile the C# SDK source code into a .dll file.
2. Right-click your Visual Studio project, and choose **Add Reference** > **Browse**. If you are using MonoDevelop, follow the MonoDevelop instructions to import the .dll file.
3. Select the .dll file and click **OK**. Then you can use Apsara Stack C# SDK in your project.

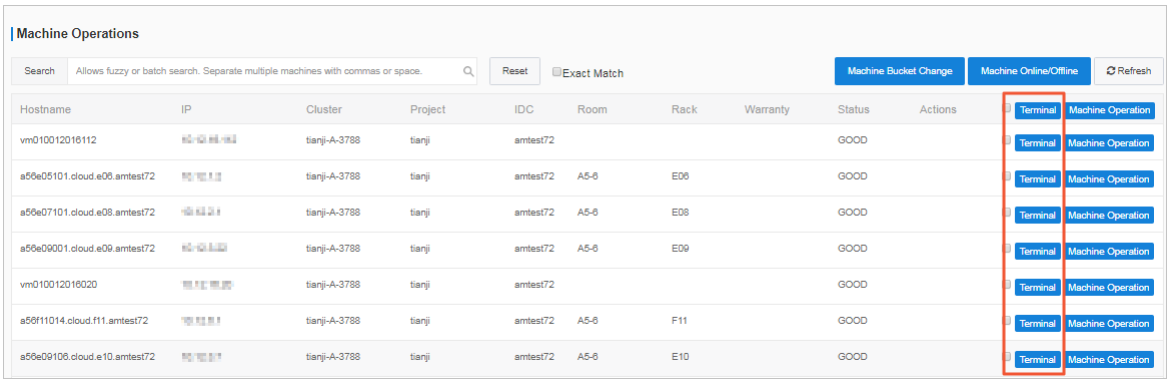
2.8.3. Obtain an endpoint

You can obtain the endpoint of RDS in the Apsara Stack Operations console.

Context

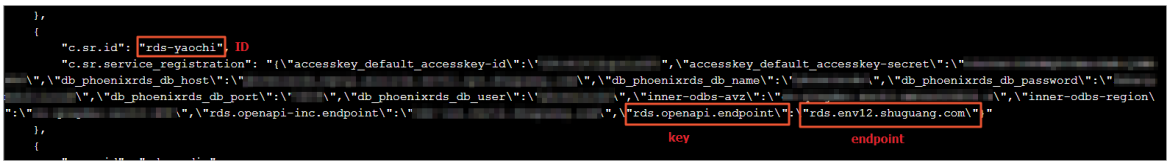
Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms** > **Apsara Stack Operations** > **Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. Choose **Operations** > **Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the command **curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration"** to obtain JSON data.

7. Obtain the *RDS* endpoint based on the ID (*rds-yaochi*) and the key value (*rds.openapi.endpoint*) of *RDS*.



2.8.4. Obtain an AccessKey pair

You can obtain an AccessKey pair in the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.

2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**.

   The system displays your AccessKey ID.

3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.9. KVStore for Redis

2.9.1. API reference

2.9.1.1. API overview

Instance lifecycle management API operations

Operation	Description
CreateInstance	Creates an instance.
DeleteInstance	Releases an instance.
ModifyInstanceSpec	Changes the specifications of a specified instance.

Instance management API operations

Operation	Description
DescribeInstanceAttribute	Queries detailed information about instances.
DescribeInstances	Queries basic information about instances.
DescribeRegions	Queries available regions.
DescribeSecurityIps	Queries the IP whitelist that allows connections to a specified instance from specified IP addresses or CIDR blocks.
FlushInstance	Clears an instance.
ModifyInstanceAttribute	Sets the attribute for a specified instance.
ModifyInstanceMaintainTime	Changes maintenance time for a specified instance.
ModifySecurityIps	Changes the whitelist for a specified instance.
ModifyInstanceNetExpireTime	Changes the period for retaining a domain name of a specified classic network.
SwitchNetwork	Changes the type of a network.

Backup and recovery API operations

Operation	Description
CreateBackup	Creates a backup.
ModifyBackupPolicy	Changes a backup policy.
DescribeBackupPolicy	Queries backup policies.
DescribeBackups	Queries available backups.
RestoreInstance	Restore a specified instance based on a specified backup set.

Monitoring management API operations

Operation	Description
DescribeMonitorItems	Queries available monitoring metrics.
DescribeHistoryMonitorValues	Queries historical monitoring data.

Parameter management API operations

Operation	Description
DescribeInstanceConfig	Queries parameters of a specified instance.
ModifyInstanceConfig	Changes parameters of a specified instance.

2.9.1.2. Request structure

Endpoints

The endpoint of KVStore for Redis API operations is `r-kvstore.*example.com*` .

For more information about how to obtain the endpoint, see Obtain an endpoint.

> **Note** The *example.com* field is a user-defined domain name used to access a project. You can request the domain name from the administrator.

Protocols

You can send API requests over HTTP or HTTPS. To secure data, we recommend that you send API requests over HTTPS.

Methods

The system allows you to send an HTTP GET request. In this request, the request URL must include the request parameters.

Request parameters

When you make an API request, you must specify the Action parameter as the operation, such as CreateInstance, that you want to perform. You also must specify common request parameters and specific request parameters of the specified operation.

Encoding

Requests and responses are encoded with the UTF-8 character set.

2.9.1.3. Common parameters

Common request parameters are used in each API operation.

Common request parameters

Common request parameters

Parameter	Type	Required	Description
Format	String	Yes	The format of the response. Valid values: JSON and XML. Default value: XML.
Version	String	Yes	The version number of the API. Specify this parameter in a date format: YYYY-MM-DD. Set this parameter to 2015-01-01.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The result string of the signature. For more information about how to calculate a signature, see Request signatures.
SignatureMethod	String	Yes	The method of signing the request. Set this parameter to HMAC-SHA1.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time must be in UTC time format. For example, 20:00:00 on January 01, 2016 in China Standard Time (UTC +8) is written as 2016-01-01T12:00:00Z.
SignatureVersion	String	Yes	The version of the signature algorithm. Set this parameter to 1.0.
SignatureNonce	String	Yes	A unique random number. This parameter is used to prevent replay attacks. You must use different random numbers for different requests.

```
https:// r-kvstore.example.com/
? Format=json
&Version=2015-01-01
&Signature=Pc5xxxxxxxxxxxxxxxxx
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2016-01-01T12:00:00Z
```

Common response parameters

Each time you call an API operation, no matter whether the call is successful, the system returns the request ID (RequestId).

```
<? xml version="1.0" encoding="utf-8"? >
<!—The root node of the response-->
<Operation name+Response>
<!—The request ID returned--->
<RequestId>4C4fdsf38-3910-447D-87AD-AC078932216</RequestId>
<!—The result data returned-->
</Operation name+Response>
```

2.9.1.4. Responses

After you call an API operation, KVStore for Redis returns data in the same format. In the response, an HTTP status code in the `2xx` format indicates that the call is successful. An HTTP status code in the `4xx` or `5xx` format indicates that the call failed. The system returns responses for successful calls in XML or JSON format. You can specify the response format in request parameters. The system uses the XML format by default.

> **Note** The response examples in this topic have been formatted with line breaks or indents to provide a clear view. The responses in your actual running environments are not properly formatted as these examples.

Sample success response

The response in XML format includes a message that indicates whether the call is successful and the specific service data. An example is as follows:

```
<? xml version="1.0" encoding="utf-8"? >
<!—The root node of the response-->
<Operation name+Response>
<!—The request ID returned-->
<RequestId>4C4fdsf38-3910-447D-87AD-AC078932216</RequestId>
<!—The result data returned-->
</Operation name+Response>
```

JSON format

```
{
"RequestId": "4C4fdsf38-3910-447D-87AD-AC078932216",
/* The result data returned */
}
```

Sample error response

When an error occurs during an API call, no result data is returned. You can locate the cause of the error by referencing the attached list of error codes. If an error occurs when you call an operation over HTTP, an HTTP status code in the `4xx` or `5xx` format is returned. The returned message body includes the specific error code and error message. The message body also contains a globally unique request ID called RequestId and a target site ID called HostId. If you cannot locate the cause, request Apsara Stack customer service, and provide the HostId and RequestId for troubleshooting.

```
<? xml version="1.0" encoding="UTF-8"? >
<Error>
<RequestId>8906582E-6722-409A-A6C4-0E7863B733A5</RequestId>
<HostId> r-kvstore.example.com</HostId>
<Code>UnsupportedOperation</Code>
<Message>The specified action is not supported. </Message>
</Error>
```

JSON format

```
{
"RequestId": "7463B73D-35CC-4D19-A010-6B8D65D242EF",
"HostId": " r-kvstore.example.com",
"Code": "UnsupportedOperation",
"Message": "The specified action is not supported."
}
```

2.9.1.5. Request signatures

KVStore for Redis authenticates each access request. You need to include a signature when you submit an HTTP or HTTPS request. KVStore for Redis authenticates the request sender identity by using symmetric encryption based on an AccessKey pair that consists of an AccessKey ID and an AccessKey Secret.

You can request and manage the AccessKey ID and the AccessKey Secret on the Alibaba Cloud website. The AccessKey ID indicates your identity. The AccessKey Secret is the key used to encrypt the signature string and to verify the signature string on the server. You must keep the AccessKey ID and AccessKey Secret confidential, and they are available only to Alibaba Cloud and yourself.

For more information about how to request the AccessKey pair, see Obtain an AccessKey pair.

Sign an access request

To sign an access request, follow these steps:

1. Use request parameters to construct a canonicalized query string.
   i. To construct a canonicalized query string, sort all request parameters by name in lexicographic order. These parameters include common request parameters and customized API request parameters, but do not include the Signature parameter mentioned in the "Common request parameters" section.

      > **Note** When you use the GET method to submit requests, you specify these parameters in the request URI following the question mark (?) and connected with the ampersand (&).

   ii. Encode the name and value of each request parameter.

      Perform URL encoding on the names and values by using the UTF-8 character set. The URL encoding rules are as follows:

      - Uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), hyphens (-), underscores (_), periods (.), and tildes (~) are not encoded.
      - Encode other characters in the `%XY` format, where `XY` indicates the ASCII code of the characters in hexadecimal format. For example, the English double quotation marks (") are encoded as `%22`.
      - Extended UTF-8 characters are encoded into the `%XY%ZA...` format.
      - The English space ( ) is encoded as `%20`, rather than the plus sign (+).

      > **Note** Most libraries that support URL encoding, such as java.net.URLEncoder, follow the Multipurpose Internet Mail Extensions (MIME) encoding rules of `application/x-www-form-urlencoded`. To generate encoded strings as specified in these rules, after you perform the URL encoding, replace the plus signs (+) in the encoded strings with `%20`, the asterisks (*) with `%2A`, and `%7E` with the tilde (~).

   iii. Separate the encoded parameter names from their encoded values with equal signs (=).
   iv. Sort the equal sign-connected strings by parameter name in lexicographic order and connect them with ampersands (&).

2. Use this canonicalized query string to construct a string for signature calculation in the following way:

```
StringToSign=
HTTPMethod + “&” +
percentEncode( “/” ) + ” &” +
percentEncode(CanonicalizedQueryString)
```

In this example,

- `HTTPMethod` specifies the HTTP method such as GET used to submit the request.
- `percentEncode("/")` is the value (`namely %2F`) as the result of encoding the slash sign (/) according to the URL encoding rule described in step 1.b.
- `percentEncode(CanonicalizedQueryString)` is the string as the result of encoding the canonicalized query string described in step 1 according to the URL encoding rules described in step 1.b.

3. As defined in RFC2104, use the preceding signature string to calculate the signature into an HMAC value.

> **Note** The key that is used to calculate the signature is the AccessKey Secret appended with an ampersand (&) (ASCII: 38). The hash algorithm SHA1 is used in the calculation.

4. Encode the preceding HMAC value as a Base64 string to generate the signature value.
5. Set the Signature parameter in the request parameters to this signature value to sign the request.

> **Note** When you submit the signature value to the KVStore for Redis instance as the final request parameter value, perform URL encoding on this parameter based on RFC3986 rules in the same way as you process other parameters.

Examples

If you call the DescribeDBInstances operation, the request URL before signing is as follows:

```
http://r-kvstore.example.com/?Timestamp=2013-06-01T10:33:56Z&Format=XML&AccessKeyId=testid&Action=DescribeInstances&SignatureMethod=HMAC-SHA1&RegionId=region1&SignatureNonce=NwDAxvLU6tFE0DVb&Version=2015-01-01&SignatureVersion=1.0
```

The calculated StringToSign is as follows:

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeInstances&Format%3DXML&RegionId%3Dregion1&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3DNwDAxvLU6tFE0DVb&SignatureVersion%3D1.0&Timestamp%3D2013-06-01T10%253A33%253A56Z&Version%3D2015-01-01
```

In this example, if the AccessKey ID is `testid` and the AccessKey Secret is `testsecret`, the key used for HMAC calculation is `testsecret&`. Therefore, the calculated signature value is `BIxxxxxxxxxxxxxxxxxxxxxx=`.

The signed request URL that includes the Signature parameter is as follows:

```
http://r-kvstore.example.com/?Timestamp=2013-06-01T10%3A33%3A56Z&Format=XML&AccessKeyId=testid&Action=DescribeInstances&SignatureMethod=HMAC-SHA1&RegionId=region1&SignatureNonce=NwDAxvLU6tFE0DVb&SignatureVersion=1.0&Version=2015-01-01&Signature=BIPOMlxxxxxxxxxxxxxxxxxxu8LXBeZtLQkJTw6iFvw1E%3D
```

2.9.1.6. RAM-based authorization

2.9.1.6.1. Grant resource permissions to a RAM user

The instances that you create by using your Alibaba Cloud account are the resources owned by the account. An account has the full operation permissions on the resources under this account by default.

Alibaba Cloud Resource Access Management (RAM) allows you to grant the access and management permissions on resources under a cloud account to RAM users.

> **Note** Ignore this topic if you do not use Resource Access Management (RAM).

2.9.1.6.2. Authorized resource type for a RAM user

You can grant the permissions on only one type of KVStore for Redis resources to a Resource Access Management (RAM) user: instances.

To grant permissions to the RAM user, describe the resource in the following way.

Resource type	Resource description in an authorization policy
Instance	acs:kvstore:$regionid:$accountid:instance/$instanceid acs:kvstore:$regionid:$accountid:instance/ acs:kvstore:::instance/

All $regionid values must be the ID of the target region or `*`. All $instanceid values must be the ID of the target instance or `*`. Similarly, $account-id specifies the numerical ID of your Alibaba Cloud account. The numerical ID can be replaced with `*`.

2.9.1.6.3. Operation permissions granted to a RAM user

You are authorized to call the following API operations to manage the specified resource as a Resource Access Management (RAM) user:

- CreateInstance

- DeleteInstance
- ModifyInstanceSpec
- RenewInstance
- RenewMultiInstance
- TransformToPrePaid
- ModifyInstanceAttribute
- FlushInstance
- DescribeInstances
- DescribeInstanceAttribute
- ModifyInstanceMaintainTime
- ModifySecurityIps
- SwitchNetwork
- ModifyInstanceNetExpireTime
- CreateBackup
- ModifyBackupPolicy
- DescribeBackupPolicy
- DescribeBackups
- RestoreInstance
- DescribeHistoryMonitorValues
- DescribeInstanceConfig
- ModifyInstanceConfig

2.9.1.6.4. API authentication rules

When you use API operations to access resources as a Resource Access Management (RAM) user, the system queries the RAM service and checks whether the RAM user is granted the required permissions.

Each API operation determines the resources for permission check according to the involved resources and the semantics of the API operation. The following table lists the authentication rules corresponding to different API operations.

Authentication rules

Operation	Authentication rule
CreateDBInstance	acs:kvstore:$regionid:$accountid:instance/$instanceid
DeleteInstance	acs:kvstore:$regionid:$accountid:instance/$instanceid
ModifyInstanceSpec	acs:kvstore:$regionid:$accountid:instance/$instanceid
RenewInstance	acs:kvstore:$regionid:$accountid:instance/$instanceid

Operation	Authentication rule
RenewMultiInstance	acs:kvstore:$regionid:$accountid:instance/$instanceid
TransformToPrePaid	acs:kvstore:$regionid:$accountid:instance/$instanceid
ModifyInstanceAttribute	acs:kvstore:$regionid:$accountid:instance/$instanceid
FlushInstance	acs:kvstore:$regionid:$accountid:instance/$instanceid
DescribeInstances	acs:kvstore:$regionid:$accountid:instance/$instanceid
DescribeInstanceAttribute	acs:kvstore:$regionid:$accountid:instance/$instanceid
ModifyInstanceMaintainTime	acs:kvstore:$regionid:$accountid:instance/$instanceid
ModifySecurityIps	acs:kvstore:$regionid:$accountid:instance/$instanceid
SwitchNetwork	acs:kvstore:$regionid:$accountid:instance/$instanceid
ModifyInstanceNetExpireTime	acs:kvstore:$regionid:$accountid:instance/$instanceid
CreateBackup	acs:kvstore:$regionid:$accountid:instance/$instanceid
ModifyBackupPolicy	acs:kvstore:$regionid:$accountid:instance/$instanceid
DescribeBackupPolicy	acs:kvstore:$regionid:$accountid:instance/$instanceid
DescribeBackups	acs:kvstore:$regionid:$accountid:instance/$instanceid
RestoreInstance	acs:kvstore:$regionid:$accountid:instance/$instanceid
DescribeHistoryMonitorValues	acs:kvstore:$regionid:$accountid:instance/$instanceid
DescribeInstanceConfig	acs:kvstore:$regionid:$accountid:instance/$instanceid
ModifyInstanceConfig	acs:kvstore:$regionid:$accountid:instance/$instanceid

2.9.1.7. Manage the lifecycle

2.9.1.7.1. CreateInstance

Description

You can call this operation to create an instance. For more information about instance types, see Instance types.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to CreateInstance.
InstanceName	String	No	The name of the instance that you want to create. The name must be a string of 2 to 128 characters in length and must start with an uppercase or lowercase letter or a Chinese character. Special characters, such as at signs (@), slashes (/), colons (:), equal signs (=), quotation marks ("), angle brackets (<>), braces ({}), brackets ([]), and spaces, are not supported.

Parameter	Type	Required	Description
Password	String	No	The password of the instance that you want to create. The password must be a string of 8 to 30 characters in length and must contain uppercase letters, lowercase letters, and numbers. Note Special characters, such as exclamation points (!), angle brackets (<>), parentheses (()), brackets ([]), braces ({}), commas (,), backticks (`), tildes (~), periods (.), hyphens (-), underscores (_), at signs (@), number signs (#), dollar signs ($), percent signs (%), carets (^), ampersands (&), and asterisks (*), are not supported.
InstanceClass	String	Yes	The type of the instance that you want to create. For more information, see Instance types.
RegionId	String	Yes	The ID of the region where the instance that you want to create is located. You can call the DescribeRegions operation to view regions.

Parameter	Type	Required	Description
ZoneId	String	No	The ID of the zone under the RegionId of the instance that you want to create. You can call the DescribeRegions operation to view zones.
ChargeType	String	No	Billing method. Valid values: PrePaid and PostPaid. Default value: PostPaid.
Period	Long	No	The billing cycle for the instance that you want to create. This parameter is required if you set ChargeType to PrePaid. Unit: months. Valid values: 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 24, and 36.
Token	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that this token is unique among different requests. The token is case sensitive, and must contain only 64 ASCII characters or fewer in length. For more information, see How to ensure idempotence.

Parameter	Type	Required	Description
NetworkType	String	No	The type of the network where the instance that you want to create is located. Valid values: • CLASSIC: specifies an instance in a classic network by default. • VPC: specifies an instance in a VPC.
VpcId	String	No	The ID of the VPC where the instance that you want to create is located.
VSwitchId	String	No	The ID of the VSwitch for the instance that you want to create.
PrivateIp	String	No	The private IP address of the instance that you want to create.
SrcDBInstanceId	String	No	The ID of the instance that generated a backup set if you want to create a valid instance based on this backup set.
BackupId	String	No	The ID of the backup set that you want to use to create a valid instance. The instance specified in SrcDBInstanceId generated this backup set. You can call the DescribeBackups operation to query the BackupId value.
InstanceType	String	No	The type of the instance that you want to create. Valid values: Redis and Memcache. Default value: Redis.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.
InstanceId	String	The globally unique ID of the instance you have created.
InstanceName	String	The name of the instance you have created.

Note Due to the compatibility with earlier versions, this topic does not describe some returned fields such as Config and Region for the operation. Alibaba Cloud will delete these fields as needed in the future. In this case, do not rely on the returned fields that this topic has not described when you call this operation.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action=CreateInstance
&RegionId=cn-hangzhou
&Password=Qa123456
&InstanceClass= redis.master.small.default
```

Sample response

```
{
"InstanceId":"73xxxxxxxxxx",
"InstanceName":"73xxxxxxxxxx"
}
```

2.9.1.7.2. DeleteInstance

Description

You can call this operation to delete a specified instance. This instance that you want to release must be in the following status:

- The instance is in the running state.
- The instance is not locked.

Note You cannot delete a subscription instance until the instance expires.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to DeleteInstance.
InstanceId	String	Yes	The globally unique ID of the specified instance.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action=DeleteInstance
&InstanceId=657xxxxxxxxxxx
```

Sample response

```
{
"RequestId" : "C2225574-1D93-4F8A-B1D5-39FCBAA40660"
}
```

2.9.1.7.3. ModifyInstanceSpec

Description

You can call this operation to change the specifications of a specified instance. For more information about instance specifications, see Instance types.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifyInstanceSpec.
InstanceId	String	Yes	The globally unique ID of the specified instance.
InstanceClass	String	Yes	The type of the specified instance. For more information, see Instance types.

Response parameters

Response parameters

Parameter	Type	Description
<Common request parameters>	-	For more information, see Common parameters.
OrderId	String	The ID of the order that you have placed.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action=ModifyInstanceSpec
&InstanceId=736538d0a6894665
&InstanceClass= redis.master.mid.default
```

Sample response

```
{
"OrderId" : "201294900260011"
"RequestId" : "283746AF-82B3-4BFF-88CC-BF34CDE2732"
}
```

2.9.1.8. Manage instances

2.9.1.8.1. DescribeInstanceAttribute

Description

You can call this operation to query details of a specified instance.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common requests.
Action	String	Yes	The operation that you want to perform. Set this parameter to DescribeInstanceAttribute.
InstanceId	String	Yes	The globally unique ID of the specified instance.

Response parameters

Response parameters

Parameter	Type	Description
Instances	List	The array that contains the DBInstanceAttribute values.

DBInstanceAttribute parameters

Parameter	Type	Description
InstanceId	String	The globally unique ID of the instance that was queried.
InstanceName	String	The name of the instance that was queried.
Capacity	Long	The capacity that you have requested for the instance that was queried, in MB.
InstanceClass	String	The type of the instance that was queried.

Parameter	Type	Description
Bandwidth	Long	The bandwidth limit of the instance that was queried, in Mbit/s.
Connections	Long	The maximum number of connections to the instance that was queried.
ConnectionDomain	String	The domain name of the instance that was queried. This domain name only supports connections over an internal network.
Port	Int	The port of the instance that was queried.
RegionId	String	The region where the instance that was queried was located. For more information, see DescribeRegions.
ZoneId	String	The ID of the zone under the RegionId of the instance that was queried. For more information, see DescribeRegions.
InstanceStatus	String	The status of the instance that was queried. Possible values: • Normal: the instance that was queried was normal. • Creating: the instance that was queried was being created. • Changing: the instance that was queried was being changed. • Inactive: the instance that was queried was disabled.
ChargeType	String	The billing method of the instance that was queried. Possible values: PrePaid and PostPaid.

Parameter	Type	Description
CreateTime	String	The time when the instance that was queried was created. The time follows the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time is displayed in UTC time format.
EndTime	String	The time when the subscription instance that was queried was about to expire. The time follows the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time is displayed in UTC time format.
NetworkType	String	The type of the network where the instance that was queried was located. Possible values: CLASSIC or VPC.
VpcId	String	The ID of the VPC where the instance that was queried was located.
VSwitchId	String	The ID of the VSwitch for the instance that was queried.
PrivateIpAddress	String	The private IP address of the instance that was queried.
MaintainStartTime	String	The time when maintenance can be started.
MaintainEndTime	String	The time when maintenance can be ended.
SecurityIPList	String	The IP whitelist for the instance that was queried.
AvailabilityValue	String	The availability metrics of the current month for the instance that was queried.

Note Due to the compatibility with earlier versions, this topic does not describe some returned fields such as Config and Region for the operation. Alibaba Cloud will delete these fields as needed in the future. In this case, do not rely on the returned fields that this topic has not described when you call this operation.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action=DescribeInstanceAttribute
&InstanceId=7xxxxxxxxxxx
```

Sample response

```
{
{
   "Instances" : {
      " DBInstanceAttribute " : [{
            "Bandwidth" : 128,
            "Capacity" : 512,
            "ConnectionDomain" : "de5d88e34d004211.m.cnhzalicm10pub001.r-kvstore.example.com.com",
            "Connections" : 300,
            "ZoneId" : "cn-qingdao-b",
            "InstanceId" : "dexxxxxxxxxx",
            "InstanceName" : "xxxxxx",
            "InstanceStatus" : "Available",
             "InstanceClass" : "redis.master.mid.default",
            "Port" : 11211,
            "QPS" : 4500,
            "RegionId" : "cn-qingdao",
             "ChargType":"PostPaid",
              "NetworkType":"ClASSSIC"
            "MaintainStartTime": "02:00Z",
             "MaintainEndTime": "06:00Z",
             "SecurityIPList":"192.168.0.1",
              "AvailabilityValue":"100%"
      }]
 }
"RequestId" : "283746AF-82B3-4BFF-88CC-BF34CDE2732"
}
```

2.9.1.8.2. DescribeInstances

Description

You can call this operation to query one or more instances under a specified account.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	-	See Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to DescribeInstances.
InstanceIds	String	No	The globally unique ID of the target instance. This parameter is required when you specify an instance ID. To query multiple instances, separate the identifiers of these instances with commas (,). If the parameter value is left blank, the system queries all instances under the specified account by default.
InstanceStatus	String	No	The instance status of the specified instance: Valid values: • Normal: the specified instance is normal. • Creating: the specified instance is being created. • Changing: the specified instance is being changed. • Inactive: the specified instance is disabled.

Parameter	Type	Required	Description
ChargeType	String	No	The billing method of the specified instance. Valid values: • PrePaid: the subscription billing method. • PostPaid: the pay-as-you-go billing method.
RegionId	String	Yes	You can call the DescribeRegions operation to query the RegionId value.
InstanceType	String	No	The type of the engine for the specified instance. Valid values: • Memcache: specifies an instance of Memcache type. • Redis: specifies an instance of Redis type.
PageNumber	Integer	No	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 1 to 50. Default value: 10.
NetworkType	String	No	The type of the network where the specified instance is located. Valid values: • CLASSIC: specifies an instance in a classic network. • VPC: specifies an instance in a VPC.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.
Instances	List	The array that contains the instances that were queried.
TotalCount	Integer	The total number of instances that were queried.
PageNumber	Integer	The number of the page returned.
PageSize	Integer	The number of entries returned on each page.

Instance parameters

Parameter	Type	Description
InstanceId	String	The globally unique ID of the instance that was queried.
InstanceName	String	The name of the instance that was queried.
Capacity	Long	The capacity that you have requested for the instance that was queried, in MB.
InstanceClass	String	The type of the instance that was queried.
Bandwidth	Long	The bandwidth limit of the instance that was queried, in Mbit/s.
Connections	Long	The maximum number of connections to the instance that was queried.
ConnectionDomain	String	The domain name of the instance that was queried. This domain name only supports connections over an internal network.
Port	Int	The port of the instance that was queried.
UserName	String	The username of the instance that was queried.

Parameter	Type	Description
RegionId	String	The region where the instance that was queried was located.
ZoneId	String	The ID of the zone under the RegionId of the instance that was queried.
InstanceStatus	String	The status of the instance that was queried. Possible values: • Normal: the instance that was queried was normal. • Creating: the instance that was queried was being created. • Changing: the instance that was queried was being changed. • Inactive: the instance that was queried was disabled. • Transforming: the instance that was queried was being transformed. • BackupRecovering: the instance that was queried was being backed up and restored. • MinorVersionUpgrading: the minor version of the instance that was queried was being upgraded.
ChargeType	String	The billing method of the instance that was queried. Possible values: PrePaid and PostPaid.
CreateTime	String	The time when the instance that was queried was created. The time follows the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time is displayed in UTC time format.

Parameter	Type	Description
EndTime	String	The time when the subscription instance that was queried was about to expire. The time follows the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time is displayed in UTC time format.
NetworkType	String	The type of the network where the instance that was queried was located. Possible values: CLASSIC or VPC.
VpcId	String	The ID of the VPC where the instance that was queried was located.
VSwitchId	String	The ID of the VSwitch for the instance that was queried.
PrivateIpAddr	String	The private IP address of the instance that was queried.

Note Due to the compatibility with earlier versions, this topic does not describe some returned fields such as Config for the operation. Alibaba Cloud will delete these fields as needed in the future. In this case, do not rely on the returned fields that this topic has not described when you call this operation.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action=DescribeInstances
&PageNumber=1
&PageSize=10
&InstanceId=dexxxxxxxxxx1
```

Sample response

```
{
   "Instances" : {
      "Instance" : [{
            "Bandwidth" : 128,
            "Capacity" : 512,
            "ConnectionDomain" : "de5d88e34d004211.m.cnhzalicm10pub001.r-kvstore.example.com",
            "Connections" : 300,
            "ZoneId" : "cn-qingdao-b",
            "InstanceId" : "dexxxxxxxxxx1",
            "InstanceName" : "xxxxxx",
            "InstanceStatus" : "Available",
             "InstanceClass" : "redis.master.mid.default",
            "Port" : 11211,
            "RegionId" : "cn-qingdao",
            "UserName" : "xxxxxxxxxx"
            "NetworkType":"CLASSSIC"
"ChargeType":" PostPaid"
         }
      ]
   },
   "PageNumber" : 1,
   "PageSize" : 10,
   "TotalCount" : 1,
   "RequestId" : "969D0A1D-C91A-4837-9F70-49785DF9BDCE"
}
```


2.9.1.8.3. DescribeRegions

Description

You can call this operation to query regions where you can create instances.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to DescribeRegions.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.
RegionIds	List	The RegionIds parameter is a list. Every element in this list consists of the RegionId and ZoneIds. ZoneIds is a string, and multiple ZoneId values are separated with commas (,).

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action=DescribeRegions
```

Sample response

```
{
  "RequestId":"535A88D3-5408-4B29-AFD4-07319D97EBC4",
  "RegionIds":
  {
      {
        "ZoneIds":"cn-qingdao-b",
        "RegionId":"cn-qingdao",
      },
      {
        "ZoneIds":"cn-shenzhen-a",
        "RegionId":"cn-shenzhen",
      },
      {
        "ZoneIds":"cn-hangzhou-d,cn-hangzhou-b",
        "RegionId":"cn-hangzhou"
      },
      {
        "ZoneIds":"cn-beijing-a",
        "RegionId":"cn-beijing"
      }
  }
}
```


2.9.1.8.4. DescribeSecurityIps

Description

You can call this operation to query the list of IP addresses or CIDR blocks that you can use to connect to an instance.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to DescribeSecurityIps.

Parameter	Type	Required	Description
InstanceId	String	Yes	The name of the specified instance.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.
SecurityIpGroups	List	The list of whitelisted IP addresses or CIDR blocks for the instance that was queried.

SecurityIpGroups parameters

SecurityIpGroups parameters

Parameter	Type	Description
SecurityIpGroupName	String	The name of the IP whitelist that was queried.
SecurityIpList	String	The list of whitelisted IP addresses or CIDR blocks that were queried. A maximum of 1,000 IP addresses or CIDR blocks are displayed. IP addresses or CIDR blocks are separated with commas (,), such as `0.0.0.0/0,10.23.12.24` (IPv4 addresses) or `10.23.12.24/24` (Classless Inter-Domain Routing or CIDR notation). In the CIDR notation, 10.23.12.24 represents the IPv4 address 10.23.12.24. Its subnet mask is 255.255.255.0. The slash (/) and the following number 24 represent 24 leading 1 bits in the subnet mask and its associated routing prefix. The length of the routing prefix ranges from 1 to 32.

Sample request

```
https://r-kvstore.example.com/
? <Common request parameters>
&Action= DescribeSecurityIps
&InstanceId=6xxxxxxxxxxxxx
```

Sample response

```
{
" SecurityIpGroups " : {
" SecurityIpGroup" : [{
" SecurityIpGroupName" : "ipsecuritytest" ,
" SecurityIpList " : "10.xx.xx. 24"
}
]
},
"RequestId" : "969D0A1D-C91A-4837-9F70-49785DF9BDCE"
}
```

2.9.1.8.5. FlushInstance

Description

You can call this operation to clear data stored on an instance. The cleared data cannot be restored.

This is an asynchronous operation. After you call this operation, the system returns the result immediately. The system clears data in the background.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	-	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to FlushInstance.
InstanceId	String	Yes	The globally unique ID of the specified instance.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= FlushInstance
&InstanceId=65xxxxxxxx
```

Sample response

```
{
"RequestId" : "96893674-E50C-495D-AB0E-2F12C1E0FD45"
}
```

2.9.1.8.6. ModifyInstanceAttribute

Description

You can call this operation to modify attributes of an instance, such as the name or the password of the instance.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	-	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifyInstanceAttribute.
InstanceId	String	Yes	The globally unique ID of the specified instance.

Parameter	Type	Required	Description
InstanceName	String	No	The instance name that you want to change to. The name must be a string of 2 to 128 characters in length and must start with an uppercase or lowercase letter or Chinese character. Special characters, such as at signs (@), slashes (/), colons (:), equal signs (=), quotation marks ("), angle brackets (<>), braces ({}), brackets ([]), and spaces, are not supported.
NewPassword	String	No	The password of the specified instance. The password must be a string of 8 to 30 characters in length and must contain uppercase letters, lowercase letters, and numbers. Note Special characters, such as exclamation points (!), angle brackets (<>), parentheses (()), brackets ([]), braces ({}), commas (,), backticks (`), tildes (~), periods (.), hyphens (-), underscores (_), at signs (@), number signs (#), dollar signs ($), percent signs (%), carets (^), ampersands (&), and asterisks (*), are not supported.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= ModifyInstanceAttribute
&InstanceId=65xxxxxxxxxx
&NewPassword=Qa12345678
&InstanceName=TestInstance
```

Sample response

```
{
"RequestId" : "E3B35BEA-9EB0-402C-88CF-C46CCCC1EE59"
}
```

2.9.1.8.7. ModifyInstanceMaintainTime

Description

You can call this operation to modify maintenance time for an instance. Alibaba Cloud may perform routine maintenance for the instance during the specified maintenance time.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifyInstanceMaintainTime.
InstanceId	String	Yes	The globally unique ID of the specified instance.

Parameter	Type	Required	Description
MaintainStartTime	String	Yes	The start time of the maintenance to be performed.
MaintainEndTime	String	Yes	The end time of the maintenance to be performed.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action=ModifyInstanceMaintainTime
&InstanceId=65xxxxxxxxx
& MaintainStartTime=02:00Z
& MaintainEndTime=06:00Z
```

Sample response

```
{
"RequestId" : "A099747A-0826-499D-9422-381C07337F73"
}
```

2.9.1.8.8. ModifyInstanceNetExpireTime

Description

You can call this operation to prolong the maximum period where the IP address in a classic network is retained if you switch an instance from the classic network to a Virtual Private Cloud (VPC) and retain the IP address in the classic network.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifyInstanceNetExpireTime.
InstanceId	String	Yes	The globally unique ID of the specified instance.
ConnectionString	String	Yes	The domain name of the specified classic network.
ClassicExpiredDays	String	Yes	The maximum number of days where the IP address in a specified classic network is retained. Valid values: 14, 30, 60, and 120.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= ModifyInstanceNetExpireTime
&ConectionString= fdafas32323ed.redis.rds.aliyuncs.com
&InstanceId=fdxxxxxxxxxx
& ClassicExpiredDays=120
```

Sample response

```
{
"RequestId" : "AAAF99B1-69ED-4E80-8CD5-272C09E46ACF"
}
```

2.9.1.8.9. ModifySecurityIps

Description

You can call this operation to set the IP whitelist for an instance, so that only authorized ECS IP addresses or CIDR blocks can be used to connect to the instance.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parametersCommon parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifySecurityIps.
InstanceId	String	Yes	The globally unique ID of the specified instance.
SecurityIps	String	Yes	The list of whitelisted IP addresses or CIDR blocks that you want to modify.
SecurityIpGroupName	String	Yes	The name of the specified whitelist group.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= ModifySecurityIps
&InstanceId=65xxxxxxxxxx
&SecurityIps=1.x.x. 1,2.x.x. 2
&SecurityIpGroupName=testgroup
```

Sample response

```
{
"RequestId" : "AAAF99B1-69ED-4E80-8CD5-272C09E46ACF"
}
```

2.9.1.8.10. SwitchNetwork

Description

You can call this operation to switch the network type of an instance. You can switch an instance from a classic network to a Virtual Private Cloud (VPC).

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to SwitchNetwork.
InstanceId	String	Yes	The globally unique ID of the specified instance.

Parameter	Type	Required	Description
TargetNetworkType	String	Yes	The type of the network that you want to switch to. • VPC • Classic You can only switch from a classic network to a VPC. In this case, set this parameter to VPC.
VpcId	String	No	The ID of the VPC that you want to switch to.
VSwitchId	String	No	The ID of the VSwitch ID for the VPC that you want to switch to. This parameter is required if you have set VpcId.
RetainClassic	String	No	Specifies whether to retain the IP address in the classic network. Valid values: • True: the classic network IP address is retained. • False: the classic network IP address is not retained. Default value: False.
ClassicExpiredDays	String	No	The maximum number of days where the IP address in the classic network are retained. Unit: days. Valid values: 14, 30, 60, and 120. This parameter is required if you have set RetainClassic to True.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= SwitchNetwork
&InstanceId=fdaxxxxxxxxxx
& TargetNetworkType=VPC
&VpcId=fadsfa
&VSwitchId=131ed
&RetainClassic=True
&ClassicExpiredDays=30
```

Sample response

```
{
"RequestId" : "AAAF99B1-69ED-4E80-8CD5-272C09E46ACF"
}
```

2.9.1.9. Backup and recovery

2.9.1.9.1. CreateBackup

Description

You can call this operation to create a backup. This is an asynchronous operation. After you call this operation, the system returns the result immediately. The system creates the backup in the background.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to CreateBackup.

Parameter	Type	Required	Description
InstanceId	String	Yes	The ID of the specified instance.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= CreateBackup
&InstanceId= de5d8xxxxxxxxxx
```

Sample response

```
{
"RequestId" : "5C97648D-C85F-4D58-A71F-7B6750856BF7"
}
```

2.9.1.9.2. ModifyBackupPolicy

Description

You can call this operation to modify a backup policy for an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifyBackupPolicy.
InstanceId	String	Yes	The ID of the specified instance.

Parameter	Type	Required	Description
PreferredBackupTime	String	Yes	The time of the backup for the specified instance in the `HH:mmZ-HH:mm Z` format.
PreferredBackupPeriod	String	Yes	The backup cycle for the specified instance. Valid values: • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= ModifyBackupPolicy
&InstanceId= de5xxxxxxxxx
&PreferredBackupTime=00:00Z-04:00Z
&PreferredBackupPeriod= Saturday
```

Sample response

```
{
"RequestId" : "5C97648D-C85F-4D58-A71F-7B6750856BF7"
}
```

2.9.1.9.3. DescribeBackupPolicy

Description

You can call this operation to query a backup policy that you have specified. You can query the backup details of an instance, such as the backup cycle and backup time.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to DescribeBackupPolicy.
InstanceId	String	Yes	The ID of the specified instance.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.
BackupRetentionPeriod	String	The maximum number of days where backups of the specified instance were retained.
PreferredBackupTime	String	The time of the backup for the specified instance in the HH:mmZ-HH:mm Z format.
PreferredBackupPeriod	String	The backup cycle for the specified instance. Possible values: • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday

Parameter	Type	Description
PreferredNextBackupTime	String	The time of the next backup for the specified instance.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= DescribeBackupPolicy
&InstanceId= de5d8xxxxxxxxxxxxx
```

Sample response

```
{
"BackupRetentionPeriod":"7"
"PreferredBackupTime":"06:00Z-07:00Z"
"PreferredNextBackupTime":"2017-10-19T06:16Z"
"PreferredBackupPeriod":"Monday,Tuesday,Wednesday,Thursday,Friday,Saturday,Sunday"
"RequestId" : "5C97648D-C85F-4D58-A71F-7B6750856BF7"
}
```

2.9.1.9.4. DescribeBackups

Description

You can call this operation to query the details of a backup file, such as the backup start time, file size, backup mode, and download address.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to DescribeBackups.
InstanceId	String	Yes	The ID of the specified instance.

Parameter	Type	Required	Description
BackupId	String	No	The ID of the backup set for the specified instance.
PageSize	String	Yes	The number of entries to return on each page. Valid values: 30, 50, and 100.
PageNumber	String	Yes	The number of the page to return. Pages start from page 1. The value of this parameter cannot exceed the maximum Integer value.
StrartTime	String	Yes	The beginning of the time range where the backups are queried.
EndTime	String	Yes	The end of the time range where the backups are queried.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.
Backups	List	An array that contains backups that were queried.
PageNumber	Integer	The number of the page returned.
TotalCount	Integer	The total number of backups that were queried.
PageSize	Integer	The number of entries returned on each page.

Backup parameters

Backup parameters

Parameter	Type	Description
BackupId	String	The ID of the backup set that was queried.
BackupDBNames	String	The name of the database that was backed up.
BackupStatus	String	The status of the backup set that was queried. Possible values: • Success: the backup was successful. • Failed: the backup failed.
BackupStartTime	String	The beginning of the time range where the backup was queried.
BackupEndTime	String	The end of the time range where the backup was queried.
BackupType	String	The type of backup that was queried. Possible values: • FullBackup: indicates a full backup. • IncrementalBackup: indicates an incremental backup.
BackupMode	String	The mode of the backup that was queried. Possible values: • Automated: indicates an automatic backup. • Manual: indicates a manual backup.
BackupMethod	String	The method of the backup that was queried. Possible values: • Logical: indicates a logical backup. • Physical: indicates a physical backup.
BackupDownloadURL	String	The URL where the backup file queried was downloaded.
BackupSize	String	The size of the backup set that was queried.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= DescribeBackups
&InstanceId= de5xxxxxxxxxxxx
&PageNumber=1
&PageSize=10
&InstanceId=de5xxxxxxxxxxxx
```

Sample response

```
{
{
   " Backups " : {
      "Backup " : [{
        "BackupId":"111111111",
        "BackupDBNames":"all",
       "BackupStatus":"Success",
      "BackupType":"FullBackup",
"BackupStartTime":"2017-10-18T10:34:52Z",
"BackupEndTime":"2017-10-18T10:36:06Z",
"BackupMode":"Manual",
"BackupMethod":"Physical",
"BackupDownloadURL":"https://rdsxxx-st-v2.oss-cn-shenzhen.example.com/custins11111111/xxxxxxxxx
_data_20171018183408.rdb",
"BackupSize":"1024"
}
      ]
   },
   "PageNumber" : 1,
   "PageSize" : 10,
   "TotalCount" : 1,
"RequestId" : "5C97648D-C85F-4D58-A71F-7111111111117"
}
```

2.9.1.9.5. RestoreInstance

Description

You can call this operation to restore data to a primary instance based on a backup set.

Note Calling this operation will cause overwriting data on the specified instance with backup data. Proceed with caution.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to RestoreInstance.
InstanceId	String	Yes	The ID of the specified instance.
BackupId	String	Yes	Backup set ID

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= RestoreInstance
&InstanceId= de5dxxxxxxxxxxx
&BackupId=fdaxxxxxx
```

Sample response

```
{
"RequestId" : "AFA391BF-808F-4DA6-80A2-A382108A0945"
}
```

2.9.1.10. Manage monitoring

2.9.1.10.1. DescribeMonitorItems

Description

You can call this operation to query available monitoring metrics. The result is returned in the <parameter:unit> format.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to DescribeMonitorItems.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.
MonitorItems	List	The list of monitoring metrics that were queried.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action=DescribeMonitorItems
```

Sample response

```
{
  "MonitorItems" : {
    "MonitorItem" : [{
          "MonitorKey" : "GetQ",
          "Unit" : "Counts/s"
        }, {
          "MonitorKey" : "Flush",
          "Unit" : "Counts/s"
        }, {
          "MonitorKey" : "UsedMemCache",
          "Unit" : "Bytes"
        }, {
          "MonitorKey" : "ReplaceQ",
          "Unit" : "Counts/s"
        }
    ]
  },
  "RequestId" : "B906A893-58A3-4644-AC2D-A2C9B08706C1"
}
```


2.9.1.10.2. DescribeHistoryMonitorValues

Description

You can call this operation to query historical monitoring data of an instance.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to DescribeHistoryMonitorValues.
InstanceId	String	Yes	The ID of the specified instance.

Parameter	Type	Required	Description
StartTime	String	Yes	The beginning of the time range where the historical monitoring data is queried. Specify the time in the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time must be in UTC time format.
EndTime	String	Yes	The end of the time range where the historical monitoring data is queried. Specify the time in the ISO 8601 standard in the `YYYY-MM-DDThh:mm:ssZ` format. The time must be in UTC time format. The value of EndTime must be greater than or equal to that of StartTime.
IntervalForHistory	String	Yes	The interval for collecting monitoring data. Monitoring samples were collected every N minutes. Valid values: 01m, 05m, 15m, and 60m.
MonitorKeys	String	No	The key of the specified metric. You can call the DescribeMonitorItems operation to query the value of this parameter.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Parameter	Type	Description
MonitorHistory	String	The monitoring data returned in the JSON format. For more information, see DescribeMonitorItems. Note To improve the data transmission efficiency, only metrics whose values are not 0 have been returned. All metrics that are not displayed have been set to the default value 0.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= DescribeHistoryMonitorValues
&InstanceId= de5xxxxxxxxxxx
&EndTime=2014-11-27T12%3A02%3A00Z
&StartTime=2014-11-27T12%3A00%3A00Z
&IntervalForHistory=01m
```

Sample response

```
{
"MonitorHistory" :
"{"2014-11-27T12:00:00Z":{"IsConnectControl":false,"IsFlowControl":false,"ItemCount":1,"QuotaConnecti
on":500,"QuotaFlow":15360,"QuotaMemCache":1073741824,"QuotaQps":9000,"UsedMemCache":14},
"2014-11-27T12:01:00Z":{"IsConnectControl":false,"IsFlowControl":false,"ItemCount":1,"QuotaConnection
":500,"QuotaFlow":15360,"QuotaMemCache":1073741824,"QuotaQps":9000,"UsedMemCache":14},
"2014-11-27T12:02:00Z":{"IsConnectControl":false,"IsFlowControl":false,"ItemCount":1,"QuotaConnection
":500,"QuotaFlow":15360,"QuotaMemCache":1073741824,"QuotaQps":9000,"UsedMemCache":14}
}",
"RequestId" : "5C97648D-C85F-4D58-A71F-7B6750856BF7"
}
```

2.9.1.11. Manage parameters

2.9.1.11.1. DescribeInstanceConfig

Description

You can call this operation to query parameters of an instance.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to DescribeInstanceConfig.
InstanceId	String	Yes	The ID of the specified instance.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.
Config	String	The parameters of the specified instance that was queried. For more information, see Instance configurations.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= DescribeInstanceConfig
&InstanceId= de5dxxxxxxxxxxx
```

Sample response

```
{
"Config":"{"EvictionPolicy":"volatile-lru","hash-max-ziplist-entries":512,
"hash-max-ziplist-value":64,"list-max-ziplist-entries":512,
"list-max-ziplist-value":64,"set-max-intset-entries":512,
"zset-max-ziplist-entries":128,"zset-max-ziplist-value":64},
"RequestId":"59A58517-F8FF-44E5-B90F-F386DB3E4AB8"
}
```


2.9.1.11.2. ModifyInstanceConfig

Description

You can call this operation to modify a parameter of an instance.

Request parameters

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifyInstanceConfig.
InstanceId	String	Yes	The ID of the specified instance.
Config	String	Yes	The parameter of the specified instance that you want to modify. The value of this parameter must be in the JSON string format. For more information, see Instance configurations.

Response parameters

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common parameters.

Sample request

```
https://r-kvstore.example.com
? <Common request parameters>
&Action= ModifyInstanceConfig
&InstanceId= de5xxxxxxxxxxx
&Config={"hash-max-ziplist-entries":"512"}
```

Sample response

```
{
"RequestId":"59A58517-F8FF-44E5-B90F-F386DB3E4AB8"
}
```

2.9.1.12. Appendixes

2.9.1.12.1. Instance types

Types of KVStore for Redis instances

Standard plan

Instance type	Service code	Maximum number of connections	Maximum bandwidth (MB)	Processing capability	Description	Zone-disaster recovery deployment
1 GB standard primary/secondary edition for zone-disaster recovery	redis.logic.sharding.drredissdb1g. 1db. 0rodb. 4proxy.default	10,000	10	Single-core	Primary/secondary instance for zone-disaster recovery	Deployed across two zones in one region
2 GB standard primary/secondary edition for zone-disaster recovery	redis.logic.sharding.drredissdb2g. 1db. 0rodb. 4proxy.default	10,000	16	Single-core	Primary/secondary instance for zone-disaster recovery	Deployed across two zones in one region

Instance type	Service code	Maximum number of connections	Maximum bandwidth (MB)	Processing capability	Description	Zone-disaster recovery deployment
4 GB standard primary/secondary edition for zone-disaster recovery	redis.logic.sharding.drredissdb4g. 1db. 0rodb. 4proxy.default	10,000	24	Single-core	Primary/secondary instance for zone-disaster recovery	Deployed across two zones in one region
8 GB standard primary/secondary edition for zone-disaster recovery	redis.logic.sharding.drredissdb8g. 1db. 0rodb. 4proxy.default	10,000	24	Single-core	Primary/secondary instance for zone-disaster recovery	Deployed across two zones in one region
16 GB standard primary/secondary edition for zone-disaster recovery	redis.logic.sharding.drredissdb16g. 1db. 0rodb. 4proxy.default	10,000	32	Single-core	Primary/secondary instance for zone-disaster recovery	Deployed across two zones in one region
32 GB standard primary/secondary edition for zone-disaster recovery	redis.logic.sharding.drredissdb32g. 1db. 0rodb. 4proxy.default	10,000	32	Single-core	Primary/secondary instance for zone-disaster recovery	Deployed across two zones in one region

Premium plan

Instance type	Service code	Maximum number of connections	Maximum bandwidth (MB)	Processing capability	Description	Zone-disaster recovery deployment
1 GB advanced primary/secondary edition	redis.master.small.special2x	20,000	48	Single-core	Primary/secondary instance	Deployed in one zone

Instance type	Service code	Maximum number of connections	Maximum bandwidth (MB)	Processing capability	Description	Zone-disaster recovery deployment
2 GB advanced primary/secondary edition	redis.master.mid.special2x	20,000	48	Single-core	Primary/secondary instance	Deployed in one zone
4 GB advanced primary/secondary edition	redis.master.stand.special2x	20,000	48	Single-core	Primary/secondary instance	Deployed in one zone
8 GB advanced primary/secondary edition	redis.master.large.special1x	20,000	48	Single-core	Primary/secondary instance	Deployed in one zone
16 GB advanced primary/secondary edition	redis.master.2xlarge.special1x	20,000	48	Single-core	Primary/secondary instance	Deployed in one zone
32 GB advanced primary/secondary edition	redis.master.4xlarge.special1x	20,000	48	Single-core	Primary/secondary instance	Deployed in one zone

Cluster edition

Instance type	Service code	Maximum number of connections	Maximum bandwidth (MB)	Processing capability	Description
16 GB cluster edition	redis.sharding.small.default	80,000	384	4-core	High-performance cluster instance
32 GB cluster edition	redis.sharding.mid.default	80,000	384	8-core	High-performance cluster instance

Instance type	Service code	Maximum number of connections	Maximum bandwidth (MB)	Processing capability	Description
64 GB cluster edition	redis.sharding.large.default	80,000	384	8-core	High-performance cluster instance
128 GB cluster edition	redis.sharding.2xlarge.default	160,000	768	16-core	High-performance cluster instance
256 GB cluster edition	redis.sharding.4xlarge.default	160,000	768	16-core	High-performance cluster instance

Cluster edition for zone-disaster recovery

Instance type	Service code	Maximum number of connections	Maximum bandwidth (MB)	Processing capability	Description
16 GB cluster edition for zone-disaster recovery	redis.logic.sharding.drredismdb16g.8db.0rodb.8proxy.default	80,000	384	8-core	Cluster instance for zone-disaster recovery
32 GB cluster edition for zone-disaster recovery	redis.logic.sharding.drredismdb32g.8db.0rodb.8proxy.default	80,000	384	8-core	Cluster instance for zone-disaster recovery
64 GB cluster edition for zone-disaster recovery	redis.logic.sharding.drredismdb64g.8db.0rodb.8proxy.default	80,000	384	8-core	Cluster instance for zone-disaster recovery
128 GB cluster edition for zone-disaster recovery	redis.logic.sharding.drredismdb128g.16db.0rodb.16proxy.default	160,000	768	16-core	Cluster instance for zone-disaster recovery

Instance type	Service code	Maximum number of connections	Maximum bandwidth (MB)	Processing capability	Description
256 GB cluster edition for zone-disaster recovery	redis.logic.sharding.drredismdb256g. 16db. 0rodb. 16proxy.default	160,000	768	16-core	Cluster instance for zone-disaster recovery

2.9.1.12.2. Error codes

Description	Error code	Error message	HTTP status code
The error message returned because the RAM user is not authorized to call the API operation.	Forbidden.RAM	User not authorized to operate on the specified resource, or this API doesn't support RAM.	403
The error message returned because the operation is not supported by RAM users.	Forbedden.NotSupportRAM	This action does not support accessed by RAM mode.	403
The error message returned because the server has an exception.	ServiceUnavailable	The request has failed due to a temporary failure of the server.	503
The error message returned because the specified instance status does not exist.	InvalidStatus.NotFound	The Status provided does not exist in our records.	404
The error message returned because the specified parameter is invalid.	InvalidParameter	The specified parameter InstanceName is not valid.	400
The error message returned because only the administrator is authorized to call the specified API operation.	Forbbiden.NotAdminUser	User not authorized to operate on the specified API as you are not the administrator.	403
The error message returned because a required parameter is not specified.	MissingParameter	Specified parameter is missing.	400

Description	Error code	Error message	HTTP status code
The error message returned because at least one of the InstanceName and NewPassword parameters must be specified.	MissingParameter	InstanceName/NewPassword at least one is mandatory for this action.	400
The error message returned because you have not specified the OwnerId parameter when calling the operation.	MissingParameter	The input parameter OwnerId, OwnerAccount that is mandatory for processing this request is not supplied.	403
The error message returned because the specified Token parameter is invalid.	InvalidToken.Malformed	The Specified parameter "Token" is not valid.	400
The error message returned because the specified InstanceName parameter is invalid.	InvalidInstanceName.Malformed	The Specified parameter "InstanceName" is not valid.	400
The error message returned because the specified Password parameter is invalid.	InvalidPassword.Malformed	The Specified parameter "Password" is not valid."	400
The error message returned because the specified Instances parameter is invalid.	InvalidInstances.Malformed	The Specified parameter "Instances" is not valid.	400
The error message returned because the specified StartTime parameter is invalid.	InvalidStartTime.Malformed	The Specified parameter "StartTime" is not valid.	400
The error message returned because the specified EndTime parameter is invalid.	InvalidEndTime.Malformed	The Specified parameter "EndTime" is not valid.	400
The error message returned because the specified InstanceIds parameter is invalid.	InvalidInstanceIds.Malformed	The Specified parameter "InstanceIds" is not valid.	400

Description	Error code	Error message	HTTP status code
The error message returned because the balance is insufficient.	InsufficientBalance	Your account does not have enough balance.	400
The error message returned because your account has not passed the real-name authentication.	RealNameAuthenticationError	Your account has not passed the real-name authentication yet.	403
The error message returned because the purchased number of instances exceeds the upper limit.	QuotaExcee	Living afterpay instances quota exceeded.	400
The error message returned because the capacity configuration is invalid.	InvalidCapacity.NotFound	The Capacity provided does not exist in our records.	400
The error message returned because two specified requests use the same ClientToken.	IdempotentParameterMismatch	Request uses a client token in a previous request but is not identical to that request.	400
The error message returned because the inventory in the specified zone is insufficient.	QuotaNotEnough	Quota not enough in this zone.	400
The error message returned because you are not authorized to call order operations.	Forbbiden.SubUser	The specified action is not available for you.	403
The error message returned because the risk control system rejects the access.	Forbidden.RiskControl	This operation is forbidden by Aliyun Risk Control system.	403
The error message returned because the specified Region parameter does not exist.	InvalidRegion.NotFound	The RegionId or ZoneId provided does not exist in our records.	404
The error message returned because the specified ZoneId parameter is invalid.	InvalidZoneId.NotFound	The ZoneId provided is invalid.	400

Description	Error code	Error message	HTTP status code
The error message returned because the specified instance ID does not exist.	InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	404
The error message returned because the password is invalid.	IncorrectPassword	The Password provided is not correct.	400
The error message returned because the specified service is not available.	ServiceNotSupported	The specified service is not supported.	400
The error message returned because renewal and scaling have not been completed.	HasRenewChangeOrder	This instance has a renewChange order.	400
The error message returned because an internal error has occurred.	InternalError	The request processing has failed due to some unknown error.	500
The error message returned because the backup time is invalid.	InvalidPreferredBackupTime	Specified preferred backup time is not valid.	400
The error message returned because the specified backup type is invalid.	InvalidBackupType.Format	Specified backup type is not valid.	400
The error message returned because the specified backup method is invalid.	InvalidBackupMethod.Format	Specified backup method is not valid.	400
The error message returned because a backup job already exists.	BackupJobExists	A backup job already exists in the specified DB instance.	400
The error message returned because the backup times exceed the upper limit.	BackupTimesExceeded	Exceeding the daily backup times of this DB instance.	400
The error message returned because at least one parameter must be specified.	ParameterLeastAssociate	Must input at least one optional parameter.	400

Description	Error code	Error message	HTTP status code
The error message returned because the specified backup retention period is invalid.	InvalidBackupRetentionPeriod.Malformed	Specified backup retention period is not valid.	400
The error message returned because the specified next backup time is invalid.	InvalidPreferredBackupTime.Format	Specified preferred backup time is not valid.	400
The error message returned because the specified backup cycle is invalid.	InvalidPreferredBackupPeriod.Malformed	Specified backup period is not valid.	400
The error message returned because the current instance type does not support the operation.	IncorrectDBInstanceType	Current DB instance type does not support this operation	400
The error message returned because the specified key is invalid.	InvalidKey.Malformed	Specified key is not valid.	400
The error message returned because the signature has been used.	SignatureNonceUsed	Specified signature nonce was used already.	400
The error message returned because no virtual IP address can be assigned.	AllocateVpcIp.NotEnough	Ip resource is not enough	400
The error message returned because instances of the specified type cannot be created in the specified zone.	Zone.NotSupport	Specified zone does not support creating with instance class.	400
The error message returned because the specified class code is invalid.	MissingClassCode	Capacity or InstanceClass is mandatory for this action.	400
The error message returned because the specified instance type is not supported.	InvalidDBInstanceClass.NotFound	Specified DB instance class is not found.	404

Description	Error code	Error message	HTTP status code
The error message returned because the specified instance has been locked.	IncorrectDBInstanceLockMode	Current DB instance lock mode does not support this operation.	400
The error message returned because the specified backup set ID does not exist.	InvalidBackupSetID.NotFound	Specified backup set ID does not exist.	400
The error message returned because the current instance status does not support the specified operation.	IncorrectDBInstanceState	Current DB instance state does not support this operation.	400
The error message returned because the resources are insufficient.	InsufficientResourceCapacity	There is insufficient capacity available for the requested instance.	400
The error message returned because the specified end time is invalid.	InvalidEndTime.Format	Specified end time is not valid.	400
The error message returned because the specified duration for retaining a classic IP address is invalid.	InvalidClassicExpiredDays.Format	The specified classicExpiredDays format is not valid.	400
The error message returned because the backup set status does not support the operation.	IncorrectBackupSetState	Current backup set state does not support operations.	400
The error message returned because the specified whitelist format is invalid.	InvalidSecurityIPList.Format	Specified security IP list format is not valid.	400

2.9.1.12.3. Instance configurations

KVStore for Redis instance configurations

Parameter	Description	Value

Parameter	Description	Value
maxmemory-policy	The eviction policy that a KVStore for Redis instance uses to evict data when the memory exceeds the threshold. KVStore for Redis supports six data eviction policies.	• VolatileLRU: only evicts original data that has Time To Live (TTL) configured based on the Least Recently Used (LRU) algorithm. • VolatileTTL: only evicts data that has TTL configured based on the TTL values in ascending order. • AllKeysLRU: evicts original data based on the LRU algorithm. • VolatileRandom: only evicts original data that has TTL configured randomly. • AllKeysRandom: evicts original data randomly. • NoEviction: evicts no data, but returns an error message when you write new data to the instance.
hash-max-ziplist-entries	A hash object uses ziplist encoding only if the hash object meets both of the following conditions: • The number of key-value pairs stored in the hash object is smaller than or equal to the value of list-max-ziplist-entries. • The string lengths of keys and values in all key-value pairs stored in the hash object are smaller than or equal to the value of list-max-ziplist-value.	Default value: 512.

Parameter	Description	Value
hash-max-ziplist-value	A hash object uses ziplist encoding only if the hash object meets both of the following conditions: • The number of key-value pairs stored in the hash object is smaller than or equal to the value of list-max-ziplist-entries. • The string lengths of keys and values in all key-value pairs stored in the hash object are smaller than or equal to the value of list-max-ziplist-value.	Default value: 64.
list-max-ziplist-entries	A list object uses ziplist encoding only if the list object meets both of the following conditions: • The number of key-value pairs stored in the list object is smaller than or equal to the value of list-max-ziplist-entries. • The string lengths of keys and values in all key-value pairs stored in the list object are smaller than or equal to the value of list-max-ziplist-value.	Default value: 512.
list-max-ziplist-value	A list object uses ziplist encoding only if the list object meets both of the following conditions: • The number of key-value pairs stored in the list object is smaller than or equal to the value of list-max-ziplist-entries. • The string lengths of keys and values in all key-value pairs stored in the list object are smaller than or equal to the value of list-max-ziplist-value.	Default value: 64.

Parameter	Description	Value
set-max-intset-entries	A set object uses intset encoding only if: the number of entries is smaller than or equal to the value of set-max-intset-entries and all entries are decimal integers.	Default value: 512.
zset-max-ziplist-entries	A zset object uses ziplist encoding only if the zset object meets both of the following conditions: • The number of key-value pairs stored in the zset object is smaller than or equal to the value of zset-max-ziplist-entries. • The string lengths of keys and values in all key-value pairs stored in the zset object are smaller than or equal to the value of zset-max-ziplist-value.	Default value: 128.
zset-max-ziplist-value	A zset object uses ziplist encoding only if the zset object meets both of the following conditions: • The number of key-value pairs stored in the zset object is smaller than or equal to the value of zset-max-ziplist-entries. • The string lengths of keys and values in all key-value pairs stored in the zset object are smaller than or equal to the value of zset-max-ziplist-value.	Default value: 64.

Parameter	Description	Value
notify-keyspace-events	The keyspace notifications allow clients to subscribe to channels or modes to receive events where Redis datasets were modified in some way.	• K: the keyspace notifications. All notifications are prefixed with `\__keyspace\@_\_` . • E: the keyevent notifications. All notifications are prefixed with `__keyevent@__` . • g: the notifications about general commands that are non-type specific, such as DEL, EXPIRE, and RENAME. • $: the string command notifications. • l: the list command notifications. • s: the set command notifications. • h: the hash command notifications. • z: the sorted set command notifications. • x: the expiration events. The system sends an expiration event after the system deletes an expired key. • e: the eviction events. The system sends an eviction event after the system evicts a key according to the maxmemory policy. • A: the alias for g$lshzxe.

2.9.2. SDK reference

2.9.2.1. Java SDK

2.9.2.1.1. Quick start

This topic describes how to obtain and use *KVStore for Redis* Java SDK.

Prerequisites

- You have an authorized Alibaba Cloud account and an AccessKey pair that includes an AccessKey ID and an AccessKey Secret. For more information about how to obtain and view your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- You have obtained the service endpoint. For more information, see Obtain an endpoint.
- The Java SDK supports JDK V1.6 and later.

Install the Java SDK

If you use Apache Maven to manage Java projects, you only need to import JAR files to *pom.xml* of the project.

To use the service development kit, you must install the SDK core library and the service SDK.

The version of the core library is 3.7.1, and the version of the *KVStore for Redis*SDK is *2.0.3*.

```
<dependencies>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-sdk-core</artifactId>
      <version>3.7.1</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-core-3.7.1.jar</systemPath>
    </dependency>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-sdk-r-kvstore</artifactId>
      <version>2.0.3</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-r-kvstore-2.0.3.jar</systemPath>
    </dependency>
  </dependencies>
```

Use the Java SDK

The following example shows how to use the Java SDK:

1. Create a DefaultAcsClient instance and initialize the instance.
2. Create an API request and set parameters.
3. Initiate the request and process a success response or an error response.

```
package com.testprogram;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
importcom.aliyuncs.r_kvstore.model.v20150101.DescribeInstanceAttributeRequest;
import com.aliyuncs.r_kvstore.model.v20150101.DescribeInstanceAttributeResponse;
public class Main {
 public static void main(String[]args) {
  // Create a DefaultAcsClient instance and initialize the instance.
  DefaultProfile profile = DefaultProfile.getProfile(
    "<your-region-id>", // The name of the region where your instance is located.
    "<your-access-key-id>", // The AccessKey ID of your account.
    "<your-access-key-secret>"); // The AccessKey Secret of your account.
  // Set the endpoint of the current service.
  /** your-region-id =cn-hangzhou; product = redisa ; endpoint = r-kvstore.aliyuncs.com **/
  profile.addEndpoint("your-region-id", "your-region-id", "product", "endpoint");
  IAcsClient client = new DefaultAcsClient(profile);
  // Create an API request and set parameters.
  DescribeInstanceAttributeRequest request = new DescribeInstanceAttributeRequest();
  request.setInstanceId("r-m5xxxxxxxxxxxxx");
  // Initiate the request and process a success response or an error response.
  DescribeInstanceAttributeResponse response;
  try {
   response = client.getAcsResponse(request);
   for (DescribeInstancesResponse.Instance instance: response.getInstances()) {
    System.out.println(instance.getPublicIpAddress());
   }
  } catch (ServerException e) {
   e.printStackTrace();
  }
  catch (ClientException e) {
   e.printStackTrace();
  }
 }
}
```

2.9.2.1.2. Use the Java SDK

2.9.2.1.2.1. Install the Java SDK

This topic describes how to install and use *KVStore for Redis* Java SDK.

The Java SDK supports JDK V1.6 and later. You can import JAR files to install the Java SDK.

Click here to download the *KVStore for Redis* JAR files.

If you use Eclipse or IntelliJ as an integrated development environment, install the *KVStore for Redis* Java SDK by importing the JAR files.

The installation methods are described as follows:

- Use Eclipse

  To install KVStore for Redis Java SDK based on Eclipse, follow these steps:

  i. Copy the downloaded `aliyun-java-sdk-r-kvstore-2.0.3.jar` file to your project folder.

  ii. In Eclipse, open your project, right-click the project, and then select **Properties** from the shortcut menu.

  iii. In the dialog box that appears, choose **Java Build Path** > **Libraries** > **Add JARs** to add the downloaded JAR files.

  iv. Click **Apply and Close**.

- Use IntelliJ

  To install KVStore for Redis Java SDK based on IntelliJ, follow these steps:

  i. Copy the downloaded `aliyun-java-sdk-r-kvstore-2.0.3.jar` file to your project folder.

  ii. In IntelliJ, open your project. In the menu bar, choose **File** > **Project Structure**.

  iii. Click **Apply** and then click **OK**.

2.9.2.1.2.2. Configure authentication credentials

To use Alibaba Cloud SDKs to access Apsara Stack resources, you must provide an authorized Alibaba Cloud account to verify your identity.

The Java SDK supports identity verification based on AccessKey pairs. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

To use an AccessKey pair as the credential, you must configure your credential when you initialize the client.

> **Notice** Do not disclose any code containing your AccessKey pair. For example, do not commit the code to public GitHub projects. Otherwise, your Alibaba Cloud account may be compromised.

```
DefaultProfile profile = DefaultProfile.getProfile(
  "<your-region-id>",        // The ID of the region where your instance is located.
  "<your-access-key-id>",    // The AccessKey ID of your account.
  "<your-access-key-secret>"); // The AccessKey Secret of your account.
```

2.9.2.1.2.3. Make API requests

This topic describes how to use *KVStore for Redis* Java SDK to make a request.

Procedure

1. Create an AcsClient.

```
IAcsClient client = new DefaultAcsClient(profile);
```

2. Create a request.

   The Request class is named in the following way: `${apiName}Request`. In this naming convention, ${apiName} specifies the name of an API operation, such as *DescribeInstances*.

   When you use multiple service SDKs, different requests may have the same class name. Distinguish the requests by service package.

```
DescribeInstancesRequest request = new DescribeInstancesRequest();
request.setPageSize(10);
```

3. Initiate the request and process the response.

```
DescribeInstancesResponse response;
                try {
                response = client.getAcsResponse(request);
                for (DescribeInstancesResponse.Instance instance:response.getInstances()) {
                System.out.println(instance.getPublicIpAddress());
                }
                } catch (ServerException e) {
                e.printStackTrace();
                } catch (ClientException e) {
                e.printStackTrace();
                }
```

   All the returned fields are deserialized into the response. You can directly use `response.getXXX()` to obtain the fields in the response.

```
instanceStatus := response.getStatus()
```

   If an error occurs, or you require the original HTTP response, you can use `doAction()` to obtain the original response.

```
HttpResponse response = client.doAction(request);
```

2.9.2.1.2.4. Process errors

If an error occurs on the server side or SDK side, the Apsara Stack Java SDK returns the corresponding exception message. An exception message contains the detailed error information, namely the error code and the error message.

Generally, you are not required to handle the errors returned by the Apsara Stack Java SDK. You are only required to handle the errors on the server side according to the error message.

- `ServerException` is the error message on the server side.
- `ClientException` is the error message on the SDK side.

For example, if the following error occurs, modify the ID of AccessKey according to the detailed error message.

```
com.aliyuncs.exceptions.ClientException: InvalidAccessKeyId.NotFound : Specified access key is not foun
d.
```

To handle the errors returned by the Apsara Stack Java SDK, see the following code example for reference:

```
try {
    FooResponse response = client.getAcsResponse(request);
    // Handle the response.
    // ...
}catch (ServerException e){
    // Add your own error handling logic here.
    // For example, print the detailed error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
    // If the problem is tricky, open a ticket and provide the RequestId for us.
    System.out.println("ResponseId=" + e.getRequestId());
}catch (ClientException e){
    // Add your own error handling logic here.
    // For example, print the detailed error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
}
```

2.9.2.1.2.5. Use CommonRequest to make a request

If no SDK is available when you want to call an API operation of a service, you can make a request by using CommonRequest. CommonRequest allows you to call any API operations.

Benefits

CommonRequest has the following benefits:

1. Lightweight: you only need to download the core package. You do not need to download and install any SDK.

2. Easy to use: you can use the latest API operations without updating the corresponding SDK.
3. Efficient iteration.

Use CommonRequest to call an API operation

To make a CommonRequest request, you must obtain the values of the following parameters. You can obtain these values from the API documents.

- Domain: the endpoint of your service.
- Version: the version of the target API in the format of YYYY-MM-DD.

  You can obtain the API version from the common parameters in the API documents.
- Parameters of an API operation: in this example, you want to call the DescribeInstances operation.

  You must obtain the Action parameter and specify the API operation name by using `request.ApiName = "<DescribeInstances>"`.

  To initiate a CommonRequest request for DescribeInstances, you must specify the API operation name by using `request.ApiName = "DescribeInstances"`.

  You must obtain the PathPattern parameter and specify the RESTful path by using `request.PathPattern = "<PathPattern>"`.

  For example, the PathPattern parameter of the API operation for querying all cluster instances is set to `/clusters`. When you initiate a CommonRequest request, you must specify the RESTful path by using `request.PathPattern = "/clusters"`.

Example: call an RPC API operation

The following example shows how to use CommonRequest to call the DescribeInstanceStatus API operation of *KVStore for Redis*:

```
import com.aliyuncs.CommonRequest;
                import com.aliyuncs.CommonResponse;
                import com.aliyuncs.DefaultAcsClient;
                import com.aliyuncs.IAcsClient;
                import com.aliyuncs.exceptions.ClientException;
                import com.aliyuncs.exceptions.ServerException;
                import com.aliyuncs.profile.DefaultProfile;
                public class Sample {
                public static void main(String[] args) {
                // Create a DefaultAcsClient instance and initialize the instance.
                DefaultProfile profile = DefaultProfile.getProfile(
                "<your-region-id>",         // The ID of the region where your instance is located.
                "<your-access-key-id>",     // The AccessKey ID of your account.
                "<your-access-key-secret>"); // The AccessKey Secret of your account.
                IAcsClient client = new DefaultAcsClient(profile);
                // Create an API request and set parameters.
                CommonRequest request = new CommonRequest();
                request.setDomain("r-kvstore.aliyuncs.com");
                request.setVersion("2015-01-01 ");
                request.setAction("DescribeInstances");
                request.putQueryParameter("PageNumber", "1");
                request.putQueryParameter("PageSize", "30");
                try {
                CommonResponse response = client.getCommonResponse(request);
                System.out.println(response.getData());
                } catch (ServerException e) {
                // TODO Auto-generated catch block
                e.printStackTrace();
                } catch (ClientException e) {
                // TODO Auto-generated catch block
                e.printStackTrace();
                }
                }
                }
```

Example: call a RESTful API operation

The following example shows how to use CommonRequest to call the operation of *KVStore for Redis* to query all cluster instances.

```
import com.aliyuncs.CommonRequest;
        import com.aliyuncs.CommonResponse;
        import com.aliyuncs.DefaultAcsClient;
        import com.aliyuncs.IAcsClient;
        import com.aliyuncs.exceptions.ClientException;
        import com.aliyuncs.exceptions.ServerException;
        import com.aliyuncs.profile.DefaultProfile;
        public class Sample {
        public static void main(String[] args) {
        // Create a DefaultAcsClient instance and initialize the instance.
        DefaultProfile profile = DefaultProfile.getProfile(
        "<your-region-id>",         // The ID of the region where your instance is located.
        "<your-access-key-id>",     // The AccessKey ID of your account.
        "<your-access-key-secret>"); // The AccessKey Secret of your account.
        IAcsClient client = new DefaultAcsClient(profile);
        // Create an API request and set parameters.
        CommonRequest request = new CommonRequest();
        request.setDomain("r-kvstore.aliyuncs.com");
        request.setVersion("2015-01-01");
        request.setUriPattern("/clusters");
        try {
        CommonResponse response = client.getCommonResponse(request);
        System.out.println(response.getData());
        } catch (ServerException e) {
        // TODO Auto-generated catch block
        e.printStackTrace();
        } catch (ClientException e) {
        // TODO Auto-generated catch block
        e.printStackTrace();
        }
        }
        }
```

2.9.2.1.2.6. Common errors

This topic describes the common errors when you use Java SDK and how to troubleshoot the problems based on the corresponding causes and solutions.

Error code	Error message	Cause	Solution
SDK.CanNotResolveEndpoint	Can not resolve endpoint, please check the user guide	The SDK cannot automatically obtain the endpoint of the called service in the specified region.	Check whether the provided region ID and endpoint are correct. After obtaining the correct endpoint, use the following code to set the endpoint: `DefaultProfile.addEndpoint("your-region-id", "your-region-id", "product", "endpoint"");`
SDK.JsonUnmarshalError	Failed to unmarshal response	The SDK response fails to be deserialized. In most cases, the cause is that the structure of the response received by the SDK does not conform to the API metadata, such as mismatched fields or incorrect formatting.	You can use the `client.doAction(request)` method to obtain the original HTTP response.
SDK.TimeoutError	The request timed out 4 times (3 for retry), perhaps we should have the threshold raised a little?	The request has timed out and all retry attempts have failed.	In scenarios such as poor network quality, we recommend that you prolong the timeout period or increase the maximum number of retries.
SDK.ServerError:InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The API only accepts HTTPS requests and does not accept HTTP requests.	You can add the following code to the request before it is sent: `request.setProtocol(ProtocolType.HTTPS)`

2.9.2.2. Python SDK

2.9.2.2.1. Quick start

This topic describes how to obtain and use *KVStore for Redis* Python SDK.

Prerequisites

- You have an authorized Alibaba Cloud account and an AccessKey pair that includes an AccessKey ID and an AccessKey Secret. For more information about how to obtain and view your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- You have obtained the service endpoint. For more information, see Obtain an endpoint.

Install the Python SDK

To install the Python SDK, follow these steps:

1. Install the core library of the SDK.
   - If you use Python V2.x, run the following command to install the core library:

     ```
     pip install aliyun-python-sdk-core
     ```

   - If you use Python V3.x, run the following command to install the core library:

     ```
     pip install aliyun-python-sdk-core-v3
     ```

2. Install the *KVStore for Redis* SDK.

   To install the KVStore for Redis SDK, run the following command:

   ```
   pip install aliyun-python-sdk-r-kvstore
   ```

Use the Python SDK

The following example shows how to use the Python SDK:

1. Create a client instance. To create a client instance, you must obtain the Region ID, AccessKey ID, and AccessKey Secret.
2. Create an API request and set parameters.
3. Initiate the request and process a success response or an error response.

```
#! /usr/bin/env python
            #coding=utf-8

            from aliyunsdkcore import client
            from aliyunsdkcore.profile import region_provider
            from aliyunsdkecs.request.v20140526 import DescribeInstancesRequest

            # global config
            region_id = 'xxxxx'
            secret_id = 'xxxxx'
            secret_key = 'xxxxx'

            # product config
            product_name = redisa
            endpoint = 'r-kvstore.aliyuncs.com'

            # create client
            client.region_provider.modify_point(product_name, region_id, endpoint)
            clt = client.AcsClient(secret_id, secret_key, region_id)

            # setup request
            request = DescribeInstancesRequest.DescribeInstancesRequest()
            request.set_accept_format('json')

            # get response
            response = clt.do_action_with_exception(request)

            print response
```

2.9.2.2.2. Use the Python SDK

2.9.2.2.2.1. Install the Python SDK

This topic describes how to install and use *KVStore for Redis* Python SDK.

The Python SDK supports Python V2.6.x, 2.7.x, 3.x, and later. You can install the SDK in any of the following ways:

- Use pip (recommended)

  To use pip to install the SDK, run the following commands:

```
pip install aliyun-python-sdk-core # Install the core library of the Alibaba Cloud SDK.
        pip install aliyun-python-sdk-r-kvstore # Install the library that manages KVStore for Redis.
```

> **Note** If you use Python V3.x, run the `pip install aliyun-python-sdk-core-v3` command instead of the `pip install aliyun-python-sdk-core` command.

- Download the SDK code from the Apsara Stack website and install the SDK.

```
# Install the core library of the SDK.
cd aliyun-python-sdk-core
python setup.py install
# Install the KVStore for Redis SDK.
cd aliyun-python-sdk-r-kvstore
python setup.py install
```

- Use the source code
  i. Download the SDK package and decompress the package.
  ii. Install the SDK in any of the following ways:
    - Modify the sys.path file and add the directory where you decompress the package to the file, as follows:

```
>>> import sys
>>> sys.path.append('/Users/michael/my_py_scripts')
```

> **Note** This setting takes effect only when the KVStore for Redis instance is running.

    - Set the PYTHONPATH environment variable to the directory where you decompress the package. The system automatically adds the content of this environment variable to the module search directory.

      You can set the PYTHONPATH environment variable in the same way as you set the Path environment variable.
    - Place the decompressed SDK package in the project. Afterward, you can directly use the Python SDK in the project.

2.9.2.2.2.2. Configure authentication credentials

To use Alibaba Cloud SDKs to access Apsara Stack resources, you must provide an authorized Alibaba Cloud account to verify your identity.

The Python SDK supports identity verification based on AccessKey pairs. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

To use an AccessKey pair as the credential, you must configure your credential when you initialize the client.

> **Notice** Do not disclose any code containing your AccessKey pair. For example, do not commit the code to public GitHub projects. Otherwise, your Alibaba Cloud account may be compromised.

```
clt = client.AcsClient(secret_id, secret_key, region_id)
```

2.9.2.2.2.3. Make API requests

This topic describes how to use *KVStore for Redis* Python SDK to make an API request.

Procedure

1. Import the SDK of the target service.

```
DescribeInstances
from aliyunsdkcore import client
                from aliyunsdkcore.profile import region_provider
                from aliyunsdkecs.request.v20150101 import DescribeInstancesRequest
```

2. Create an AcsClient.

```
client.region_provider.modify_point(product_name, region_id, endpoint)
                clt = client.AcsClient(secret_id, secret_key, region_id)
```

3. Create a Request object.

```
request = DescribeInstancesRequest.DescribeInstancesRequest()
                request.set_accept_format('json')
```

4. Initiate the request and process the response.

```
response = clt.do_action_with_exception(request)


                print response
```

2.9.2.2.2.4. Set HTTPS requests

The Python SDK allows you to make API requests over HTTP and HTTPS.

When you use the Python SDK, you can specify an HTTP or HTTPS protocol for a request, or set a global protocol for all requests.

> **Note** The default HTTP or HTTPS protocol for each service takes precedence over the global protocol.

Add OpenSSL dependencies

The HTTPS protocol for the Python SDK is dependent on the OpenSSL library in Python. To use the Python SDK to send HTTPS requests, you must add OpenSSL dependencies in Python.

Run the `python -c "import ssl"` command to verify that the Python SDK supports OpenSSL. If the error message `ImportError: No module named ssl` is not returned, the Python SDK has supported OpenSSL.

If OpenSSL is not available, run the following command to install OpenSSL:

```
pip install pyopenssl
```

Specify an HTTP or HTTPS protocol for a request

The following example shows how to specify an HTTPS protocol for a request:

```
request = CreateInstanceRequest.CreateInstanceRequest()
request.set_protocol_type("https")
# Valid values: "https" or "http".
```

Specify a default global protocol for all requests

The following example shows how to set a default global protocol for all requests:

```
import aliyunsdkcore.request
aliyunsdkcore.request.set_default_protocol_type("https")
# Create a request and call client.do_action_with_exception() to send the request.
```

2.9.2.2.2.5. Process errors

When you use Alibaba Cloud Python SDK, if an error occurs in your application server or in the Python SDK, the SDK returns the corresponding error. The error message contains error details, such as an error code and an error message.

You do not need to process Python SDK errors. You only need to process server errors according to server error messages.

- `ServerException` indicates a server error.
- `ClientException` indicates an SDK error.

For example, if the following error occurs, you can modify the AccessKey ID according to the error message.

```
aliyunsdkcore.acs\_exception.exceptions.ServerException: HTTP Status: 404 Error:InvalidAccessKeyId.N
otFound Specified access key is not found.
```

If you need to process Python SDK errors, write your code as follows:

```
try:
    response = client.do_action_with_exception(request)
except ServerException as e:
    # Add your logic that you use to process the error here.
    # For example, print the error message.
    print e.get_http_status()
    print e.get_error_code()
    print e.get_error_msg()
```

2.9.2.2.2.6. Use CommonRequest to make a request

If no SDK is available when you want to call an API operation of a service, you can make a request by using CommonRequest. CommonRequest allows you to call any API operations.

Benefits

CommonRequest has the following benefits:

1. Lightweight: you only need to download the core package. You do not need to download and install any SDK.
2. Easy to use: you can use the latest API operations without updating the corresponding SDK.
3. Efficient iteration.

Use CommonRequest to call an API operation

To make a CommonRequest request, you must obtain the values of the following parameters. You can obtain these values from API documents.

- Domain: the endpoint of your service.
- Version: the version of the target API in the format of YYYY-MM-DD.

  You can obtain the API version from common parameters in the API documents.
- Parameters of an API operation: in this example, the operation that you want to call is DescribeInstances.

  You must obtain the Action parameter and specify the API operation name by using `request.ApiName = "<DescribeInstances>"`.

  To initiate a CommonRequest request for DescribeInstances, you must specify the API operation name by using `request.ApiName = "DescribeInstances"`.

  You must obtain the PathPattern parameter and specify the RESTful path by using `request.PathPattern = "<PathPattern>"`.

  For example, the PathPattern parameter of the API operation for querying all cluster instances is set to `/clusters`. When you initiate a CommonRequest request, you must specify the RESTful path by using `request.PathPattern = "/clusters"`.

Example: call an RPC API operation

The following example shows how Python2.x uses CommonRequest to call the DescribeInstanceStatus API operation of *KVStore for Redis*:

```
from aliyunsdkcore.client import AcsClient
        from aliyunsdkcore.request import CommonRequest
        client = AcsClient('{your_access_key_id}', '{your_access_key_secret}', '{your_region_id}')
        request = CommonRequest()
        request.set_domain('r-kvstore.aliyuncs.com')
        request.set_version('2015-01-01')
        request.set_action_name('DescribeInstances')
        # or:
        # request = CommonRequest(domain=' r-kvstore.aliyuncs.com', version='2015-01-01', action_na
me='DescribeInstances')
        request.add_query_param('PageNumber', '1')
        request.add_query_param('PageSize', '30')
        response = client.do_action_with_exception(request)
```

Example: call an RESTful API operation

The following example shows how Python2.x uses CommonRequest to call the operation of *KVStore for Redis* to query all cluster instances.

```
from aliyunsdkcore.client import AcsClient
        from aliyunsdkcore.request import CommonRequest
        client = AcsClient('{your_access_key_id}', '{your_access_key_secret}', '{your_region_id}')
        request = CommonRequest()
        request.set_domain('r-kvstore.aliyuncs.com')
        request.set_version('2015-01-01')
        request.set_uri_pattern('/clusters')
        # or:
        # request = CommonRequest(domain='r-kvstore.aliyuncs.com', version='2015-01-01', uri_pattern
='/clusters')
        response = client.do_action_with_exception(request)
```

2.9.2.2.2.7. Common errors

This topic lists the causes and solutions for some common errors you may encounter when you use the SDK.

Error code	Error message	Cause	Solution

Error code	Error message	Cause	Solution

SDK.InvalidRegionId	Can not find endpoint to access.	The error message returned because the SDK failed to automatically obtain the endpoint of the requested service in the specified region.	Check whether the specified region ID and endpoint are correct. After you obtain the endpoint, set the endpoint in the following way:
			`from aliyunsdkcore.profile import region_provider`
			`region_provider.modify_point('product_name', 'region_id', 'endpoint')`

SDK.TimeoutError	—	The error message returned because the request timed out and all retries failed.	In scenarios such as low network quality, we recommend that you increase the timeout period or the maximum number of retries.
SDK.ServerError: InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The error message returned because you made an HTTP request. The API operation only accepts HTTPS requests.	Before you send a request, add the following code: `request.set_protocol_type('https')`

2.9.2.3. PHP SDK

2.9.2.3.1. Quick start

Alibaba Cloud PHP SDK allows you to easily connect to *KVStore for Redis* instead of complex programming. This topic describes how to obtain and use the PHP SDK.

Prerequisites

- You have an authorized Alibaba Cloud account and an AccessKey pair that includes an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- You have obtained the service endpoint. For more information, see Obtain an endpoint.
- The PHP SDK applies to PHP V5.3, V5.4, V5.5, V5.6, V7.0, and V7.1. You can run the **php -v** command to obtain the current PHP version number.

Install the PHP SDK

To install the PHP SDK, follow these steps:

1. Download the PHP SDK source code from the Apsara Stack website.
2. Add the PHP SDK reference to your code.

   In this example, the PHP SDK is downloaded to `/path/to/aliyun-openapi-php-sdk`.

   ```
   require_once '/path/to/aliyun-openapi-php-sdk/aliyun-php-sdk-core/Config.php';
   ```

Use the PHP SDK

The following example shows how to use the PHP SDK:

1. Create a DefaultAcsClient instance and initialize the instance.

   When you create and initialize a DefaultAcsClient instance, you must provide the values of Region ID, AccessKeyId, and AccessKeySecret.
2. Create an API request and set parameters.
3. Initiate the request and process a success response or an error response.

```
<? php

        use R_kvstore\Request\V20150101\DescribeInstancesRequest;

        # Create a DefaultAcsClient instance and initialize the instance.
        $clientProfile = DefaultProfile::getProfile(
        "<your-region-id>"              # The ID of the region where your instance is located.
        "<your-access-key-id>"          # The AccessKey ID of your account.
        "<your-access-key-secret>"      # The AccessKey Secret of your account.
        );
        $client = new DefaultAcsClient($clientProfile);

        # Set the endpoint of your service.
        $profile->endpoint ="your-region-id", "your-region-id", "product", "endpoint";
        # Create an API request and set parameters.
        $request = new DescribeInstancesRequest();
        $request->setPageSize(10);

        # Initiate a request and process the response.
        try {
        $response = $client->getAcsResponse($request);
        print_r($response);
        } catch(ServerException $e) {
        print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
        } catch(ClientException $e) {
        print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
        }
        ? >
```

2.9.2.4. Go SDK

2.9.2.4.1. Quick start

Alibaba Cloud Go SDK allows you to easily connect to *KVStore for Redis* instead of complex programming. This topic describes how to obtain and use the Go SDK.

Prerequisites

- You have an authorized Alibaba Cloud account and an AccessKey pair that includes an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- You have obtained the service endpoint. For more information, see Obtain an endpoint.

Install the Go SDK

1. Download the Go SDK source code from the Apsara Stack website.
2. Decompress the source code to the directory where your *GO_PATH* file is located.

Use the Go SDK

The following example shows how to use the Go SDK:

1. Create a client instance.
2. Create an API request and set parameters.
3. Initiate the request and process a success response or an error response.

```
package main

        import (
        "github.com/aliyun/alibaba-cloud-sdk-go/services/r-kvstore"
        "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
        "fmt"
        )

        func main() {
        // Create an r-kvstoreClient instance.
        r-kvstoreClient, err := r-kvstore.NewClientWithAccessKey(
        "<your-region-id>",           // The ID of the region where your instance is located.
        "<your-access-key-id>",       // The AccessKey ID of your account.
        "<your-access-key-secret>")       // The AccessKey Secret of your account.
        if err ! = nil {
        // Process an error response.
        panic(err)}

        // Set the endpoint of your service.
        request.Domain = "endpoint"
        // Create an API request and set parameters.
        request := r-kvstore.CreateDescribeInstancesRequest()
        // Set request.PageSize to 10.
        request.PageSize = requests.NewInteger(10)
        // Initiate the request and process an error response.
        response, err := r-kvstore Client.DescribeInstances(request)
        if err ! = nil {
        // Process an error response.
        panic(err)
        }
        fmt.Println(response)
        }
```

2.9.2.4.2. Use the Go SDK

2.9.2.4.2.1. Install the Go SDK

This topic describes how to install *KVStore for Redis* Go SDK.

The Go SDK supports Go V1.7 and later. To install the Go SDK, follow these steps:

1. Download the Go SDK source code from the Apsara Stack website.
2. Decompress the source code to the directory where your *GO_PATH* file is located.

2.9.2.4.2.2. Configure authentication credentials

To use Alibaba Cloud SDKs to access Apsara Stack resources, you must provide an authorized Alibaba Cloud account to verify your identity.

The Go SDK supports identity verification based on AccessKey pairs. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

To use an AccessKey pair as the credential, you must configure your credential when you initialize the client.

> **Notice** Do not disclose any code containing your AccessKey pair. For example, do not commit the code to public GitHub projects. Otherwise, your Alibaba Cloud account may be compromised.

```
// Create an r-kvstoreClient instance.
ecsClient, err := r-kvstore.NewClientWithAccessKey(
    "<your-region-id>",             // The ID of the region where your instance is located.
    "<your-access-key-id>",         // The AccessKey ID of your account.
    "<your-access-key-secret>")     // The AccessKey Secret of your account.
```

If you want to customize *Config* or use a credential other than an AccessKey pair, you must first create a `Credential` object to save the credential. Afterward, submit the `Credential` object when initializing the client.

```
// Customize Config.
config := NewConfig()
// Create a Credential object.
credential := &credentials.BaseCredential{
  AccessKeyId:    "<your-access-key-id>",
  AccessKeySecret: "<your-access-key-secret>",
}
// Initialize the client.
client, err := NewClientWithOptions("cn-hangzhou", config, credential)
```

2.9.2.4.2.3. Make API requests

This topic describes how to use *KVStore for Redis*Go SDK to make an API request.

1. Import the Go SDK of KVStore for Redis.

   ```
   import github.com/aliyun/alibaba-cloud-sdk-go/services/ecs
   ```

2. Create a *KVStore for Redis* client that contains all API operations of *KVStore for Redis*.

```
r-kvstoreClient := r-kvstore.NewClientWithAccessKey(
        "<your-region-id>",
        "<your-access-key-id>",
        "<your-access-key-secret>")
```

3. Use the `xxx.CreateXXXRequest` method to create a request.

   This method is named in the following way: `${service}.Create${apiName}Request`. In this naming convention,

   - The ${service} field specifies the lower-case service name, such as *r-kvstore*.
   - The ${apiName} field specifies the name of an API operation, such as *DescribeInstanceAttribute*.

```
request := r-kvstore.CreateDescribeInstanceAttributeRequest()
            request.InstanceId = ""
```

4. Initiate the request.

```
response, err := r-kvstoreClient.DescribeInstanceAttribute(request)
```

5. Process the response.

   All the returned fields are deserialized into the response. You can directly use `response.getXXX()` to obtain the fields in the response.

```
instanceStatus := response.Status
```

   If the error `(err ! = nil)` occurs, or you require the original HTTP response, you can obtain the original response in the following ways:

```
// Obtain the original HTTP response. The response type is *http.Response.
        httpResponse := response.GetOriginHttpResponse()

        // Obtain the status code of the original HTTP response. The response type is int.
        statusCode := response.GetHttpStatus()

        // Obtain the header of the original HTTP response. The response type is map[string][]string.
        headers := response.GetHttpHeaders()

        // Obtain the content of the original HTTP response. The response type is []byte.
        contentBytes := response.GetHttpContentBytes()

        // Obtain the content of the original HTTP response and transcode the content to a string based on UTF-8. The response type is string.
        contentString := response.GetHttpContentString()
```

2.9.2.4.2.4. Process errors

When an error occurs in your application server or in Alibaba Cloud Go SDK, Alibaba Cloud Go SDK returns the corresponding error information, including the `ClientError` and `ServerError` under the `sdk.errors` package. These errors are based on standard Go error API. You can process errors that Alibaba Cloud Go SDK returns in the same way as you process standard Go errors.

ClientError

When an error occurs in a SDK where an automatic call fails, the SDK returns a `ClientError` message.

The following code shows how to determine and obtain the error message in `ClientError` :

```
response, err := r-kvstoreClient.DescribeInstances(request)
if clientError, ok := err.(*errors.ClientError); ok{
    // Obtain the error code.
    clientError.ErrorCode()
    // Obtain the error description.
    clientError.Message()
    // Obtain the original error. The returned value may be nil.
    clientError.OriginError()
}
```

ServerError

When the SDK receives an error response from your application server, the SDK encapsulates the response into a `ServerError` message and returns the message to your application.

> **Note** In this case, you can still obtain the original HTTP response from the response.

The following code shows how to determine and obtain the error message in ServerError and the response:

```
response, err := r-kvstoreClient.DescribeInstances(request)
if serverError, ok := err.(*errors.ServerError); ok{
    // Obtain the error code.
    serverError.ErrorCode()
    // Obtain the error description.
    serverError.Message()
    // Obtain the original HTTP response.
    response.GetOriginHttpResponse()
}
```

2.9.2.4.2.5. Custom configurations

The topic lists the configurations that you can customize when you use the Go SDK.

Configuration

The Go SDK allows you to customize the configuration in the following way:

```
config := NewConfig().
    WithEnableAsync(true).
    WithGoRoutinePoolSize(5).
    WithMaxTaskQueueSize(1000)
client, err := ecs.NewClientWithOptions("<region-id>", config, credential)
```

Note The `config` module of the Go SDK does not support the following request:

```
config := &Config{EnableAsync: true,}
```

Supported custom configurations

The following table lists the custom configurations that the Go SDK supports.

Parameter	Default value	Description
AutoRetry	true	Whether to enable the automatic retry feature.
MaxRetryTime	3	The maximum number of retries. If the automatic retry feature is enabled, the maximum time consumption for a single call is: Timeout (MaxRetryTime + 1)
Timeout	10time.Second	The timeout value. The timeout period covers the entire lifecycle of a call, including establishing a connection, redirecting a request, and reading a response. If the value is set to *0*, no timeout occurs.
HttpTransport	nil	This parameter enables the configuration of `net/http.client`. You can configure `http.client` by using this parameter to establish a persistent connection.
EnableAsync	false	Whether to enable the asynchronous request feature.
MaxTaskQueueSize	1000	This parameter takes effect only when you specify the following configuration: `EnableAsync=true`. When a queue is full, the system blocks new requests.

Parameter	Default value	Description
GoRoutinePoolSize	5	This parameter takes effect only when you specify the following configuration: `EnableAsync=true`.

2.9.2.4.2.6. Make asynchronous requests

Due to the concurrency of the Go language, we recommend that you control the concurrent requests of Go SDKs in your applications. Alibaba Cloud Go SDK provides the concurrent request method that you can use directly. The SDK controls concurrent requests.

Enable the concurrency feature of an SDK client

In the following example, the `Credential` object specifies the user credential.

```
// The maximum number of concurrent requests.
poolSize := 10

// The maximum number of cacheable requests.
maxTaskQueueSize := 10000

// Enable asynchronous requests when you create a SDK client.
config := sdk.NewConfig().
   WithEnableAsync(true).
   WithGoRoutinePoolSize(poolSize).          // Optional. Default value: 5.
   WithMaxTaskQueueSize(maxTaskQueueSize)     // Optional. Default value: 1000

// Use the custom configuration to initialize the client.
ecsClient, err := ecs.NewClientWithOptions("<your-region-id>", config, credential)

// Or enable asynchronous requests after you initialize the client.
client.EnableAsync(poolSize, maxTaskQueueSize)
```

Make asynchronous requests

You can make asynchronous Go SDK requests in the following ways:

- Use channel as the response value.

  ```
  // this will not block
  responseChannel, errChannel := client.FooWithChan(request)
  // this will block
  response := <-responseChannel
  err = <-errChanne
  ```

- Use callback to control callbacks.

```
// this will not block
blocker := client.FooWithCallback(request, func(response *FooResponse, err error) {
      // handle the response and err
    }
  )
// The blocker of (chan int) type is used to control synchronization. A response value of 1 indicates th
at the call is successful. A response value of 0 indicates that the call has failed.
// When <-blocker returns 0, the error message in err is passed to callback.
// this will block
result := <-blocker
```

2.9.2.4.2.7. Use CommonRequest to make a request

If no SDK is available when you want to call an API operation of a service, you can make a request by using CommonRequest. CommonRequest allows you to call any API operations.

Example: call an RPC API operation

The following example shows how to use CommonRequest to call the DescribeInstanceStatus API operation of *KVStore for Redis*:

```
package main

        import (
        "github.com/aliyun/alibaba-cloud-sdk-go/sdk/r-kvstore"
        "github.com/aliyun/alibaba-cloud-sdk-go/sdk"
        "fmt"
        )

        func main() {
        client, err := sdk.NewClientWithAccessKey("{your_access_key_id}", "{your_access_key_id}", "{y
our_access_key_id}")
        if err ! = nil {
        panic(err)
        }

        request := r-kvstore.NewCommonRequest()
        request.Domain = "r-kvstore.aliyuncs.com"
        request.Version = "2015-01-01"
        // You must specify a value for the ApiName(Action) parameter, because this is an RPC API o
peration.
        request.ApiName = "DescribeInstanceStatus"
        request.QueryParams["PageNumber"] = "1"
        request.QueryParams["PageSize"] = "30"
        response, err := client.ProcessCommonRequest(request)
        if err ! = nil {
        panic(err)
        }
        fmt.Print(response.GetHttpContentString())
        }
```

2.9.2.4.2.8. Common errors

This topic lists the causes and solutions for some common errors you may encounter when you use the SDK.

Error code	Error message	Cause	Solution

Error code	Error message	Cause	Solution
SDK.CanNotResolveEndpoint	Can not resolve endpoint, please check the user guide	The error message returned because the SDK failed to automatically obtain the endpoint of the requested service in the specified region.	Check whether the specified region ID and endpoint are correct. After you obtain the endpoint, you can run the following code to set the endpoint: `request.Domain = "<endpoint>"`
SDK.JsonUnmarshalError	Failed to unmarshal response, but you can get the data via response.GetHttpStatusCode() and response.GetHttpContentString()	The error message returned because the SDK failed to deserialize the response. The possible cause is that the structure of the response received by the SDK was different from that specified by ApiMeta. For example, the fields did not match or the format was invalid.	For more information, see Parse the response.
SDK.TimeoutError	*The request timed out 4 times(3 for retry), perhaps we should have the threshold raised a little?*	The error message returned because the request timed out and all retry attempts failed.	• If you use the SDK in multi-region scenarios or poor network conditions, we recommend that you increase the timeout value or the maximum number of retries. • If the problem persists even in excellent network conditions, we recommend that you submit a ticket.
SDK.AsyncFunctionNotEnabled	Async function is not enabled in client, please invoke 'client.EnableAsync()' function	The error message returned because you used an asynchronous function when the asynchronous request had not been enabled.	Enable the asynchronous request feature. For more information, see Make asynchronous requests.

Parse the response

If the SDK failed to deserialize the response, you can ignore the error and extract the original HTTP response to obtain the response attributes.

> Note Alibaba Cloud Go SDK has a dependency on JMESPath. Therefore, when the response content is in the JSON format, you can directly use JMESPath to parse the response.

```
response, err := client.CreateInstance(request)
    if err ! = nil {
        // Process the error.
        if clientErr, isClientErr := err.(*errors.ClientError); isClientErr {
            if clientErr.ErrorCode() == errors.JsonUnmarshalErrorCode {
                // You can obtain the data in the original response by using the following encapsulation metho
d.
                // The HTTP status code in the response. Type: integer.
                statusCode := response.GetHttpStatus()
                // The HTTP header in the response. Type: map[string][]string.
                responseHeader := response.GetHttpHeaders()
                // The response body content. Type: []byte.
                responseBytes := response.GetHttpContentBytes()
                //  The response body content. Type: string, equivalent to `string(response.GetHttpContentByt
es())`.
                responseContent := response.GetHttpContentString()
                // You can also directly obtain the original response. Type: net/http.Response.
                httpResponse := response.GetOriginHttpResponse()
            }
        }
    }
```

2.9.2.5. .NET SDK

2.9.2.5.1. Quick start

Alibaba Cloud .NET SDK allows you to easily connect to *KVStore for Redis* instead of complex programming. This topic describes how to obtain and use the .NET SDK.

Prerequisites

- You have an authorized Alibaba Cloud account and an AccessKey pair that includes an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- You have obtained the service endpoint. For more information, see Obtain an endpoint.
- The .NET SDK applies to .NET Framework 4.0 and later.

Install the .NET SDK

To use the service development kit, you must install the SDK core library and the service SDK. For example, to call the *KVStore for Redis* SDK, you must obtain and install the SDK core library and the *KVStore for Redis* SDK. You can install the .NET SDK in any of the following methods:

- Add a DLL reference
  i. Download the compressed package that contains a DLL file from Developer Resources, and decompress the package to obtain the DLL file.
  ii. Right-click your project in the Solution Explorer of Visual Studio and select **Reference**.
  iii. In the menu that appears, click **Add Reference**.
  iv. In the dialog box that appears, click **Browse**, select the downloaded DLL file, and then click **Confirm**.
- Add a project reference
  i. Download the source code of the .NET SDK from Apsara Stack official website.
  ii. Find the *aliyun-net-openapi-XXX* subfolder in the downloaded folder, and then locate the \ *.*csproj* file. This is the .NET project file. For example, the `aliyun-net-openapi-r-kvstore` subfolder contains the `aliyun-net-sdk-r-kvstore.csproj` file.
  iii. In Visual Studio, right-click your solution.
  iv. Choose **Add** > **Existing Projects**.
  v. In the dialog box that appears, select the corresponding .NET project file from downloaded source code, such as `aliyun-net-sdk-ecs.csproj`, and click **Open**.
  vi. Right-click your project and choose **Reference** > **Add Reference**.

Use the .NET SDK

The following example shows how to use the .NET SDK:

1. Create a DefaultAcsClient instance and initialize the instance.
2. Create an API request and set parameters.
3. Initiate the request and process a success response or an error response.

```
using Aliyun.Acs.Core;
            using Aliyun.Acs.Core.Profile;
            using Aliyun.Acs.Core.Exceptions;
            using Aliyun.Acs.R_kvstore.Model.V20150101;

            class TestProgram
            {
            static void Main(string[] args)
            {
            // Create a client to initiate a request.
            IClientProfile profile = DefaultProfile.GetProfile(
            "<your-region-id>",
            "<your-access-key-id>",
            "<your-access-key-secret>");
            DefaultAcsClient client = new DefaultAcsClient(profile);
            try
            {
            // Set the endpoint of the current service.
            profile.setEndpoint("your-region-id", "your-region-id", "product", "endpoint");
            DefaultAcsClient client = new DefaultAcsClient(profile);
            try
            {
            // Create a request.
            DescribeInstancesRequest request = new DescribeInstancesRequest();
            request.PageSize = 10;
            // Initiate the request and obtain the response.
            DescribeInstancesResponse response = client.GetAcsResponse(request);
            System.Console.WriteLine(response.TotalCount);
            }
            catch (ServerException ex)
            {
            System.Console.WriteLine(ex.ToString());
            }
            catch (ClientException ex)
            {
            System.Console.WriteLine(ex.ToString());
            }
            }
            }
```

2.9.2.5.2. Use the .NET SDK

2.9.2.5.2.1. Install the .NET SDK

This topic describes how to install *KVStore for Redis* .NET SDK.

You can install the .NET SDK in any of the following methods:

- Add a DLL reference
  i. Download the compressed package that contains a DLL file from Developer Resources, and decompress the package to obtain the DLL file.
  ii. Right-click your project in the Solution Explorer of Visual Studio and select **Reference**.
  iii. In the menu that appears, click **Add Reference**.
  iv. In the dialog box that appears, click **Browse**, select the downloaded DLL file, and then click **Confirm**.
- Add a project reference
  i. Download the source code of the .NET SDK from Apsara Stack official website.
  ii. Find the *aliyun-net-openapi-XXX* subfolder in the downloaded folder, and then locate the \ *.csproj file. This is the .NET project file. For example, the `aliyun-net-openapi- r-kvstore` subfolder contains the `aliyun-net-sdk-r-kvstore.csproj` file.
  iii. In Visual Studio, right-click your solution.
  iv. Choose **Add** > **Existing Projects**.
  v. In the dialog box that appears, select the corresponding .NET project file from downloaded source code, such as `aliyun-net-sdk-ecs.csproj` , and click **Open**.
  vi. Right-click your project and choose **Reference** > **Add Reference**.

2.9.2.5.2.2. Configure authentication credentials

To use Alibaba Cloud SDKs to access Apsara Stack resources, you must provide an authorized Alibaba Cloud account to verify your identity.

The .NET SDK supports identity verification based on AccessKey pairs. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

To use an AccessKey pair as the credential, you must configure your credential when you initialize the client.

> **Notice** Do not disclose any code containing your AccessKey pair. For example, do not commit the code to public GitHub projects. Otherwise, your Alibaba Cloud account may be compromised.

```
IClientProfile clientProfile = DefaultProfile.GetProfile(
  "<your-region-id>",        // The ID of the region where your instance is located.
  "<your-access-key-id>", //  The AccessKey ID of your account.
  "<your-access-key-secret>"); // The AccessKey Secret of your account.
```

2.9.2.5.2.3. Make API requests

This topic describes how to use *KVStore for Redis* .NET SDK to make an API request.

1. Create a default client instance.

   ```
   DefaultAcsClient client = new DefaultAcsClient(clientProfile);
   ```

2. Create a request.

   The Request class is named in the following way: `${apiName}Request`. In this naming convention, ${apiName} specifies the name of an API operation, such as *DescribeInstances*.

   When you use multiple service SDKs, different requests may have the same class name. Distinguish the requests by service package.

   ```
   DescribeInstancesRequest request = new DescribeInstancesRequest();
               request.PageSize = 10;
   ```

3. Initiate the request and process the response.

   ```
   DescribeInstancesResponse response = client.GetAcsResponse(request);
   ```

   All the returned fields are deserialized into the response. You can directly use `response.getXXX()` to obtain the fields in the response.

   ```
   System.Console.WriteLine(response.TotalCount);
   ```

2.9.2.5.2.4. Process errors

When you use Alibaba Cloud .NET SDK, if an error occurs in your application server or in the .NET SDK, the SDK returns the corresponding error. The error contains error details, such as an error code and an error message.

You do not need to process SDK errors. You only needs to process server errors according to server error messages.

- `ServerException` indicates a server error.
- `ClientException` indicates an SDK error.

For example, if the following error occurs, you can modify the AccessKey ID according to the error message.

```
InvalidAccessKeyId.NotFound : Specified access key is not found.
```

If you need to process .NET SDK errors, write your code as follows:

```
try
{
    CreateInstanceResponse response = client.GetAcsResponse(request);
    // Process the response.
    // ...
}
catch (ServerException e)
{
    // Add your logic that you use to process the error here.
    // For example, print the error message when the error occurs.
    Console.WriteLine("ErrorCode=" + e.ErrorCode);
    Console.WriteLine("ErrorMessage=" + e.ErrorMessage);
    // If the problem persists, you can submit a ticket and provide the request ID to request technical sup
port.
    Console.WriteLine("ErrorCode=" + e.RequestId);
}
catch (ClientException e)
{
    // Add your logic that you use to process the error here.
    // For example, print the error message when the error occurs.
    Console.WriteLine("ErrorCode=" + e.ErrorCode);
    Console.WriteLine("ErrorMessage=" + e.ErrorMessage);
}
```

2.9.2.5.2.5. Use CommonRequest to make a request

If no SDK is available when you want to call an API operation of a service, you can make a request by using CommonRequest. CommonRequest allows you to call any API operations.

Benefits

CommonRequest has the following benefits:

1. Lightweight: you only need to download the core package. You do not need to download and install any SDK.
2. Easy to use: you can use the latest API operations without updating the corresponding SDK.
3. Efficient iteration.

Use CommonRequest to call an API operation

To make a CommonRequest request, you must obtain the values of the following parameters. You can obtain these values from the API documents.

- Domain: the endpoint of your service.
- Version: the version of the target API in the format of YYYY-MM-DD.

You can obtain the API version from the common parameters in the API documents.

- Parameters of an API operation: the name of the operation that you want to call.

  You must obtain the Action parameter and specify the API operation name by using `request.ApiName = "<Action>"`.

  To initiate a CommonRequest request for Runinstances, you must specify the API operation name by using `request.ApiName = "RunInstances"`.

  You must obtain the PathPattern parameter and specify the RESTful path by using `request.PathPattern = "<PathPattern>"`.

  For example, the PathPattern parameter of the API operation for querying all cluster instances is set to `/clusters`. When you initiate a CommonRequest request, you must specify the RESTful path by using `request.PathPattern = "/clusters"`.

Example: call an RPC API operation

The following example shows how to use CommonRequest to call the DescribeInstances API operation of *KVStore for Redis*:

```
using Aliyun.Acs.Core;
        using Aliyun.Acs.Core.Exceptions;
        using Aliyun.Acs.Core.Profile;

        class Sample
        {
        static void Main(string[] args)
        {
        // Create a client instance to initiate a request.
        IClientProfile profile = DefaultProfile.GetProfile(
        "<your-region-id>",
        "<your-access-key-id>",
        "<your-access-key-secret>");
        DefaultAcsClient client = new DefaultAcsClient(profile);

        try
        {
        // Create a request.
        CommonRequest request = new CommonRequest();
        request.Domain = "r-kvstore.aliyuncs.com";
        request.Version = "2015-01-01";

        // You must specify a value for the ApiName(Action) parameter, because this is an RPC API ope
ration.
        request.Action = "DescribeInstances";
```

```
request.AddQueryParameters("PageNumber", "1");
request.AddQueryParameters("PageSize", "30");

// Initiate the request and obtain the response.
CommonResponse response = client.GetCommonResponse(request);
System.Console.WriteLine(response.Data);
}
catch (ServerException ex)
{
System.Console.WriteLine(ex.ToString());
}
catch (ClientException ex)
{
System.Console.WriteLine(ex.ToString());
}
}
}
```

Example: call a RESTful API operation

The following example shows how to use CommonRequest to call the operation of KVStore for Redis to query all cluster instances.

```
using Aliyun.Acs.Core;
            using Aliyun.Acs.Core.Exceptions;
            using Aliyun.Acs.Core.Profile;

            class Sample
            {
            static void Main(string[] args)
            {
            // Create a client instance to initiate a request.
            IClientProfile profile = DefaultProfile.GetProfile(
            "<your-region-id>",
            "<your-access-key-id>",
            "<your-access-key-secret>");
            DefaultAcsClient client = new DefaultAcsClient(profile);

            try
            {
            // Create a request.
            CommonRequest request = new CommonRequest();
            request.Domain = "r-kvstore.aliyuncs.com";
            request.Version = "2015-01-01";

            // You must specify a value for the UriPattern parameter, because this is a Restful API opera
tion.
            request.UriPattern = "/clusters";

            // Initiate the request and obtain the response.
            CommonResponse response = client.GetCommonResponse(request);
            System.Console.WriteLine(response.Data);
            }
            catch (ServerException ex)
            {
            System.Console.WriteLine(ex.ToString());
            }
            catch (ClientException ex)
            {
            System.Console.WriteLine(ex.ToString());
            }
            }
            }
```

2.9.2.5.2.6. Common errors

This topic lists the causes and solutions for some common errors you may encounter when you use the SDK.

Error code	Cause	Solution
SDK.InvalidRegionId	The error message returned because the SDK failed to automatically obtain the endpoint of the requested service in the specified region.	Check whether the specified endpoint is correct.
InvalidAccessKeyId.NotFound	The error message returned because the specified AccessKey ID was invalid.	Check whether your AccessKey ID is correct.
SDK.ConnectionReset	The error message returned because the endpoint was not accessible when you initiated a request.	Make sure that your network is available.
SDK.InvalidProfile	The error message returned because the DefaultProfile parameter that you provided when initializing DefaultAcsClient was invalid.	Make sure that the DefaultProfile parameter object that you provide has been properly initialized and had the corresponding parameters configured.
SDK.SessionTokenExpired	The error message returned because the DefaultProfile parameter that you provided when initializing DefaultAcsClient was invalid.	Make sure that the SessionToken parameter is valid. The validity period of this parameter is one hour.
SignatureDoesNotMatch	The error message returned because the SessionToken you provided was invalid or expired.	Make sure that the DefaultProfile parameter object that you provide has been properly initialized and had the corresponding parameters configured.
SDK.InvalidProfile	The error message returned because the AccessKey Secret did not match the AccessKey ID.	Make sure that the AccessKey Secret is valid.

2.9.2.6. Obtain an AccessKey pair

You can obtain the AccessKey pair on the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**.

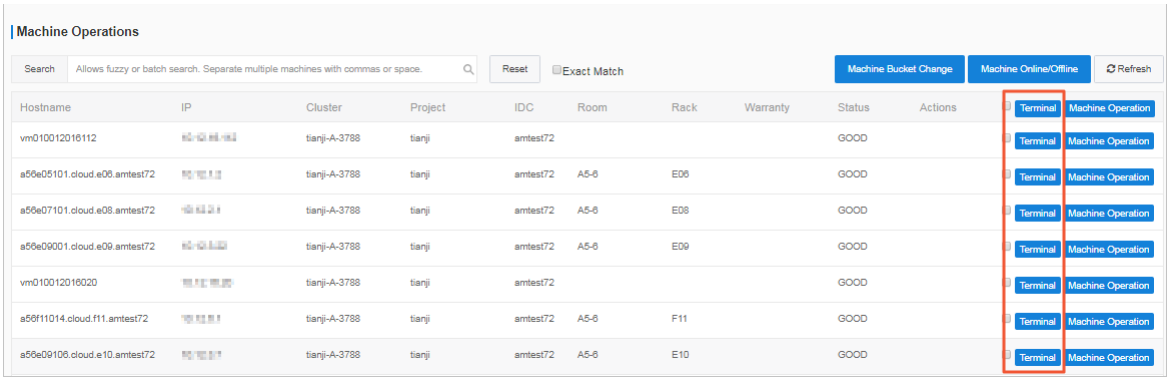
   The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.9.2.7. Obtain an endpoint

You can obtain the product endpoint in Apsara Stack Operations.

Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms** > **Apsara Stack Operations** > **Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. Choose **Operations** > **Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the command **curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration"** to obtain JSON data.

7. Locate the *KVStore for Redis* endpoint based on the ID (*kvstore-yaochi*) and key (*r-kvstore.openapi.endpoint*) of the *KVStore for Redis* service.

2.10. ApsaraDB for MongoDB

2.10.1. List of operations by function

2.10.1.1. Lifecycle management

API	Description
CreateDBInstance	Creates a replica set instance.
ModifyDBInstanceSpec	Modifies specifications for a replica set instance.
DeleteDBInstance	Releases a replica set instance.
RenewDBInstance	Renews a replica set instance.

2.10.1.2. Instance management

API	Description
DescribeRegions	Queries the list of available regions.
DescribeDBInstances	Queries the list of instances.
RestartDBInstance	Restarts an instance.
ModifyDBInstanceMaintainTime	Modifies the maintenance time of an instance.
ModifyDBInstanceDescription	Modifies the description of an instance.
DescribeDBInstanceAttribute	Queries the details of an instance.
ModifyDBInstanceNetworkType	Modifies the network type of an instance.
ModifyDBInstanceNetExpireTime	Prolongs the retention period of the classic network endpoint.

2.10.1.3. Account management

Operation	Description
DescribeAccounts	Queries accounts.
ResetAccountPassword	Resets the password of an account.

2.10.1.4. Database security management

API	Description
DescribeSecurityIps	Queries the IP address whitelist for an instance.
ModifySecurityIps	Modifies the IP address whitelist for an instance.
DescribeAuditRecords	Queries audit logs.
DescribeAuditFiles	Queries audit log files.

2.10.1.5. Backup and restoration management

API	Description
DescribeBackupPolicy	Queries a backup policy.
ModifyBackupPolicy	Modifies a backup policy.
CreateBackup	Creates a backup.
DescribeBackups	Queries the list of backups.
RestoreDBInstance	Restores a backup set to an instance.

2.10.1.6. Monitoring alert management

API	Description
DescribeDBInstancePerformance	Queries the instance performance data.

2.10.2. Make API requests

2.10.2.1. Request structure

Endpoints

The service endpoint of ApsaraDB for MongoDB APIs is mongodb.example.com.

Protocols

You can send requests over HTTP or HTTPS. We recommend that you use HTTPS for enhanced security.

Methods

The HTTP GET method can be used to send requests. Request parameters must be included in the request URL.

Parameters

Each request must specify the action to be performed (such as CreateDBInstance) in the Action parameter. Each action must include both the common request parameters that are used for all API requests as well as the specific request parameters of the API being called.

Encoding

Requests and responses are encoded in UTF-8.

2.10.2.2. Common parameters

Common request parameters must be included in the request of each API.

2.10.2.2.1. Common request parameters

Request parameters

Parameter	Type	Required	Description
Format	String	Yes	The format of the returned data. Valid values: JSON and XML. Default value: XML.
Version	String	Yes	The API version, in the format of YYYY-MM-DD. The current version is 2015-12-01.
AccessKeyId	String	Yes	The AccessKey ID provided by Alibaba Cloud for you to access services.
Signature	String	Yes	The signature result string. For more information about signature calculation methods, see the "Sign signatures" topic.
SignatureMethod	String	Yes	The algorithm used to create the request signature. Valid value: HMAC-SHA1.
Timestamp	String	Yes	The request timestamp. The timestamp uses UTC and complies with the ISO8601 standard. The format is YYYY-MM-DDThh:mm:ssZ. Example: 2016-01-01T12:00:00Z.
SignatureVersion	String	Yes	The signature algorithm version. The current version is 1.0.
SignatureNonce	String	Yes	A unique, randomly generated number used to prevent network replay attacks. You must use a different random number for each request.

Examples

```
https://mongodb.example.com/
? Format=json
&Version=2015-12-01
&Signature=Pc5WBxxxxxxxx
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2016-01-01T12:00:00Z
```

2.10.2.2.2. Common response parameters

The system returns a unique RequestId for each API request, regardless of whether the API operation is successful.

Examples

```
<? xml version="1.0" encoding="utf-8"? >
<!—Result root node-->
<API name + response>
<!—Returned request tag-->
<RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
<!—Response-->
</API name + response>
```

2.10.2.2.2.1. Responses

The response data for API requests is displayed in a uniform format. In the response data, HTTP status code 2xx indicates that the API operation is successful. HTTP status code 4xx or 5xx indicates that the API operation fails. The response data for called API operations is returned in either the XML or JSON format. You can add parameters to an API request to specify the format of the response data. Response data uses the XML format by default. The response examples in this topic are formatted with line breaks or indents for a clear view. Actual response data is not formatted in the same manner as these examples.

2.10.2.3. Sign signatures

ApsaraDB for MongoDB authenticates the sender identity of each request that it receives. Therefore, you must include a signature in HTTP or HTTPS requests. ApsaraDB for MongoDB performs symmetric encryption to verify the request sender's identity by using the AccessKey ID and AccessKey Secret. The AccessKey ID and AccessKey Secret are officially issued to visitors by Alibaba Cloud. Visitors can apply for and manage them on the official Alibaba Cloud website. The AccessKey ID indicates the identity of the visitor. The AccessKey Secret is used by the client to encrypt signature strings and used by the server to verify signature strings. You must keep your AccessKey Secret confidential. Perform the following steps to sign an access request:

1. Use request parameters to construct a canonicalized query string.
   i. To construct a canonicalized query string, sort all request parameters by name in alphabetic order. These parameters include common request parameters and customized API request parameters , but do not include the Signature parameter.

      > **Notice** If a request is submitted using the GET method, these parameters are placed in the request section after a question mark (?) in the request URI and connected with ampersands (&).

   ii. Encode the name and value of each request parameter. Perform UTF-8 URL encoding on the names and values of each request parameter. The URL encoding rules are described as follows:
      - Uppercase letters (A-Z), lowercase letters (a-z), digits (0-9), hyphens (-), underscores (_), periods (.), and tildes (~) are not encoded.
      - Extended UTF-8 characters are encoded in the %XY%ZA... format. A space is encoded as %20, rather than the plus sign (+).

        > **Notice** Most libraries that support URL encoding, such as java.net.URLEncoder, comply with the MIME encoding rules of application/x-www-form-urlencoded. If this encoding method is used, replace the plus signs (+) in the encoded strings with %20, the asterisks (*) with %2A, and %7E with a tilde (~) to conform to the encoding rules.

   iii. Connect the encoded parameter names and values with equal signs (=).
   iv. Sort the equal sign-connected strings by their parameter names alphabetically and connect them with ampersands (&).
2. Use the created canonicalized query string to construct a string for signature calculation based on the following rules:

   ```
   StringToSign=
   HTTPMethod + "&" +
   percentEncode("/") + "&" +
   percentEncode(CanonicalizedQueryString)
   ```

   In the preceding example, HTTPMethod indicates the HTTP method that is used to submit a request, such as GET. percentEncode("/") is the encoded value ("%2F") of a forward slash (/). The encoding follows the URL encoding rules described in the previous step. percentEncode(CanonicalizedQueryString) is the string constructed using the canonicalized query string. The encoding follows the URL encoding rules described in the previous step.
3. Use the signature string to calculate the HMAC value of the signature as defined by RFC 2104.

   > **Notice** The key used for signature calculation is your AccessKey Secret with an ampersand (&) added at the end. The corresponding number of an ampersand (&) is 38 in ASCII codes. The string is then hashed with the SHA1 hash algorithm.

4. Encode the HMAC value into a string based on the Base64 encoding rules. This encoded string is the signature value.
5. Add the signature value as the Signature parameter value to the request parameters to complete the request signing process.

> **Notice** When the obtained signature value is submitted to the RDS server as the final request parameter value, the value must undergo URL encoding based on RFC 3986 rules like other parameters.

DescribeCdnService is used here as an example. The request URL before signing is:

```
http://mongodb.example.com/?Timestamp=2016-01-01T10:33:56Z&Format=XML&AccessKeyId=testid
&Action=DescribeInstances&SignatureMethod=HMAC-SHA1&RegionId=region1&SignatureNonce=Nw
DAxvLU6tFE0DVb&Version=2015-12-01&SignatureVersion=1.0
```

The StringToSign placed after the signature is as follows:

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeInstances&Format%3DXML&RegionId%3Dregio
n1&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3DNwDAxvLU6tFE0DVb&SignatureVersion%3
D1.0&Timestamp%3D2013-06-01T10%253A33%253A56Z&Version%3D2015-01-01
```

Assume that the AccessKey ID is testid, the AccessKey Secret is testsecret, and the Key used for HMAC calculation is testsecret&. The calculated signature value is as follows:

BIPOMlu8LXBeZtLQkJTw6iFvw1E=

The signed request URL with the Signature parameter added is as follows:

```
http://mongodb.example.com/?TimeStamp=2016-01-01T10%3A33%3A56Z&Format=XML&AccessKeyI
d=testid&Action=DescribeInstances&SignatureMethod=HMAC-SHA1&RegionId=region1&SignatureN
once=NwDAxvLU6tFE0DVb&SignatureVersion=1.0&Version=2015-12-01&Signature=Pc5WBxxxxxxxx
```

2.10.3. Lifecycle management

2.10.3.1. CreateDBInstance

2.10.3.1.1. Description

- This API supports replica set instances only.
- This API supports both data restoration and instance clone functions.

2.10.3.1.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateDBInstance.
RegionId	String	Yes	The region ID of the instance. It can be up to 50 characters in length. You can call the DescribeRegions operation to query the latest region list.

Parameter	Type	Required	Description
ZoneId	String	No	The zone ID of the instance. You can call the DescribeRegions operation to query the latest zone list.
Engine	String	Yes	The type of the database. Set the value to MongoDB.
EngineVersion	String	Yes	The version of the database. Set the value to 3.2.
StorageEngine	String	No	The storage engine. Valid values: WiredTiger and RocksDB. Default value: WiredTiger.
DBInstanceClass	String	Yes	The specifications of the instance. For more information, see Instance specifications.
DBInstanceStorage	Integer	Yes	The custom storage space. Valid values: 5 to 1000 for ApsaraDB for MongoDB instances. You can only specify this value in 5 GB increments. Unit: GB.
DBInstanceDescription	String	No	The description of the instance. This parameter must be 2 to 256 characters in length. It must start with a letter and can contain letters, digits, underscores (_), and hyphens (-).
SecurityIPList	String	No	The IP addresses in an IP address whitelist. Separate multiple IP addresses with commas (,). You can add a maximum of 1,000 different IP addresses to a whitelist. Supported formats of IP addresses are IP addresses such as %, 0.0.0.0/0 and 10.23.12.24 or Classless Inter-Domain Routing (CIDR) blocks such as 10.23.12.24/24. /24 indicates the length of the IP address prefix. The IP address prefix can consist of 1 to 32 bits. 0.0.0.0/0 indicates that all IP addresses are allowed. Default value: 0.0.0.0/0.
AccountPassword	String	No	The password of the root account. The password must be 6 to 32 characters in length and can contain letters, digits, and underscores (_).
ChargeType	String	No	The billing method of the instance. Valid values: PrePaid and PostPaid. PrePaid: subscription. PostPaid: pay-as-you-go. Default value: PostPaid.
Period	Integer	No	The expiration time of a subscription instance. This parameter must be specified when ChargeType is set to PrePaid. Valid values: 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 24, and 36. Unit: month.

Parameter	Type	Required	Description
ClientToken	String	Yes	The client token that is used to ensure idempotence of the request. The value of this parameter is generated by the client and is unique among different requests. The maximum length is 64 ASCII characters. For more information, see How to ensure idempotence.
NetworkType	String	No	The network type of the instance. Valid values: Classic and VPC. Default value: Classic.
VpcId	String	No	The ID of the VPC. If NetworkType is set to VPC, this parameter is required.
VSwitchId	String	No	The ID of the VSwitch. If NetworkType is set to VPC, this parameter is required.
DBInstanceId	String	No	The ID of the source instance. This parameter can only be specified when this operation is called to clone instances.
BackupId	String	No	The ID of the specified backup set.
RestoreTime	String	No	The time when the cloned instance is restored.

2.10.3.1.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.
DBInstanceId	String	The ID of the instance to be queried.
OrderId	String	The ID of an order.

2.10.3.2. ModifyDBInstanceSpec

2.10.3.2.1. Description

This API supports replica set instances only.

2.10.3.2.2. Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceSpec.
DBInstanceId	String	Yes	The ID of the instance whose configuration is to be modified.
DBInstanceClass	String	No	The specifications of the instance. For more information, see Appendix Instance specifications.
OrderType	String	No	The type of the configuration change. Valid values: UPGRADE and DOWNGRADE. Default value: DOWNGRADE. This parameter is applicable to subscription instances only.
DBInstanceStorage	Integer	No	The storage capacity of the instance. Valid values: 5 to 1,000. Unit: GB. The value can be increased in increments of 5 GB.

2.10.3.2.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.
OrderId	String	The ID of an order.

2.10.3.3. DeleteDBInstance

2.10.3.3.1. Description

This API supports replica set instances only.

2.10.3.3.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteDBInstance.
DBInstanceId	String	Yes	The ID of the instance to be deleted.

2.10.3.3.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.3.4. RenewDBInstance

2.10.3.4.1. Description

This API supports replica set instances only.

2.10.3.4.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RenewDBInstance.
DBInstanceId	String	Yes	The ID of the instance to be renewed.
Period	Integer	Yes	The renewal period of the instance. Valid values: 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 24, and 36.
ClientToken	String	Yes	The token used to guarantee the idempotence of requests.

2.10.3.4.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.
OrderId	String	The ID of an order.

2.10.4. Instance management

2.10.4.1. DescribeRegions

2.10.4.1.1. Description

This API supports replica set instances only.

2.10.4.1.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeRegions.
RegionId	String	No	The ID of the region to be queried.
ZoneId	String	No	The ID of the zone in the target region.

2.10.4.1.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.4.1.3.1. Region data structure

Parameter	Type	Description
RegionId	String	The ID of the region where an instance resides, such as cn-beijing.
Zones	List<Zones>	The list of zones.

2.10.4.1.3.2. Zones

Parameter	Type	Description
ZoneId	String	The ID of the zone, such as cn-beijing-a.
VpcEnabled	String	Indicates whether the VPC is available.

2.10.4.2. DescribeDBInstances

2.10.4.2.1. Description

This API supports replica set instances only.

2.10.4.2.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstances.
RegionId	String	Yes	The ID of the region where an instance resides. You can use the DescribeRegions function to view available regions.
Engine	String	No	The database type of the instance. Valid value: MongoDB.
DBInstanceType	String	No	The queried instance type. Valid values: sharding and replicate. Default value: replicate.
PageSize	Integer	No	The number of records on each page. Valid values: 30, 50, and 100. Default value: 30.
PageNumber	Integer	No	The page number to request, which must be any integer greater than 0. Default value: 1.

2.10.4.2.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.
DBInstances	List<DBInstance>	The array consisting of ApsaraDB for MongoDB instances.

2.10.4.2.3.1. DBInstance data structure

Parameter	Type	Description
DBInstanceId	String	The ID of the instance.
DBInstanceDescription	String	The description of the instance.
RegionId	String	The region ID of the instance.
ZoneId	String	The zone ID of the instance.
Engine	String	The database type of the instance.
EngineVersion	String	The database version of the instance.
DBInstanceClass	String	The specifications of the instance.
DBInstanceStorage	Integer	The storage capacity of the instance.
DBInstanceStatus	String	The status of the instance. For more information, see Instance states.
ChargeType	String	The billing method of the instance. Valid values: PrePaid and PostPaid. PrePaid: subscription. PostPaid: pay-as-you-go.
NetworkType	String	The network type of the instance. Valid values: Classic and VPC.

Parameter	Type	Description
CreationTime	String	The time when the instance was created. The time is in the *yyyy-MM-dd*T*HH:mm:ss*Z format and displayed in UTC.
ExpireTime	String	The time that the instance is scheduled to expire.
DBInstanceType	String	The instance type. Valid values: sharding and replicate.
MongosList	List<Mongos>	The array that consists of mongos nodes.
ShardList	List<Shard>	The array that consists of shard nodes.
LastDowngradeTime	Integer	The time of the last configuration downgrade.

2.10.4.2.3.2. Mongos

Parameter	Type	Description
NodeId	String	The ID of a mongos node.
NodeDescription	String	The description of the mongos node.
NodeClass	String	The specifications of the mongos node.

2.10.4.2.3.3. Shard

Parameter	Type	Description
NodeId	String	The ID of a shard node.
NodeDescription	String	The description of the shard node.
NodeClass	String	The specifications of the shard node.
NodeStorage	Integer	The storage capacity of the shard node.

2.10.4.3. RestartDBInstance

2.10.4.3.1. Description

This API supports replica set instances only.

2.10.4.3.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RestartDBInstance.
DBInstanceId	String	Yes	The ID of the instance to be restarted.

2.10.4.3.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.4.4. ModifyDBInstanceMaintainTime

2.10.4.4.1. Description

This API supports replica set instances only.

2.10.4.4.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceMaintainTime.
DBInstanceId	String	Yes	The ID of the instance for which to modify maintenance time.
StartTime	String	Yes	The start time of the maintenance period.
EndTime	String	Yes	The end time of the maintenance period.

2.10.4.4.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.4.5. ModifyDBInstanceDescription

2.10.4.5.1. Description

This API supports replica set instances only.

2.10.4.5.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifyDBInstanceDescription.
DBInstanceId	String	Yes	The name of the instance.
DBInstanceDescription	String	Yes	The description of the instance. • The description cannot start with http:// or https://. • It must start with a letter. • It must be 2 to 256 characters in length and can contain letters, underscores (_), hyphens (-), and digits.

2.10.4.5.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.4.6. DescribeInstanceAttribute

2.10.4.6.1. Description

This API supports replica set instances only.

2.10.4.6.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceAttribute.
DBInstanceId	String	Yes	The ID of one or more instances to be queried. You can enter a maximum of 30 IDs at a time. Separate multiple IDs by using commas (,).

2.10.4.6.3. Response parameters

2.10.4.6.3.1. DBInstance parameters

Parameter	Type	Description
DBInstanceId	String	The ID of the instance to be queried.
DBInstanceDescription	String	The description of the instance.
RegionId	String	The ID of the region where the instance resides.
ZoneId	String	The ID of the zone to which the instance belongs.
Engine	String	The database type of the instance.
EngineVersion	String	The database version of the instance.
DBInstanceClass	String	The specifications of the instance.
DBInstanceStorage	String	The storage capacity of the instance.

Parameter	Type	Description
DBInstanceStatus	String	The status of the instance. For more information, see Appendix Instance statuses.
ChargeType	String	The billing method of the instance. Valid values: PrePaid and PostPaid.
ReplicaSetName	String	The name of the replica set for the instance.
CreationTime	String	The time when the instance is created.
ExpireTime	String	The time that the instance is scheduled to expire. Pay-As-You-Go instances never expire.
MaintainStartTime	String	The start time of instance maintenance.
MaintainEndTime	String	The end time of instance maintenance.
NetworkType	String	The network type of the instance. Valid values: Classic and VPC.
DBInstanceType	String	The instance type. Valid values: sharding and replicate.
LastDowngradeTime	Integer	The time of the most recent configuration downgrade.

2.10.4.7. DescribeReplicaSetRole

2.10.4.7.1. Description

This API supports replica set instances only.

2.10.4.7.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeReplicaSetRole.

Parameter	Type	Required	Description
DBInstanceId	String	Yes	The ID of the instance to be queried.

2.10.4.7.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.
DBInstanceId	String	The ID of the instance to be queried.
ReplicaSets	List<ReplicaSet>	The list of replica set roles.

2.10.4.7.3.1. ReplicaSetRole data structure

Parameter	Type	Description
ReplicaSetRole	String	The role of the replica set instance node. Valid values: Primary and Secondary.
ConnectionDomain	String	The domain name used to connect the instance.
ConnectionPort	String	The port used to connect the instance.
ExpiredTime String	String	The remaining duration of the classic network address of the current instance. Unit: seconds.
NetworkType	String	The network type of the instance. • VPC • Classic • Public
ReplicaSets	List<ReplicaSet>	A list of roles that belong to the replica set instance node.

2.10.4.8. ModifyDBInstanceNetworkType

2.10.4.8.1. Description

This API supports replica set instances only.

2.10.4.8.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceNetworkType.
DBInstanceId	String	Yes	The ID of the instance for which you want to modify the network type.
RetainClassic	String	No	Indicates whether to retain the classic network endpoint. Valid values: True and False.
ClassicExpiredDays	Integer	No	The retention period of the classic network endpoint. Unit: day. Maximum value: 180. When RetainClassic is set to True, this parameter must be specified.
VpcId	String	No	The ID of the VPC to which the instance belongs. This parameter must be specified if you are changing the network type of an instance from classic network to VPC.
VSwitchId	String	No	The ID of the VSwitch. This parameter must be specified if you are changing the network type of an instance from classic network to VPC.

2.10.4.8.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.4.9. ModifyDBInstanceNetExpireTime

2.10.4.9.1. Description

This API supports replica set instances only.

2.10.4.9.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceNetExpireTime.
DBInstanceId	String	Yes	The ID of the instance for which the endpoint expiration time is to be modified.
ConnectionString	String	Yes	The domain name used to connect to the instance.
ClassicExpendExpiredDays	Integer	Yes	The number of days for which the classic network endpoint is retained.

2.10.4.9.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.5. Account management

2.10.5.1. ResetAccountPassword

2.10.5.1.1. Description

This API supports replica set instances only.

2.10.5.1.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ResetAccountPassword.
DBInstanceId	String	Yes	The ID of the instance.
AccountName	String	Yes	The name of the account.
AccountPassword	String	Yes	The new password. It must be 6 to 32 characters in length and can contain letters, digits, and underscores (_).

2.10.5.1.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.5.2. DescribeAccounts

2.10.5.2.1. Description

This API supports replica set instances only.

2.10.5.2.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeAccounts.

Parameter	Type	Required	Description
DBInstanceId	String	Yes	The ID of the instance to be queried.
AccountName	String	Yes	The name of the account used to access the instance.

2.10.5.2.3. Response parameters

Parameter	Type	Description
Accounts	List<Account>	The array consisting of accounts.

2.10.5.2.3.1. Account data structure

Parameter	Type	Description
DBInstanceId	String	The ID of the instance.
AccountName	String	The name of the account.
AccountStatus	String	The status of the account. Valid values: Unavailable and Available.
AccountDescription	String	The description of the account.

2.10.5.3. ModifyAccountDescription

2.10.5.3.1. Description

This API supports replica set instances only.

2.10.5.3.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyAccountDescription.
DBInstanceId	String	Yes	The ID of the instance.

Parameter	Type	Required	Description
AccountName	String	Yes	The name of the account.
AccountDescription	String	Yes	The description of the account. • The description cannot start with http:// or https://. • It must start with a letter. • It must be 2 to 256 characters in length and can contain letters, digits, underscores (_), and hyphens (-).

2.10.5.3.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.6. Database security management

2.10.6.1. DescribeSecurityIps

2.10.6.1.1. Description

This API supports replica set instances only.

2.10.6.1.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSecurityIps.
DBInstanceId	String	Yes	The ID of the instance to be queried.

2.10.6.1.3. Response parameters

Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see Common response parameters.
SecurityIps	String	The default whitelist.
SecurityIpGroups	List<SecurityIpGroup>	The list of IP address groups.

SecurityIpGroup parameters

Parameter	Type	Description
SecurityIpGroupName	String	The name of the IP whitelist.
SecurityIpList	String	The list of IP addresses.
SecurityIpAttribute	String	The attribute of the IP whitelist. The default value is an empty string.

2.10.6.2. ModifySecurityIps

2.10.6.2.1. Description

This API supports replica set instances only.

2.10.6.2.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifySecurityIps.
DBInstanceId	String	Yes	The ID of the instance.

Parameter	Type	Required	Description
SecurityIps	String	Yes	The IP addresses in an IP address whitelist. Separate multiple IP addresses with commas (,). You can add a maximum of 1,000 different IP addresses to a whitelist. Supported formats of IP addresses are IP addresses such as 0.0.0.0/0 and 10.23.12.24, or Classless Inter-Domain Routing (CIDR) blocks such as 10.23.12.24/24. /24 indicates the length of the IP address prefix. The IP address prefix can consist of 1 to 32 bits.
ModifyMode	String	Yes	The modification mode. Valid values: - Cover, - Add, and - Delete.
SecurityIpGroupName	String	No	The name of the group to be modified. Default value: default.
SecurityIpGroupAttribute	String	No	The attribute of the IP address group. Default value: null.

2.10.6.2.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.6.3. DescribeAuditRecords

2.10.6.3.1. Description

This API supports replica set instances only.

2.10.6.3.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeAuditRecords.
DBInstanceId	String	Yes	The ID of the instance.
NodeId	String	No	The ID of mongos or shard. If this parameter is not specified, no result is returned. You do not need to specify this parameter for nodes of replica set instances.
StartTime	String	Yes	The beginning of the time range to query. Specify the time in the *yyyy-MM-dd*T*HH:mm:ss*Z format. The time must be in UTC.
EndTime	String	Yes	The end of the time range to query. Specify the time in the *yyyy-MM-dd*T*HH:mm:ss*Z format. The time must be in UTC.
Database	String	No	The database to be queried. By default, all databases are queried.
User	String	No	The username to be queried. By default, all users are queried.

Parameter	Type	Required	Description
Form	String	No	The file or stream to be downloaded. If you set this parameter to File, only common parameters are returned. In this case, you need to call the DescribeSQLLogFiles operation to obtain the final URL to download the file. If you set this parameter to Stream, the data stream is returned. Default value: Stream.
QueryKeywords	String	No	The keywords used for a query. Use spaces to separate multiple keywords. You can specify a maximum of 10 keywords.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30.
PageNumber	Integer	No	The number of the page to return. Valid values: any non-zero positive integer. Default value: 1.

2.10.6.3.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see Common response parameters.
TotalRecordCount	Integer	The total number of entries.
PageNumber	Integer	The number of the current page.
PageRecordCount	Integer	The number of SQL logs on the current page.
Items	List<SQLRecord>	The array that consists of SQLRecord data.

Parameter	Type	Description
TotalRecordCount	Integer	The total number of entries.

SQLRecord parameters

Parameter	Type	Description
DBName	String	The name of the database.
AccountName	String	The name of the account.
HostAddress	String	The IP address of the client.
Syntax	String	The executed statement.
TotalExecutionTimes	Long	The amount of time taken to execute the operation. Unit: microseconds.
ReturnRowCounts	Long	The number of entries returned.
ExecuteTime	String	The execution time. The time is in the *yyyy-MM-dd*T*HH:mm:ss*Z format and displayed in UTC.
ThreadID	String	The ID of the thread.
Node	String	The node on which the statement is executed. If you specify this parameter, the information about primary and secondary nodes is returned for a replica set instance, while for a sharded cluster instance the information about each mongos is returned.

2.10.6.4. DescribeAuditFiles

2.10.6.4.1. Description

This API supports replica set instances only.

2.10.6.4.2. Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeAuditFiles.
DBInstanceId	String	Yes	The ID of the instance for which to describe audit files.
NodeId	String	No	The ID of a mongos or shard node in a sharded cluster instance. If this parameter is not specified, both a mongos ID and a shard ID are displayed. This parameter cannot be used for replica set instances.

2.10.6.4.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see Common parameters.
TotalRecordCount	Integer	The total number of records.
PageNumber	Integer	The number of the current page.
PageRecordCount	Integer	The number of records on the current page.
Items	List<LogFile>	An array that consists of LogFile data.

LogFile parameters

Parameter	Type	Description
FileID	Integer	The ID of the file.
DBInstanceId	String	The name of the instance.

Parameter	Type	Description
LogStatus String	String	Success: The log file is archived. - Failed: The log file failed to be archived. - Generating: The log file is being archived. - Initializing: Log archiving has not started yet.
LogStartTime	String	The beginning of the time range where the log audit was executed.
LogEndTime	String	The end of the time range where the log audit was executed.
LogDownloadURL	String	The URL to download audit logs. If the download URL is unavailable, this parameter will be empty.
LogSize	Long	The size of the audit log file. Unit: Byte.

2.10.7. Backup and restoration management

2.10.7.1. DescribeBackupPolicy

2.10.7.1.1. Description

This API supports replica set instances only.

2.10.7.1.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeBackupPolicy.
DBInstanceId	String	Yes	The ID of the instance for which to describe the backup policy.

2.10.7.1.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see Common parameters.
BackupRetentionPeriod	String	The number of days for which backup files can be retained.
PreferredBackupTime	String	The period of time to execute backup. The format is HH:mmZ-HH:mm Z.
PreferredBackupPeriod	String	The time cycle to execute backup. Valid values: • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday

2.10.7.2. ModifyBackupPolicy

2.10.7.2.1. Description

This API supports replica set instances only.

2.10.7.2.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to ModifyBackupPolicy.
DBInstanceId	String	Yes	The ID of the instance.
PreferredBackupTime	String	Yes	The period of time to execute backup. Specify the time in the HH:mmZ-HH:mmZ format.

Parameter	Type	Required	Description
PreferredBackupPeriod	String	Yes	The time cycle to execute backup. Valid values: • Monday • Tuesday • Wednesday • Thursday • Friday • Saturday • Sunday

2.10.7.2.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.7.3. CreateBackup

2.10.7.3.1. Description

This API supports replica set instances only.

2.10.7.3.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateBackup.
DBInstanceId	String	Yes	The ID of the instance for which to create a backup.

2.10.7.3.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

Parameter	Type	Description
BackupId	String	The ID of a backup.

2.10.7.4. DescribeBackups

2.10.7.4.1. Description

This API supports replica set instances only.

2.10.7.4.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeBackups.
DBInstanceId	String	Yes	The ID of the instance to be queried.
StartTime	String	Yes	The start time of data returned by a query. The format is YYYYMM-DD'T'HH:mmZ. Example: 2011-06-11T15:00Z.
EndTime	String	Yes	The end time of data returned by a query. The format is YYYYMM-DD'T'HH:mmZ. Example: 2011-06-11T16:00Z.
BackupId	Integer	No	The ID of a backup.
NodeId	String	No	The ID of a shard node. This parameter applies only to sharded cluster instances.
PageSize	Integer	No	The number of records on each page. Valid values: 30, 50, and 100. Default value: 30.

Parameter	Type	Required	Description
PageNumber	Integer	No	The page number to request, which must be any integer greater than 0. Default value: 1.

2.10.7.4.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see Common response parameters.
Items	List<Backup>	The array that consists of backups.
PageNumber	Integer	The number of the returned page.
TotalCount	Integer	The total number of backups.
PageSize	Integer	The number of entries returned per page.

Backup data structure

Parameter	Type	Description
BackupDBNames (TBD)	String	The list of databases in a backup set. Separate multiple databases with commas (,), such as "Db1,Db2,Db3...". It is used to check whether a full backup is performed.
BackupId	Integer	The ID of a backup.
BackupStatus	String	The status of the backup task. Valid values: • Success: The backup task is completed. • Failed: The backup task fails.
BackupStartTime	String	The beginning of the backup time range. The time is in the *yyyy-MM-dd*T*HH:mm:ss*Z format and displayed in UTC.

Parameter	Type	Description
BackupEndTime	String	The end of the backup time range. The time is in the *yyyy-MM-dd*T*HH:mm:ss*Z format and displayed in UTC.
BackupType	String	The type of the backup. Valid values: • FullBackup • IncrementalBackup
BackupMode	String	The backup mode. Valid values: • Automated: indicates an automatic backup. • Manual: indicates a manual backup.
BackupMethod	String	The method of the backup. Valid values: • Logical • Physical
BackupDownloadURL	String	The download URL of the backup file. If the download URL is unavailable, the value is an empty string.
BackupSize	Long	The size of the backup file. Unit: Byte.

2.10.7.5. RestoreDBInstance

2.10.7.5.1. Description

This API supports replica set instances only.

2.10.7.5.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to RestoreDBInstance.
DBInstanceId	String	Yes	The ID of the instance to be queried. Only replica set instances are supported.

Parameter	Type	Required	Description
BackupId	String	Yes	The ID of a backup.

2.10.7.5.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see the "Common response parameters" topic.

2.10.8. Performance monitoring management

2.10.8.1. DescribeDBInstancePerformance

2.10.8.1.1. Description

This API supports replica set instances only.

2.10.8.1.2. Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstancePerformance.
DBInstanceId	String	Yes	The ID of the instance.
StartTime	String	Yes	The beginning of the time range to query. Specify the time in the *yyyy-MM-dd*T*HH:mm:ss*Z format. The time must be in UTC.
EndTime	String	Yes	The end of the time range to query. Specify the time in the *yyyy-MM-dd*T*HH:mm:ss*Z format. The time must be in UTC.

Parameter	Type	Required	Description
ReplicaSetRole	String	Yes	The role of a replica set. Valid values: Primary and Secondary.
Key	String	Yes	The monitoring metrics for database performance. Separate multiple metrics with commas (,). For more information about the metrics, see Performance metrics.

2.10.8.1.3. Response parameters

Parameter	Type	Description
Common response parameters	-	For more information, see Common response parameters.
DBInstanceId	String	The ID of the instance.
Engine	String	The database type of the instance.
StartTime	String	The beginning of the time range to query. The time is in the *yyyy-MM-dd*T*HH:mm:ss*Z format and displayed in UTC.
EndTime	String	The end of the time range to query. The time is in the *yyyy-MM-dd*T*HH:mm:ss*Z format and displayed in UTC.
PerformanceKeys	List<PerformanceKey>	The array that consists of performance metrics. It is in the {perf1, perf2, perf3, ...} format.

PerformanceKey parameters

Parameter	Type	Description
Key	String	The name of a metric.
Unit	String	The unit of a metric.

Parameter	Type	Description
ValueFormat	String	The format of a value. • If a value is null, VALUE will be returned. • If multiple metrics return in the parameter value, these metrics will be separated with ampersands (&), such as com_delete&com_insert&com_insert_select&com_replace.
Values	List<PerformanceValue>	The array that consists of the metric values. It is in the {value1, value2, ...} format.

PerformanceValue parameters

Parameter	Type	Description
Value	String	The value of a metric.
date	String	The calculation time. The time is in the *yyyy-MM-dd*T*HH:mm:ss*Z format and displayed in UTC.

2.10.9. Appendix

2.10.9.1. Error codes

Description	Error code	Error message	HTTP status code
The error message returned because RAM users are not authorized to call the API.	Forbidden.RAM	User not authorized to operate on the specified resource, or this API doesn't support RAM.	403
The error message returned because this operation is not allowed in RAM mode.	Forbedden.NotSupport RAM	This action does not support accessed by RAM mode.	403
The error message returned because an exception occurred on the server.	ServiceUnavailable	The request has failed due to a temporary failure of the server.	503

Description	Error code	Error message	HTTP status code
The error message returned because the specified instance status does not exist.	InvalidStatus.NotFound	The Status provided does not exist in our records.	404
The error message returned because the specified parameter is invalid	InvalidParameter	The specified parameter "InstanceName" is not valid.	400
The error message returned because you are not authorized to call the administrator-specific API.	Forbbiden.NotAdminUser	User not authorized to operate on the specified API as you are not the administrator.	403
The error message returned because a required parameter is not specified.	MissingParameter	Specified parameter is missing.	400
The error message returned because neither of the InstanceName and NewPassword parameters is specified.	MissingParameter	InstanceName/NewPassword at least one is mandatory for this action.	400
The error message returned because the required OwnerId parameter is not specified for this operation.	MissingParameter	The input parameter OwnerId,OwnerAccount that is mandatory for processing this request is not supplied.	403
The error message returned because the specified Token parameter is invalid.	InvalidToken.Malformed	The Specified parameter \" Token\" is not valid.	400
The error message returned because the specified InstanceName parameter is invalid.	InvalidInstanceName.Malformed	The Specified parameter \" InstanceName\" is not valid.	400
The error message returned because the specified Password parameter is invalid.	InvalidPassword.Malformed	The Specified parameter \" Password\" is not valid."	400

Description	Error code	Error message	HTTP status code
The error message returned because the specified Instances parameter is invalid.	InvalidInstances.Malformed	The Specified parameter \" Instances\" is not valid.	400
The error message returned because the specified StartTime parameter is invalid.	InvalidStartTime.Malformed	The Specified parameter \" StartTime\" is not valid.	400
The error message returned because the specified EndTime parameter is invalid.	InvalidEndTime.Malformed	The Specified parameter \" EndTime\" is not valid.	400
The error message returned because the specified InstanceIds parameter is invalid.	InvalidInstanceIds.Malformed	The Specified parameter \" InstanceIds\" is not valid.	400
The error message returned because your balance is insufficient to perform the current operation.	InsufficientBalance	Your account does not have enough balance.	400
The error message returned because your account fails to pass real-name verification.	RealNameAuthenticationError	Your account has not passed the real-name authentication yet.	403
The error message returned because the purchase amount exceeds the limit for each subscription.	QuotaExceed	Living afterpay instances quota exceeded.	400
The error message returned because the capacity configuration is invalid.	InvalidCapacity.NotFound	The Capacity provided does not exist in our records.	400
The error message returned because the two specified requests use the same ClientToken.	IdempotentParameterMismatch	Request uses a client token in a previous request but is not identical to that request.	400
The error message returned because the available inventory in the specified zone is insufficient.	QuotaNotEnough	Quota not enough in this zone.	400

Description	Error code	Error message	HTTP status code
The error message returned because you are not authorized to call the subscription service API.	Forbbiden.SubUser	The specified action is not available for you.	403
The error message returned because the Alibaba Cloud risk control system rejects this access request.	Forbidden.RiskControl	This operation is forbidden by Aliyun Risk Control system.	403
The error message returned because the specified region ID does not exist.	InvalidRegion.NotFound	The RegionId or ZoneId provided does not exist in our records.	404
The error message returned because the specified ZoneId parameter is invalid.	InvalidZoneId.NotFound	The ZoneId provided is invalid.	400
The error message returned because the specified instance ID does not exist.	InvalidInstanceId.NotFound	The InstanceId provided does not exist in our records.	404
The error message returned because the provided password is incorrect.	IncorrectPassword	The Password provided is not correct.	400
The error message returned because the service is unavailable.	ServiceNotSupported	The specified service is not supported.	400
The error message returned because this instance has a subscription renewal order that has not gone into effect.	HasRenewChangeOrder	This instance has a renewChange order.	400
The error message returned because an internal error occurs.	InternalError	The request processing has failed due to some unknown error.	500
The error message returned because the specified backup time is invalid.	InvalidPreferredBackupTime	Specified preferred backup time is not valid.	400

Description	Error code	Error message	HTTP status code
The error message returned because the specified backup type is invalid.	InvalidBackupType.Format	Specified backup type is not valid.	400
The error message returned because the specified backup method is invalid.	InvalidBackupMethod.Format	Specified backup method is not valid.	400
The error message returned because the backup task already exists.	BackupJobExists	A backup job already exists in the specified DB instance.	400
The error message returned because the maximum number of daily backup operations has been reached.	BackupTimesExceeded	Exceeding the daily backup times of this DB instance.	400
The error message returned because no parameters are specified.	ParameterLeastAssociate	Must input at least one optional parameter.	400
The error message returned because the specified backup retention period is invalid.	InvalidBackupRetentionPeriod.Malformed	Specified backup retention period is not valid.	400
The error message returned because the specified next backup time is invalid.	InvalidPreferredBackupTime.Format	Specified preferred backup time is not valid.	400
The error message returned because the specified backup period is invalid.	InvalidPreferredBackupPeriod.Malformed	Specified backup period is not valid.	400
The error message returned because the current instance type does not support this operation.	IncorrectDBInstanceType	Current DB instance type does not support this operation.	400
The error message returned because the specified key is invalid.	InvalidKey.Malformed	Specified key is not valid.	400

Description	Error code	Error message	HTTP status code
The error message returned because the signature nonce requested has already been used and cannot be used again.	SignatureNonceUsed	Specified signature nonce was used already.	400
The error message returned because no available virtual IP addresses can be allocated.	AllocateVpcIp.NotEnough	Ip resource is not enough	400
The error message returned because the current zone does not support instances of the specified type.	Zone.NotSupport	Specified zone does not support creating with instance class.	400
The error message returned because the instance type is invalid.	MissingClassCode	Capacity or InstanceClass is mandatory for this action.	400
The error message returned because the specified instance type is not supported.	InvalidDBInstanceClass.NotFound	Specified DB instance class is not found.	404
The error message returned because the instance is locked.	IncorrectDBInstanceLockMode	Current DB instance lock mode does not support this operation.	400
The error message returned because the specified backup set ID does not exist.	InvalidBackupSetID.NotFound	Specified backup set ID does not exist.	400
The error message returned because the instance is in a state that does not support the current operation.	IncorrectDBInstanceState	Current DB instance state does not support this operation.	400
The error message returned because the available capacity in the specified instance is insufficient.	InsufficientResourceCapacity	There is insufficient capacity available for the requested instance.	400
The error message returned because the specified end time is invalid.	InvalidEndTime.Format	Specified end time is not valid.	400

Description	Error code	Error message	HTTP status code
The error message returned because the specified retention period of the classic network endpoint is invalid.	InvalidClassicExpiredDays.Format	The specified classicExpiredDays format is not valid.	400
The error message returned because the backup set is in a state that does not support the current operation.	IncorrectBackupSetState	Current backup set state does not support operations.	400
The error message returned because the specified whitelist format is invalid.	InvalidSecurityIPList.Format	Specified security IP list format is not valid.	400

2.11. AnalyticDB for PostgreSQL

2.11.1. API reference

2.11.1.1. List of operations by function

Instance management

Operation	Description
CreateDBInstance	Creates an instance.
DeleteDBInstance	Deletes an instance.
DescribeDBInstanceAttribute	Lists all attributes of an instance.
DescribeDBInstances	Returns a list of instances.
DescribeRegions	Returns a list of available regions and zones.
DescribeResourceUsage	Returns the resource usage of an instance.
ModifyDBInstanceConnectionMode	Modifies the connection mode of an instance.
ModifyDBInstanceDescription	Modifies the description of an instance.
ModifyDBInstanceMaintainTime	Modifies the maintenance period of an instance.
RestartDBInstance	Restarts an instance.
DescribeDBInstancePerformance	Returns the performance data of an instance.

Database management

Operation	Description
DeleteDatabase	Deletes a database.
DescribeAccounts	Returns the account information of a database.
ModifyAccountDescription	Modifies the description of a database.

Account management

Operation	Description
CreateAccount	Creates an account.
ResetAccountPassword	Resets the password of an account.

Security management

Operation	Description
DescribeDBInstanceIPArrayList	Returns a whitelist of IP addresses that are allowed to access an instance.
ModifySecurityIps	Modifies the whitelist of IP addresses.

Log management

Operation	Description
DescribeSlowLogRecords	Returns the details of a slow query log.
DescribeSQLCollectorPolicy	Checks the SQL collection status.
DescribeSQLLogFiles	Returns a list of SQL audit files.
DescribeSQLLogRecords	Returns a SQL audit log for an instance.
ModifySQLCollectorPolicy	Modifies the SQL collection status for an instance.

Network management

Operation	Description
AllocateInstancePublicConnection	Allocates a public network connection string for an instance.
DescribeDBInstanceNetInfo	Returns the network connection information of an instance.

Operation	Description
ModifyDBInstanceConnectionString	Modifies the connection string and the port.
ModifyDBInstanceNetworkType	Switches the network connection type of an instance.
ReleaseInstancePublicConnection	Releases the public connection string of an instance.

2.11.1.2. Request structure

To make an API call is to send an HTTP GET request to the API server with request parameters based on the description of the corresponding API operation. The processing results are returned in the response.

Endpoints

The endpoint of the AnalyticDB for PostgreSQL API is gpdb.example.com.

For more information about how to obtain the endpoint, see Obtain an endpoint.

Protocols

You can send requests over HTTP or HTTPS. To ensure higher security, we recommend that you send operation requests over HTTPS. Some password-related operations only support HTTPS.

Methods

The system allows you to send HTTP GET requests. This requires request parameters to be included in the request URL.

Parameters

When you make an API request, you must specify the Action parameter as the operation, such as CreateDBInstance, that you want to perform. You must also specify common request parameters and the request parameters specific to this operation.

Encoding

Requests and responses are encoded by using the UTF-8 character set.

2.11.1.3. Common parameters

Common request parameters

Common request parameters must be included in each API request.

Common request parameters

Parameter	Type	Required	Description
Format	String	No	The format of the response. Valid values: JSON and XML. Default value: XML.

Parameter	Type	Required	Description
Version	String	Yes	The version of the API. Specify the version in the YYYY-MM-DD format. The current version is 2018-07-23.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The result string of the signature. For more information about the signature calculation method, see Request signatures.
SignatureMethod	String	Yes	The method of signature. HMAC-SHA1 is supported.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard and it must be in UTC. The format is: `YYYY-MM-DDThh:mm:ssZ` For example, 2013-01-10T12:00:00Z indicates 20:00:00, January 10, 2013, China Standard Time (UTC+8).
SignatureVersion	String	Yes	The version of the signature algorithm. The current version is 1.0.
SignatureNonce	String	Yes	A unique random number that is used to prevent network replay attacks. You must use different random numbers for different requests.

Examples

```
https://gpdb.example.com/
? Format=xml
&Version=2013-08-15
&Signature=Pcxxxxxxxxxxxxxxxxxxxxxxx
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2013-06-01T12:00:00Z
```

Common response parameters

Each time you call an operation, the system returns a globally unique ID (RequestId), regardless of whether the request is successful.

Example:

```
<? xml version="1.0" encoding="utf-8"? >
<!—The root node of the response-->
<API name + Response>
 <!—The returned request tag-->
 <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
 <!—The returned result-->
</API name + Response>
```

2.11.1.4. Responses

After the operation is called, data is returned in a unified format. A returned HTTP status code of 2xx indicates that the call was successful. A returned HTTP status code of 4xx or 5xx indicates that the call failed.

For a successful call, the formats of returned data are XML and JSON. When a request is sent, an external system can customize parameters to specify the format of data to be returned. The default format is XML. The response examples in this topic are formatted with line breaks or indents for a clear view. Actual response data is not formatted in the same manner as these examples.

Sample success responses

XML format

The XML response includes a message that indicates whether the request is successful and the specific service data. Example:

```
<? xml version="1.0" encoding="utf-8"? >
<!—The root node of the response-->
<API name + Response>
   <!—The returned request tag-->
 <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
   <!—The returned result-->
</API name + Response>
```

JSON format

```
{
   "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
   /*The returned result*/
}
```

Sample error responses

No result is returned after the API call fails. You can locate the cause of the error by referring to the appendix.

When a request failed, an HTTP response containing an HTTP status code (4xx or 5xx) is returned. The returned message body contains the specific error code and error message. The message body also contains a globally unique RequestId and the HostId of the site you request to access. If you are unable to find the error cause, you can contact Alibaba Cloud customer service and provide the HostId and RequestId to help solve the problem as quickly as possible.

XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<Error>
  <RequestId>8906582E-6722-409A-A6C4-0E7863B733A5</RequestId>
  <HostId>gpdb.example.com</HostId>
  <Code>UnsupportedOperation</Code>
  <Message>The specified action is not supported. </Message>
</Error>
```

JSON format

```
{
   "RequestId": "7463B73D-35CC-4D19-A010-6B8D65D242EF",
   "HostId": "gpdb.example.com",
   "Code": "UnsupportedOperation",
   "Message": "The specified action is not supported."
}
```

2.11.1.5. Request signatures

AnalyticDB for PostgreSQL authenticates each access request. Therefore, each request sent over HTTP or HTTPS must contain signature information. AnalyticDB for PostgreSQL performs symmetric encryption by using the AccessKey ID and AccessKey Secret to verify the identity of request senders. The AccessKey ID and AccessKey Secret are officially issued to you by Alibaba Cloud. You can apply for and manage them on the Alibaba Cloud official website. The AccessKey ID is used to confirm the identity of the user.The AccessKey Secret is the key used to encrypt signature strings and used by the server to verify the signature strings. The AccessKey must be kept confidential.

For more information about how to obtain the AccessKey pair, see Obtain an AccessKey pair.

Follow these steps to sign an access request:

1. Use request parameters to construct a canonicalized query string.

i. To construct a canonicalized query string, sort all request parameters by name in alphabetic order. These parameters include common request parameters and customized API request parameters, but do not include the Signature parameter.

> **Note** When you use the GET method to submit requests, these parameters constitute the parameter field of the request URI following the question mark (?) and connected by the ampersand (&).

ii. Encode the name and value of each request parameter. Perform URL encoding on the names and values by using the UTF-8 character set. The URL encoding rules are as follows:

- Uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), hyphens (-), underscores (_), periods (.), and tildes (~) are not encoded.
- Encode other characters in the format of %XY. XY represents the ASCII code in hexadecimal notation of the characters. For example, double quotation marks (") are encoded as %22.
- Extended UTF-8 characters are encoded in the %XY%ZA... format.
- Encode the space as %20 rather than the plus sign (+).

> **Note** Libraries that support URL encoding (such as java.net.URLEncoder in Java) are encoded based on the rules for the application/x-www-form-urlencoded of the MIME type. If this encoding method of the MIME type is used, replace the plus signs (+) in the encoded strings with %20, the asterisks (*) with %2A, and %7E with a tilde (~) to conform to the preceding encoding rules.

iii. Connect the encoded parameter name and value by using an equal sign (=).

iv. Sort the parameter name and value pairs connected by equal signs (=) in alphabetical order and connect the pairs with ampersands (&).

2. Use the created canonicalized query string to construct a string for signature calculation based on the following rules:

```
StringToSign= HTTPMethod + "&" + percentEncode("/") + "&" +
percentEncode(CanonicalizedQueryString)
```

HTTPMethod specifies an HTTP-style request such as GET.

percentEncode("/") specifies the encoded value for the character "/" according to the URL encoding rules described in step 1.b, that is %2F.

percentEncode(CanonicalizedQueryString) specifies the encoded string of the canonicalized query string constructed in step 1, produced by following the URL encoding rules described in step 1.b.

3. As defined in RFC 2104, the preceding signature string is used to calculate the HMAC value of the signature.

> **Note** The key used for signature calculation is your AccessKey Secret. An ampersand (&) (38 in ASCII codes) is added to the end of the key. The SHA-1 hashing algorithm is used.

4. Encode the preceding HMAC value as a Base64 string to obtain the signature value.
5. Add the signature value to the request parameters as the signature parameter. The request signing process is completed.

> **Note**
>
> When the obtained signature value is submitted to the AnalyticDB for PostgreSQL server as the final request parameter value, the URL encoding must be performed for the value in compliance with the RFC 3986 rules. Take DescribeDBInstances as an example, the request URL before signing is:
>
> ```
> http://gpdb.example.com/?Timestamp=2013-06-01T10:33:56Z&Format=XML&Acce ssKeyId=testi
> d&Action=DescribeDBInstances&SignatureMethod=HMAC-SHA1&Regi onId=region1&SignatureN
> once=NwDAxvLU6tFE0DVb&Version=2014-08-15&Signatur eVersion=1.0
> ```
>
> The calculated StringToSign is:
>
> ```
> GET&%2F&AccessKeyId%3Dtestid%26Action%DescribeDBInstances%26Format%3DXML %26Regio
> nId%3Dregion1%26SignatureMethod%3DHMAC-SHA1%26SignatureNonce%3DN wDAxvLU6tFE0DV
> b%26SignatureVersion%3D1.0%26Timestamp%3D2013-06-01T10%253 A33%253A56Z%26Version%
> 3D2014-08-15
> ```
>
> Assume that the AccessKey ID is testid, the AccessKey Secret is testsecret, and the key used to calculate the HMAC value is testsecret&. The calculated signature value is:
>
> GfQRtWbwdE8sp7q9lBgZyutVht8=
>
> The signed request URL with the Signature parameter added is as follows:
>
> ```
> http://gpdb.example.com/?Timestamp=2012-12-26T10%3A33%3A56Z&Format=XML& AccessKeyI
> d=testid&Action=DescribeDBInstances&SignatureMethod=HMAC-SHA1& RegionId=region1&Sign
> atureNonce=NwDAxvLU6tFE0DVb&Version=2012-09-13&Sign atureVersion=1.0&Signature= Gfxxx
> xxxxxxxxxxxxxxxx
> ```

2.11.1.6. RAM authorization

2.11.1.6.1. Use RAM to authorize resources

All instances created through an Apsara Stack tenant account are resources owned by that account. An account has the full operation permissions on resources under the account by default.

Resource Access Management (RAM) allows you to grant RAM users the access and management permissions on resources owned by an Apsara Stack tenant account.

> **Note** If you do not need to use RAM, skip this procedure.

2.11.1.6.2. Resources that can be authorized in RAM

Only one type of AnalyticDB for PostgreSQL resource can be authorized in RAM: DBInstance.

The following table lists the descriptions of resources when you use RAM to authorize access permissions to these resources:

Resource description

Resource	Resource description in the authorization policy
DBInstance	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid acs:gpdb:$regionid:$accountid:dbinstance/* acs:gpdb:* : *:dbinstance/*

> **Note**
>
> - All $regionids must be the ID of a region or *.
> - All $instanceids must be the ID of an instance or *.
> - All $accountid must be the ID of a resource owner or *.

2.11.1.6.3. Operations that can be authorized in RAM

You can use RAM to authorize access permissions to AnalyticDB for PostgreSQL resources. All operations except the DescribeRegions operation can be authorized.

2.11.1.6.4. Authentication rules of API operations

When you call API operations to access resources as a RAM user, AnalyticDB for PostgreSQL checks whether the RAM user is granted the required permissions by querying Resource Access Management (RAM).

When you call API operations to access resources as a RAM user, AnalyticDB for PostgreSQL checks with RAM whether you are granted the required permissions. The permissions to be checked are determined by the resources used by the API operation. For more information about authentication rules for each API operation, see Authentication rules of API operations.

Authentication rules of API operations

Operation	Authentication rule
CreateDBInstance	acs:gpdb:$regionid: dbinstance /$*
DeleteDBInstance	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeDBInstanceAttribute	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeDBInstances	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid

Operation	Authentication rule
DescribeRegions	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeResourceUsage	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
ModifyDBInstanceConnectionMode	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
ModifyDBInstanceDescription	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
ModifyDBInstanceMaintainTime	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
RestartDBInstance	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DeleteDatabase	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeAccounts	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
ModifyAccountDescription	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
CreateAccount	acs:gpdb:$regionid: dbinstance /$*
ResetAccountPassword	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeDBInstanceIPArrayList	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeDBClusterIPArrayList	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
ModifySecurityIps	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeSlowLogRecords	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeSQLCollectorPolicy	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeSQLLogFiles	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid
DescribeSQLLogRecords	acs:gpdb:$regionid: $accountid:dbinstance/$dbinstanceid

Operation	Authentication rule
ModifySQLCollectorPolicy	acs:gpdb:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeDBInstancePerformance	acs:gpdb:$regionid:$accountid:dbinstance/$dbinstanceid
AllocateInstancePublicConnection	acs:gpdb:$regionid:$accountid:dbinstance/$dbinstanceid
DescribeDBInstanceNetInfo	acs:gpdb:$regionid:$accountid:dbinstance/$dbinstanceid
ReleaseClusterPublicConnection	acs:gpdb:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyDBInstanceConnectionString	acs:gpdb:$regionid:$accountid:dbinstance/$dbinstanceid
ModifyDBInstanceNetworkType	acs:gpdb:$regionid:$accountid:dbinstance/$dbinstanceid
ReleaseInstancePublicConnection	acs:gpdb:$regionid:$accountid:dbinstance/$dbinstanceid

2.11.1.7. Instance management

2.11.1.7.1. CreateDBInstance

Description

You can call this operation to create an instance of AnalyticDB for PostgreSQL.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	CreateDBInstance
RegionId	String	Yes	Specifies a region for the instance, such as cn-hangzhou. For more information about available regions, see the DescribeRegions operation.

Parameter	Type	Required	Description
ZoneId	String	Yes	Specifies a zone for the instance, such as cn-hangzhou-d. For more information about available zones, see the DescribeRegions operation.
InstanceNetworkType	String	Yes	The network type of the instance. Valid values: Classic and VPC. Default value: Classic.
VPCId	String	No	The ID of the VPC. If you set InstanceNetworkType to VPC, you must also specify the VPCId parameter. The specified region of the VPC must be the same as RegionId.
VSwitchId	String	No	The ID of the VSwitch. If you set InstanceNetworkType to VPC, you must also specify the VSwitchId parameter. The specified zone of the VSwitch must be the same as ZoneId.
DBInstanceClass	String	Yes	The type of the instance. For more information, see Instance types.
DBInstanceGroupCount	String	Yes	The number of compute groups in the AnalyticDB for PostgreSQL instance.
DBInstanceDescription	String	No	The description of the instance. The description cannot exceed 256 characters in length.

Parameter	Type	Required	Description
SecurityIPList	String	No	The IP addresses that are allowed to access the instance. Default value: `127.0.0.1`.
ClientToken	String	Yes	The client token that is used to perform idempotence check.

Response parameters

Parameter	Type	Description
<Common response parameters>	String	For more information, see Common response parameters.
DBInstanceId	String	The ID of the instance.
OrderId	String	The ID of the order.

Sample requests

```
https://gpdb.example.com/?Action=CreateDBInstance
&Engine=gpdb
&RegionId=cn-hangzhou
&ZoneId=cn-hangzhou-b&PayType=Postpaid
&InstanceNetworkType=Classic
&DBInstanceClass=gpdb.group.segsdx1
&DBInstanceGroupCount=2
&ClientToken=f918f59c-89be-42ee-bb86-d027243b2cfb
&<Common request parameters>
```

Sample responses

XML format

```
<CreateDBInstanceResponse>
 <dbInstanceId>gp-xxxxxxxxxxxxxx</dbInstanceId>
 <orderId>xxxxxxxxxxxxxx</orderId>
</CreateDBInstanceResponse>
```

JSON format

```
{
   "dbInstanceId":"gp-xxxxxxxxxxxxxx",
   "orderId":xxxxxxxxxxxxxx
}
```

2.11.1.7.2. DeleteDBInstance

Description

You can call this operation to delete an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DeleteDBInstance.
DBInstanceId	String	Yes	The ID of the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=DeleteDBInstance
&DBInstanceId=gp-xxxxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<DeleteDBInstanceResponse>
    <RequestId>65BDA532-28AF-4122-AA39-B382721EEE64</RequestId>
</DeleteDBInstanceResponse>
```

JSON format

{"RequestId":" 65BDA532-28AF-4122-AA39-B382721EEE64"}

2.11.1.7.3. DescribeDBInstanceAttribute

Description

You can call this operation to query the details of an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceAttribute.
DBInstanceId	String	Yes	The ID of the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Items	List<DBInstanceAttribute>	The list of instance details.

DBInstanceAttribute parameters

Parameter	Type	Description
AvailabilityValue	String	The service availability of the current instance. Unit: %.
ConnectionMode	String	• Performance: standard mode • Safty: safe mode
ConnectionString	String	The connection string to connect to the database.
CreationTime	String	The time when you create an instance. It is in the `YYYY-MM-DDThh:mm:ssZ` format, such as 2011-05-30T12:11:4Z.

Parameter	Type	Description
DBInstanceClass	String	The type of the instance.
DBInstanceClassType	String	The instance family. Valid values: • s: shared instances • x: general-purpose instances • d: dedicated instances • h: dedicated-host instances
DBInstanceCpuCores	String	The number of CPU cores.
DBInstanceDescription	String	The description of the instance.
DBInstanceDiskMBPS	Long	The maximum disk throughput of a compute group. Unit: Mbit/s.
DBInstanceGroupCount	String	The number of compute groups.
DBInstanceId	String	The ID of the instance.
DBInstanceMemory	Long	The memory capacity of the instance. Unit: MB.
DBInstanceNetType	String	• Internet: the public network • Intranet: the internal network
DBInstanceStatus	String	For more information about the instance status, see Instance states.
DBInstanceStorage	Long	The disk space of an instance. Unit: GB.
Engine	String	• Internet: the public network • Intranet: the internal network
EngineVersion	String	The version of the database engine.
ExpireTime	String	The expiration time of the instance.
HostType	String	The disk type of compute groups. • 0: SSD • 1: SATA

Parameter	Type	Description
InstanceNetworkType	String	• Classic: classic network • VPC: Virtual Private Cloud
LockMode	String	• Unlock: The instance is not locked. • ManualLock: The instance is locked manually. • LockByExpiration: The instance is locked automatically after the instance expires. • LockByRestoration: The instance is locked automatically before a rollback of the instance. • LockByDiskQuota: The instance is locked automatically when the disk space is full.
MaintainEndTime	String	The end of the time range where the instance is maintained.
MaintainStartTime	String	The start of the time range where the instance is maintained.
MaxConnections	Integer	The maximum number of concurrent connections to an instance.
Port	String	The port number to connect to the instance.
RegionId	String	The region where the instance is located.
SecurityIPList	String	The IP addresses that are allowed to access the instance.
VpcId	String	The ID of the VPC where ClassicLink is enabled.
ZoneId	String	The zone where the instance is located.

Sample requests

```
https://gpdb.example.com/?Action=DescribeDBInstanceAttribute
&DBInstanceId=gp-xxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeDBInstanceAttributeResponse>
 <RequestId>B4CAF581-2AC7-41AD-8940-D56DF7AADF5B</RequestId>
 <Items>
  <DBInstanceAttribute>
       <DBInstanceDiskMBPS>300</DBInstanceDiskMBPS>
       <ConnectionString>gp-xxxxxxxxxxxxxxx.gpdb.rds.example.com</ConnectionString>
       <ZoneId>cn-hangzhou-e</ZoneId>
       <ConnectionMode>Performance</ConnectionMode>
       <VpcId>vpc-xxxxxxxxxxxxxxxx</VpcId>
       <Engine>gpdb</Engine>
       <MaxConnections>500</MaxConnections>
       <MaintainStartTime>18:00Z</MaintainStartTime>
       <DBInstanceGroupCount>2</DBInstanceGroupCount>
       <HostType>0</HostType>
       <DBInstanceMemory>16384</DBInstanceMemory>
       <EngineVersion>4.3</EngineVersion>
       <DBInstanceStatus>Running</DBInstanceStatus> <PayType>Prepaid</PayType>
       <LockMode>Unlock</LockMode>
       <DBInstanceNetType>1</DBInstanceNetType>
       <MaintainEndTime>22:00Z</MaintainEndTime>
       <DBInstanceClass>gpdb.group.segsdx2</DBInstanceClass>
       <DBInstanceId>gp-xxxxxxxxxxxxxxx</DBInstanceId>
       <DBInstanceClassType>x</DBInstanceClassType>
       <InstanceNetworkType>Classic</InstanceNetworkType>
       <DBInstanceDescription>gp-xxxxxxxxxxxxxxx</DBInstanceDescription>
       <DBInstanceStorage>160</DBInstanceStorage>
       <CreationTime>2018-06-27T12:07:10Z</CreationTime>
       <Port>3432</Port>
       <ExpireTime>2019-06-27T16:00:00Z</ExpireTime>
       <RegionId>cn-hangzhou</RegionId>
       <AvailabilityValue>100.0%</AvailabilityValue>
       <DBInstanceCpuCores>2</DBInstanceCpuCores>
       <SecurityIPList>127.0.0.1</SecurityIPList>
  </DBInstanceAttribute>
 </Items>
</DescribeDBInstanceAttributeResponse>
```

JSON format

```
{
  "Items":{
    "DBInstanceAttribute":[
      {
        "DBInstanceDiskMBPS":300,
        "ConnectionString":"gp-xxxxxxxxxxxxxxx.gpdb.rds.example.com",
        "ZoneId":"cn-hangzhou-e",
        "ConnectionMode":"Performance",
        "VpcId":"vpc-xxxxxxxxxxxxxx",
        "Engine":"gpdb",
        "MaxConnections":500,
        "MaintainStartTime":"18:00Z",
        "DBInstanceGroupCount":"2",
        "HostType":"0",
        "DBInstanceMemory":16384,
        "EngineVersion":"4.3",
        "DBInstanceStatus":"Running", "PayType":"Prepaid",
        "LockMode":"Unlock",
        "DBInstanceNetType":"1",
        "MaintainEndTime":"22:00Z",
        "DBInstanceClass":"gpdb.group.segsdx2",
        "DBInstanceId":"gp-xxxxxxxxxxxxxxx",
        "DBInstanceClassType":"x",
        "InstanceNetworkType":"Classic",
        "DBInstanceDescription":"gp-xxxxxxxxxxxxxxx",
        "DBInstanceStorage":160,
        "CreationTime":"2018-06-27T12:07:10Z",
        "Port":"3432",
        "ExpireTime":"2019-06-27T16:00:00Z",
        "RegionId":"cn-hangzhou",
        "AvailabilityValue":"100.0%",
        "DBInstanceCpuCores":2,
        "SecurityIPList":"127.0.0.1"
      }
    ]
  },
  "RequestId":"B4CAF581-2AC7-41AD-8940-D56DF7AADF5B"
}
```


2.11.1.7.4. DescribeDBInstances

Description

You can call this operation to query the list of instances.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstances.
RegionId	String	Yes	The region where the instance is located. You can call the DescribeRegions operation to query the region.
Engine	String	No	The engine of the database. Default value: PostgreSQL.
DBInstanceType	String	No	The role of the instance. Valid values: • Primary: primary instances. • Readonly: read-only instances. • Guard: disaster recovery instances. • Temp: temporary instances. • If you do not specify this parameter, all instances will be returned.
DBInstanceDescription	String	No	The description of the instance.

Parameter	Type	Required	Description
InstanceNetworkType	String	No	The network type of the instance. Valid values: • VPC: Virtual Private Cloud • Classic: classic network • If you do not specify this parameter, instances of all network types will be returned.
ConnectionMode	String	No	• Standard: standard mode • Safe: safe mode • If you do not specify this parameter, instances of both modes will be returned.
Tags	String	No	The name of the tag that is assigned to an instance. It is a JSON string. The tag includes a key-value pair of TagKey and TagValue. You must specify TagKey, and you can specify TagValue as needed. It is in the `{"key1":"value1"}` format.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30
PageNumber	Integer	No	The number of the page to return. Valid values: any non-zero positive integer. Default value: 1

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
PageNumber	Integer	The number of the page returned.
TotalRecordCount	Integer	The total number of entries.
PageRecordCount	Integer	The number of entries on the current page.
Items	List<DBInstance>	The array consisting of DBInstance data.

DBInstance parameters

Parameter	Type	Description
DBInstanceId	String	The ID of the instance.
DBInstanceDescription	String	The description of the instance.
InstanceNetworkType	String	• VPC: Virtual Private Cloud • Classic: classic network
ConnectionMode	String	• Standard: standard mode • Safe: safe mode
RegionId	String	The region where the instance is located.
ZoneId	String	The zone where the instance is located.
ExpireTime	String	The time when the instance is scheduled to expire. Pay-as-you-go instances do not expire.
DBInstanceStatus	String	For more information, see Instance states.
Engine	String	The engine of the database.
EngineVersion	String	The version of the database engine.
DBInstanceNetType	String	• Internet: the public network • Intranet: the private network

Parameter	Type	Description
LockMode	String	• Unlock: The instance is not locked. • ManualLock: The instance is locked manually. • LockByExpiration: The instance is locked automatically after the instance expires. • LockByRestoration: The instance is locked automatically before a rollback of the instance. • LockByDiskQuota: The instance is locked automatically when the disk space is full.
LockReason	String	The reason why the instance is locked.
CreateTime	String	The time when you create an instance.
VPCId	String	The ID of the VPC.
VSwitchId	String	The ID of the VSwitch.

Sample requests

```
https://gpdb.example.com/?Action=DescribeDBInstances
&RegionId=cn-hangzhou
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeDBInstancesResponse>
  <Items>
    <DBInstance>
      <LockMode>Unlock</LockMode>
      <DBInstanceNetType>1</DBInstanceNetType>
      <DBInstanceId>gp-xxxxxxxxxxxxxxxxx</DBInstanceId>
      <ZoneId>cn-hangzhou-e</ZoneId>
      <DBInstanceDescription>gpdb_test</DBInstanceDescription>
      <InstanceNetworkType>Classic</InstanceNetworkType>
```

```
    <VSwitchId>vsw-xxxxxxxxxxxxxxxxx</VSwitchId>
    <VpcId>vpc-xxxxxxxxxxxxxxxxx</VpcId>
    <Engine>gpdb</Engine>
    <ExpireTime>2019-06-27T16:00:00Z</ExpireTime>
    <CreateTime>2018-06-27T12:07:11Z</CreateTime>
    <RegionId>cn-hangzhou</RegionId>
    <EngineVersion>4.3</EngineVersion>
    <LockReason></LockReason>
    <DBInstanceStatus>Running</DBInstanceStatus> <PayType>Prepaid</PayType>
  </DBInstance>
  <DBInstance>
    <LockMode>Unlock</LockMode>
    <DBInstanceNetType>1</DBInstanceNetType>
    <DBInstanceId>gp-xxxxxxxxxxxxxxxxx</DBInstanceId>
    <ZoneId>cn-hangzhou-e</ZoneId>
    <DBInstanceDescription>gp-xxxxxxxxxxxxxxxxx</DBInstanceDescription>
    <InstanceNetworkType>Classic</InstanceNetworkType>
    <VSwitchId>vsw-xxxxxxxxxxxxxxxxx</VSwitchId>
    <VpcId>vpc-xxxxxxxxxxxxxxxxx</VpcId>
    <Engine>gpdb</Engine>
    <ExpireTime>2999-09-08T16:00:00Z</ExpireTime>
    <CreateTime>2018-06-27T11:51:46Z</CreateTime>
    <RegionId>cn-hangzhou</RegionId>
    <EngineVersion>4.3</EngineVersion>
    <LockReason></LockReason>
    <DBInstanceStatus>Running</DBInstanceStatus> <PayType>Postpaid</PayType>
  </DBInstance>
  <DBInstance>
    <LockMode>Unlock</LockMode>
    <DBInstanceNetType>2</DBInstanceNetType>
    <DBInstanceId>gp-xxxxxxxxxxxxxxxxx</DBInstanceId>
    <ZoneId>cn-hangzhou-e</ZoneId>
    <DBInstanceDescription>Test</DBInstanceDescription>
    <InstanceNetworkType>VPC</InstanceNetworkType>
    <VSwitchId>vsw-xxxxxxxxxxxxxxxxx</VSwitchId>
    <VpcId>vpc-xxxxxxxxxxxxxxxxx</VpcId>
    <Engine>gpdb</Engine>
    <ExpireTime>2018-07-27T16:00:00Z</ExpireTime>
    <CreateTime>2018-06-27T11:46:11Z</CreateTime>
    <RegionId>cn-hangzhou</RegionId>
    <EngineVersion>4.3</EngineVersion>
```

```
    <LockReason></LockReason>
    <DBInstanceStatus>Running</DBInstanceStatus> <PayType>Prepaid</PayType>
  </DBInstance>
  <DBInstance>
    <LockMode>Unlock</LockMode>
    <DBInstanceNetType>1</DBInstanceNetType>
    <DBInstanceId>gp-xxxxxxxxxxxxxxxxx</DBInstanceId>
    <ZoneId>cn-hangzhou-f</ZoneId>
    <DBInstanceDescription>Test 2</DBInstanceDescription>
    <InstanceNetworkType>Classic</InstanceNetworkType>
    <VSwitchId></VSwitchId>
    <VpcId></VpcId>
    <Engine>gpdb</Engine>
    <ExpireTime>2018-07-20T16:00:00Z</ExpireTime>
    <CreateTime>2018-06-20T05:42:03Z</CreateTime>
    <RegionId>cn-hangzhou</RegionId>
    <EngineVersion>4.3</EngineVersion>
    <LockReason></LockReason>
    <DBInstanceStatus>Running</DBInstanceStatus> <PayType>Prepaid</PayType>
  </DBInstance>
  <DBInstance>
    <LockMode>Unlock</LockMode>
    <DBInstanceNetType>2</DBInstanceNetType>
    <DBInstanceId>gp-xxxxxxxxxxxxxxxxx</DBInstanceId>
    <ZoneId>cn-hangzhou-b</ZoneId>
    <DBInstanceDescription>gp-xxxxxxxxxxxxxxxxx</DBInstanceDescription>
    <InstanceNetworkType>VPC</InstanceNetworkType>
    <VSwitchId>vsw-xxxxxxxxxxxxxxxxx</VSwitchId>
    <VpcId>vpc-xxxxxxxxxxxxxxxxx</VpcId>
    <Engine>gpdb</Engine>
    <ExpireTime>2999-09-08T16:00:00Z</ExpireTime>
    <CreateTime>2018-06-05T03:42:41Z</CreateTime>
    <RegionId>cn-hangzhou</RegionId>
    <EngineVersion>4.3</EngineVersion>
    <LockReason></LockReason>
    <DBInstanceStatus>Running</DBInstanceStatus> <PayType>Postpaid</PayType>
  </DBInstance>
  <DBInstance>
    <LockMode>Unlock</LockMode>
    <DBInstanceNetType>2</DBInstanceNetType>
    <DBInstanceId>gp-xxxxxxxxxxxxxxxxx</DBInstanceId>
    <ZoneId>cn-hangzhou-b</ZoneId>
```

```
        <ZoneId>cn-hangzhou-b</ZoneId>
        <DBInstanceDescription>Test</DBInstanceDescription>
        <InstanceNetworkType>Classic</InstanceNetworkType>
        <VSwitchId></VSwitchId>
        <VpcId></VpcId>
        <Engine>gpdb</Engine>
        <ExpireTime>2999-09-08T16:00:00Z</ExpireTime>
        <CreateTime>2018-05-07T06:48:47Z</CreateTime>
        <RegionId>cn-hangzhou</RegionId>
        <EngineVersion>4.3</EngineVersion>
        <LockReason></LockReason>
        <DBInstanceStatus>Running</DBInstanceStatus> <PayType>Postpaid</PayType>
      </DBInstance>
      <DBInstance>
        <LockMode>Unlock</LockMode>
        <DBInstanceNetType>2</DBInstanceNetType>
        <DBInstanceId>gp-xxxxxxxxxxxxxxxxx</DBInstanceId>
        <ZoneId>cn-hangzhou-b</ZoneId>
        <DBInstanceDescription>gp-xxxxxxxxxxxxxxxxx</DBInstanceDescription>
        <InstanceNetworkType>VPC</InstanceNetworkType>
        <VSwitchId>vsw-xxxxxxxxxxxxxxxxx</VSwitchId>
        <VpcId>vpc-xxxxxxxxxxxxxxxxx</VpcId>
        <Engine>gpdb</Engine>
        <ExpireTime>2999-09-08T16:00:00Z</ExpireTime>
        <CreateTime>2018-03-16T07:10:03Z</CreateTime>
        <RegionId>cn-hangzhou</RegionId>
        <EngineVersion>4.3</EngineVersion>
        <LockReason></LockReason>
        <DBInstanceStatus>Running</DBInstanceStatus> <PayType>Postpaid</PayType>
      </DBInstance>
    </Items>
    <PageNumber>1</PageNumber>
    <TotalRecordCount>7</TotalRecordCount>
    <RequestId>BBE00C04-A3E8-4114-881D-0480A72CB92E</RequestId>
    <PageRecordCount>7</PageRecordCount>
</DescribeDBInstancesResponse>
```

JSON format

```
{
    "Items":{
      "DBInstance":[
```

```
        {
          "LockMode":"Unlock",
          "DBInstanceNetType":"1",
          "DBInstanceId":"gp-xxxxxxxxxxxxxxxx",
          "ZoneId":"cn-hangzhou-e",
          "DBInstanceDescription":"gpdb_test",
          "InstanceNetworkType":"Classic",
          "VSwitchId":"vsw-xxxxxxxxxxxxxxxx",
          "VpcId":"vpc-xxxxxxxxxxxxxxxx",
          "Engine":"gpdb",
          "ExpireTime":"2019-06-27T16:00:00Z",
          "CreateTime":"2018-06-27T12:07:11Z",
          "RegionId":"cn-hangzhou",
          "EngineVersion":"4.3",
          "LockReason":"",
          "DBInstanceStatus":"Running", "PayType":"Prepaid"
        },
        {
          "LockMode":"Unlock",
          "DBInstanceNetType":"1",
          "DBInstanceId":"gp-xxxxxxxxxxxxxxxxx",
          "ZoneId":"cn-hangzhou-e",
          "DBInstanceDescription":"gp-xxxxxxxxxxxxxxxxx",
          "InstanceNetworkType":"Classic",
          "VSwitchId":"vsw-xxxxxxxxxxxxxxxx",
          "VpcId":"vpc-xxxxxxxxxxxxxxxx",
          "Engine":"gpdb",
          "ExpireTime":"2999-09-08T16:00:00Z",
          "CreateTime":"2018-06-27T11:51:46Z",
          "RegionId":"cn-hangzhou",
          "EngineVersion":"4.3",
          "LockReason":"",
          "DBInstanceStatus":"Running", "PayType":"Postpaid"
        },
        {
          "LockMode":"Unlock",
          "DBInstanceNetType":"2",
          "DBInstanceId":"gp-xxxxxxxxxxxxxxxx",
          "ZoneId":"cn-hangzhou-e",
          "DBInstanceDescription":"Test",
          "InstanceNetworkType":"VPC",
          "VSwitchId":"vsw-xxxxxxxxxxxxxxxx",
```

```
        "VpcId":"vpc-xxxxxxxxxxxxxxxxx",
        "Engine":"gpdb",
        "ExpireTime":"2018-07-27T16:00:00Z",
        "CreateTime":"2018-06-27T11:46:11Z",
        "RegionId":"cn-hangzhou",
        "EngineVersion":"4.3",
        "LockReason":"",
        "DBInstanceStatus":"Running", "PayType":"Prepaid"
      },
      {
        "LockMode":"Unlock",
        "DBInstanceNetType":"1",
        "DBInstanceId":"gp-xxxxxxxxxxxxxxxxx",
        "ZoneId":"cn-hangzhou-f",
        "DBInstanceDescription":"Test 2",
        "InstanceNetworkType":"Classic",
        "VSwitchId":"",
        "VpcId":"",
        "Engine":"gpdb",
        "ExpireTime":"2018-07-20T16:00:00Z",
        "CreateTime":"2018-06-20T05:42:03Z",
        "RegionId":"cn-hangzhou",
        "EngineVersion":"4.3",
        "LockReason":"",
        "DBInstanceStatus":"Running", "PayType":"Prepaid"
      },
      {
        "LockMode":"Unlock",
        "DBInstanceNetType":"2",
        "DBInstanceId":"gp-xxxxxxxxxxxxxxxxx",
        "ZoneId":"cn-hangzhou-b",
        "DBInstanceDescription":"gp-xxxxxxxxxxxxxxxxx",
        "InstanceNetworkType":"VPC",
        "VSwitchId":"vsw-xxxxxxxxxxxxxxxxx",
        "VpcId":"vpc-xxxxxxxxxxxxxxxxx",
        "Engine":"gpdb",
        "ExpireTime":"2999-09-08T16:00:00Z",
        "CreateTime":"2018-06-05T03:42:41Z",
        "RegionId":"cn-hangzhou",
        "EngineVersion":"4.3",
        "LockReason":"",
```

```
            "DBInstanceStatus":"Running", "PayType":"Postpaid"
        },
        {
            "LockMode":"Unlock",
            "DBInstanceNetType":"2",
            "DBInstanceId":"gp-xxxxxxxxxxxxxxxxx",
            "ZoneId":"cn-hangzhou-b",
            "DBInstanceDescription":"Test",
            "InstanceNetworkType":"Classic",
            "VSwitchId":"",
            "VpcId":"",
            "Engine":"gpdb",
            "ExpireTime":"2999-09-08T16:00:00Z",
            "CreateTime":"2018-05-07T06:48:47Z",
            "RegionId":"cn-hangzhou",
            "EngineVersion":"4.3",
            "LockReason":"",
            "DBInstanceStatus":"Running", "PayType":"Postpaid"
        },
        {
            "LockMode":"Unlock",
            "DBInstanceNetType":"2",
            "DBInstanceId":"gp-xxxxxxxxxxxxxxxxx",
            "ZoneId":"cn-hangzhou-b",
            "DBInstanceDescription":"gp-xxxxxxxxxxxxxxxxx",
            "InstanceNetworkType":"VPC",
            "VSwitchId":"vsw-xxxxxxxxxxxxxxxxx",
            "VpcId":"vpc-xxxxxxxxxxxxxxxxx",
            "Engine":"gpdb",
            "ExpireTime":"2999-09-08T16:00:00Z",
            "CreateTime":"2018-03-16T07:10:03Z",
            "RegionId":"cn-hangzhou",
            "EngineVersion":"4.3",
            "LockReason":"",
            "DBInstanceStatus":"Running", "PayType":"Postpaid"
        }
    ]
},
"PageNumber":1,
"TotalRecordCount":7,
"RequestId":"BBE00C04-A3E8-4114-881D-0480A72CB92E",
```

```
  "PageRecordCount":7
}
```

2.11.1.7.5. DescribeRegions

Description

You can call this operation to query available regions and zones. You must call the DescribeRegions operation to query the available regions before calling the CreateDBInstance operation.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeRegions.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Regions	List<Region>	The list of regions.

Region parameters

Parameter	Type	Description
RegionId	String	The data center in the specified region.
Zones	List<Zones>	The list of zones.

Zone parameters

Parameter	Type	Description
ZoneId	String	The zone where the instance is located.

Parameter	Type	Description
VpcEnabled	Boolean	Indicates whether the VPC in the zone is available.

Sample requests

```
https://gpdb.example.com/?Action=DescribeRegions
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeRegionsResponse>
 <RequestId>FF8EB261-5447-4B1B-9F14-294CEA008A9F</RequestId>
 <Regions>
  <Region>
   <RegionId>cn-beijing</RegionId>
   <Zones>
    <Zone>
     <VpcEnabled>true</VpcEnabled>
     <ZoneId>cn-beijing-c</ZoneId>
    </Zone>
    <Zone>
     <VpcEnabled>true</VpcEnabled>
     <ZoneId>cn-beijing-g</ZoneId>
    </Zone>
   </Zones>
  </Region>
  <Region>
   <RegionId>cn-zhangjiakou</RegionId>
   <Zones>
    <Zone>
     <VpcEnabled>true</VpcEnabled>
     <ZoneId>cn-zhangjiakou-b</ZoneId>
    </Zone>
   </Zones>
  </Region>
  <Region>
   <RegionId>cn-hangzhou</RegionId>
   <Zones>
    <Zone>
     <VpcEnabled>true</VpcEnabled>
```

```
  <VpcEnabled>true</VpcEnabled>
  <ZoneId>cn-hangzhou-b</ZoneId>
 </Zone>
 <Zone>
  <VpcEnabled>true</VpcEnabled>
  <ZoneId>cn-hangzhou-e</ZoneId>
 </Zone>
 <Zone>
  <VpcEnabled>true</VpcEnabled>
  <ZoneId>cn-hangzhou-f</ZoneId>
 </Zone>
</Zones>
</Region>
<Region>
 <RegionId>cn-shanghai</RegionId>
 <Zones>
  <Zone>
   <VpcEnabled>true</VpcEnabled>
   <ZoneId>cn-shanghai-b</ZoneId>
  </Zone>
  <Zone>
   <VpcEnabled>true</VpcEnabled>
   <ZoneId>cn-shanghai-d</ZoneId>
  </Zone>
 </Zones>
</Region>
<Region>
 <RegionId>cn-shenzhen</RegionId>
 <Zones>
  <Zone>
   <VpcEnabled>true</VpcEnabled>
   <ZoneId>cn-shenzhen-a</ZoneId>
  </Zone>
 </Zones>
</Region>
<Region>
 <RegionId>ap-southeast-1</RegionId>
 <Zones>
  <Zone>
   <VpcEnabled>true</VpcEnabled>
   <ZoneId>ap-southeast-1b</ZoneId>
  </Zone>
```

```
 </Zones>
</Region>
<Region>
 <RegionId>ap-southeast-2</RegionId>
 <Zones>
  <Zone>
   <VpcEnabled>true</VpcEnabled>
   <ZoneId>ap-southeast-2a</ZoneId>
  </Zone>
  <Zone>
   <VpcEnabled>true</VpcEnabled>
   <ZoneId>ap-southeast-2b</ZoneId>
  </Zone>
 </Zones>
</Region>
<Region>
 <RegionId>us-east-1</RegionId>
 <Zones>
  <Zone>
   <VpcEnabled>true</VpcEnabled>
   <ZoneId>us-east-1b</ZoneId>
  </Zone>
 </Zones>
</Region>
<Region>
 <RegionId>us-west-1</RegionId>
 <Zones>
  <Zone>
   <VpcEnabled>true</VpcEnabled>
   <ZoneId>us-west-1a</ZoneId>
  </Zone>
 </Zones>
</Region>
<Region>
 <RegionId>cn-chengdu</RegionId>
 <Zones>
  <Zone>
   <VpcEnabled>true</VpcEnabled>
   <ZoneId>cn-chengdu-a</ZoneId>
  </Zone>
 </Zones>
```

```
  </Region>
  <Region>
   <RegionId>ap-southeast-3</RegionId>
   <Zones>
    <Zone>
     <VpcEnabled>true</VpcEnabled>
     <ZoneId>ap-southeast-3a</ZoneId>
    </Zone>
   </Zones>
  </Region>
  <Region>
   <RegionId>cn-huhehaote</RegionId>
   <Zones>
    <Zone>
     <VpcEnabled>true</VpcEnabled>
     <ZoneId>cn-huhehaote-a</ZoneId>
    </Zone>
   </Zones>
  </Region>
  <Region>
   <RegionId>ap-south-1</RegionId>
   <Zones>
    <Zone>
     <VpcEnabled>true</VpcEnabled>
     <ZoneId>ap-south-1a</ZoneId>
    </Zone>
   </Zones>
  </Region>
  <Region>
   <RegionId>ap-southeast-5</RegionId>
   <Zones>
    <Zone>
     <VpcEnabled>true</VpcEnabled>
     <ZoneId>ap-southeast-5a</ZoneId>
    </Zone>
   </Zones>
  </Region>
 </Regions>
</DescribeRegionsResponse>
```

JSON format

```
{
  "RequestId":"FF8EB261-5447-4B1B-9F14-294CEA008A9F",
  "Regions":{
    "Region":[
      {
        "RegionId":"cn-beijing",
        "Zones":{
          "Zone":[
            {
              "VpcEnabled":true,
              "ZoneId":"cn-beijing-c"
            },
            {
              "VpcEnabled":true,
              "ZoneId":"cn-beijing-g"
            }
          ]
        }
      },
      {
        "RegionId":"cn-zhangjiakou",
        "Zones":{
          "Zone":[
            {
              "VpcEnabled":true,
              "ZoneId":"cn-zhangjiakou-b"
            }
          ]
        }
      },
      {
        "RegionId":"cn-hangzhou",
        "Zones":{
          "Zone":[
            {
              "VpcEnabled":true,
              "ZoneId":"cn-hangzhou-b"
            },
            {
              "VpcEnabled":true,
              "ZoneId":"cn-hangzhou-e"
```

```
            },
            {
              "VpcEnabled":true,
              "ZoneId":"cn-hangzhou-f"
            }
          ]
        }
      },
      {
        "RegionId":"cn-shanghai",
        "Zones":{
          "Zone":[
            {
              "VpcEnabled":true,
              "ZoneId":"cn-shanghai-b"
            },
            {
              "VpcEnabled":true,
              "ZoneId":"cn-shanghai-d"
            }
          ]
        }
      },
      {
        "RegionId":"cn-shenzhen",
        "Zones":{
          "Zone":[
            {
              "VpcEnabled":true,
              "ZoneId":"cn-shenzhen-a"
            }
          ]
        }
      },
      {
        "RegionId":"ap-southeast-1",
        "Zones":{
          "Zone":[
            {
              "VpcEnabled":true,
              "ZoneId":"ap-southeast-1b"
            }
```

```
        ]
      }
    },
    {
      "RegionId":"ap-southeast-2",
      "Zones":{
        "Zone":[
          {
            "VpcEnabled":true,
            "ZoneId":"ap-southeast-2a"
          },
          {
            "VpcEnabled":true,
            "ZoneId":"ap-southeast-2b"
          }
        ]
      }
    },
    {
      "RegionId":"us-east-1",
      "Zones":{
        "Zone":[
          {
            "VpcEnabled":true,
            "ZoneId":"us-east-1b"
          }
        ]
      }
    },
    {
      "RegionId":"us-west-1",
      "Zones":{
        "Zone":[
          {
            "VpcEnabled":true,
            "ZoneId":"us-west-1a"
          }
        ]
      }
    },
    {
```

```
      "RegionId":"cn-chengdu",
      "Zones":{
        "Zone":[
          {
            "VpcEnabled":true,
            "ZoneId":"cn-chengdu-a"
          }
        ]
      }
    },
    {
      "RegionId":"ap-southeast-3",
      "Zones":{
        "Zone":[
          {
            "VpcEnabled":true,
            "ZoneId":"ap-southeast-3a"
          }
        ]
      }
    },
    {
      "RegionId":"cn-huhehaote",
      "Zones":{
        "Zone":[
          {
            "VpcEnabled":true,
            "ZoneId":"cn-huhehaote-a"
          }
        ]
      }
    },
    {
      "RegionId":"ap-south-1",
      "Zones":{
        "Zone":[
          {
            "VpcEnabled":true,
            "ZoneId":"ap-south-1a"
          }
        ]
```

```
          }
        },
        {
          "RegionId":"ap-southeast-5",
          "Zones":{
            "Zone":[
              {
                "VpcEnabled":true,
                "ZoneId":"ap-southeast-5a"
              }
            ]
          }
        }
      ]
    }
}
```

2.11.1.7.6. DescribeResourceUsage

Description

You can call this operation to query the disk space that is used by an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeResourceUsage.
DBInstanceId	String	Yes	The ID of the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
DBInstanceId	String	The ID of the instance.

Parameter	Type	Description
Engine	String	The engine of the database.
DiskUsed	Integer	The used space of a disk. The used space indicates the user data space (DataSize) and log data space (LogSize). The value of -1 indicates that the space is not used. Unit: Bytes.
DataSize	Integer	The disk space that is used to store user data. The value of -1 indicates that the space is not used. Unit: Bytes.
LogSize	Integer	The disk space that is used to store log files. The value of -1 indicates that the space is not used. Unit: Bytes.
BackupSize	Integer	The disk space that is used to store backup files. The value of -1 indicates that the space is not used. Unit: Bytes.

Sample requests

```
https://gpdb.example.com/?Action=DescribeResourceUsage
&DBInstanceId=gp-xxxxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeResourceUsageResponse>
    <DBInstanceId>gp-xxxxxxxxxxxxxxxx</DBInstanceId>
    <RequestId>860FBA9E-BFFD-493E-91A1-2349B9D74AE7</RequestId>
    <LogSize>201326592</LogSize>
    <DataSize>83886080</DataSize>
    <BackupSize>26624</BackupSize>
    <Engine>gpdb</Engine>
    <DiskUsed>285212672</DiskUsed>
</DescribeResourceUsageResponse>
```

JSON format

```
{
  "DBInstanceId":"gp-xxxxxxxxxxxxxxxx",
  "RequestId":"860FBA9E-BFFD-493E-91A1-2349B9D74AE7",
  "LogSize":201326592,
  "DataSize":83886080,
  "BackupSize":26624,
  "Engine":"gpdb",
  "DiskUsed":285212672
}
```


2.11.1.7.7. ModifyDBInstanceConnectionMode

Description

You can call this operation to modify the access mode of an instance. The following two modes are supported:

- Standard mode
- Safe mode

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceConnectionMode.
DBInstanceId	String	Yes	The ID of the instance.
ConnectionMode	String	Yes	• Standard • Safe

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ModifyDBInstanceConnectionMode
&DBInstanceId=gp-xxxxxxxxxxxxxxxx
&ConnectionMode=Safe
&<Common request parameters>
```

Sample responses

XML format

```
<BaseResponse>
 <RequestId>8361E350-4CCC-4D28-B020-55B4DCB75D3B</RequestId>
</BaseResponse>
```

JSON format

```
{
   "RequestId":"8361E350-4CCC-4D28-B020-55B4DCB75D3B",
}
```

2.11.1.7.8. ModifyDBInstanceDescription

Description

You can call this operation to modify the description of an instance to help identify the instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceDescription.
DBInstanceId	String	Yes	The ID of the instance.
DBInstanceDescription	Sting	Yes	The description of the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ModifyDBInstanceDescription
&DBInstanceId=gp-xxxxxxxxxxxxxxxx
&DBInstanceDescription=testInstanceDescribe
&<Common request parameters>
```

Sample responses

XML format

```
<ModifyDBInstanceDescriptionResponse>
      <RequestId>107BE202-D1A2-479E-98E0-A892B472562F</RequestId>
</ModifyDBInstanceDescriptionResponse>
```

JSON format

```
{
  "RequestId": "107BE202-D1A2-479E-98E0-A892B472562F"
}
```

2.11.1.7.9. ModifyDBInstanceMaintainTime

Description

You can call this operation to modify the maintenance window of an instance. Typically, it is set to the off-peak hours to minimize the impact on services. Alibaba Cloud will perform routine maintenance for instances at the specified maintenance time.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceMaintainTime.

Parameter	Type	Required	Description
DBInstanceId	String	Yes	The ID of the instance.
StartTime	String	Yes	The start time of the maintenance window. For example, 02:00Z.
EndTime	String	Yes	The end time of the maintenance window. For example, 03:00Z. The end time must be later than the start time.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ModifyDBInstanceMaintainTime
&DBInstanceId=gp-xxxxxxxxxxxxxxxx
&StartTime=02:00Z
&EndTime=03:00Z
&<Common request parameters>
```

Sample responses

XML format

```
<ModifyDBInstanceMaintainTimeResponse>
      <RequestId>CA9A34C8-AC95-413B-AC6A-CEBF67429CCA</RequestId>
</ModifyDBInstanceMaintainTimeResponse>
```

JSON format

```
{
  "RequestId": "CA9A34C8-AC95-413B-AC6A-CEBF67429CCA"
}
```

2.11.1.7.10. RestartDBInstance

Description

You can call this operation to restart an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to RestartDBInstance.
DBInstanceId	String	Yes	The ID of the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=RestartDBInstance
        &DBInstanceId=gp-xxxxxxxxxxxxxxxx
        &<Common request parameters>
```

Sample responses

XML format

```
<RestartDBInstance>
        <RequestId>A7356493-7141-4393-8951-CDA8AB5D67EC</RequestId>
        </RestartDBInstance>
```

JSON format

```
{
        "RequestId":"A7356493-7141-4393-8951-CDA8AB5D67EC"
        }
```

2.11.1.7.11. DescribeDBInstancePerformance

Description

You can call this operation to query the specified performance metrics for an instance over a period of time.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstancePerformance.
DBInstanceId	String	Yes	The ID of the instance.
Key	String	Yes	The performance metrics. Separate multiple performance metrics with commas (,). For more information, see Performance parameters.
StartTime	String	Yes	The start time of a period during which you need to query the metrics. For example, 2018-06-11T15:00Z.
EndTime	String	Yes	The end time of a period during which you need to query the metrics. For example, 2018-06-11T16:00Z.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common request parameters.
DBInstanceId	String	The ID of the instance.
Engine	String	The engine of the database.

Parameter	Type	Description
StartTime	String	The start time of a period during which you need to query the metrics. It is in the `YYYY-MM-DDTHH:mmZ` format such as 2018-05-30T03:29Z.
EndTime	String	The end time of a period during which you need to query the metrics. It is in the `YYYY-MM-DDTHH:mmZ` format such as 2018-05-30T03:29Z. The end time must be later than the start time.
PerformanceKeys	List<PerformanceKey>	The array that contains the performance metrics. It is in the {perf1, perf2, perf3, ...} format.

PerformanceKey parameters

Parameter	Type	Description
Key	String	The performance metric.
Unit	String	The unit of the metric.
ValueFormat	String	The format of a value. • If this parameter is null, the values of performance metrics are returned. • If this parameter is not null, multiple metrics are parsed and separated with ampersands (&), such as `com_delete&com_insert&com_insert_select&com_replace`.
GroupValues	List<GroupValue>	The array that contains the metric values. It is in the {value1, value2, ...} format.

GroupValue parameters

Parameter	Type	Description
Name	String	The name of the group.

Parameter	Type	Description
Values	List<Value>	The array that contains the metric values. It is in the {value1, value2, ...} format.

Value parameters

Parameter	Type	Description
Value	String	The value of the performance metric.
date	String	The time when the metric value was recorded. Unit: milliseconds.

Sample requests

```
https://gpdb.example.com/?Action=DescribeDBInstancePerformance
&DBInstanceId=gp-xxxxxxxxxxxxx
&key=CpuUsage,MemoryUsage,Gpdb_SpaceUsage,Gpdb_IOPS,Gpdb_session
&EndTime=2018-07-09T03:43Z
&StartTime=2018-07-08T03:43Z
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeDBInstancePerformanceResponse>
  <RequestId>5E85244A-AB47-46A3-A3AD-5F307DCB407E</RequestId>
  <DBInstanceId>gp-xxxxxxxxxxxxx</DBInstanceId>
  <PerformanceKeys>
    <Key>MemoryUsage</Key>
    <GroupValues>
      <Name>7198315-1530522046144-1</Name>
      <Values />
    </GroupValues>
    <GroupValues>
      <Name>7198315-1530522046144-0</Name>
      <Values />
    </GroupValues>
    <GroupValues>
      <Values />
      <Name>master</Name>
```

```
    </GroupValues>
    <Unit>%</Unit>
    <ValueFormat>mem_usage</ValueFormat>
  </PerformanceKeys>
  <PerformanceKeys>
    <Key>Gpdb_session</Key>
    <GroupValues>
      <Name>7198315-1530522046144-1</Name>
      <Values />
    </GroupValues>
    <GroupValues>
      <Name>7198315-1530522046144-0</Name>
      <Values />
    </GroupValues>
    <GroupValues>
      <Values />
      <Name>master</Name>
    </GroupValues>
    <Unit>int</Unit>
    <ValueFormat>conn_count</ValueFormat>
  </PerformanceKeys>
  <PerformanceKeys>
    <Key>CpuUsage</Key>
    <GroupValues>
      <Name>7198315-1530522046144-1</Name>
      <Values />
    </GroupValues>
    <GroupValues>
      <Name>7198315-1530522046144-0</Name>
      <Values />
    </GroupValues>
    <GroupValues>
      <Values />
      <Name>master</Name>
    </GroupValues>
    <Unit>%</Unit>
    <ValueFormat>cpu_usage</ValueFormat>
  </PerformanceKeys>
  <PerformanceKeys>
    <Key>Gpdb_IOPS</Key>
    <GroupValues>
      <Name>7198315-1530522046144-1</Name>
```

```
        <Name>7198315-1530522046144-1</Name>
        <Values />
      </GroupValues>
      <GroupValues>
        <Name>7198315-1530522046144-0</Name>
        <Values />
      </GroupValues>
      <GroupValues>
        <Values />
        <Name>master</Name>
      </GroupValues>
      <Unit>int</Unit>
      <ValueFormat>data_iops&amp;amp;write_iops&amp;amp;read_iops</ValueFormat>
    </PerformanceKeys>
    <PerformanceKeys>
      <Key>Gpdb_SpaceUsage</Key>
      <GroupValues>
        <Name>7198315-1530522046144-1</Name>
        <Values />
      </GroupValues>
      <GroupValues>
        <Name>7198315-1530522046144-0</Name>
        <Values />
      </GroupValues>
      <GroupValues>
        <Values />
        <Name>master</Name>
      </GroupValues>
      <Unit>Byte</Unit>
      <ValueFormat>space</ValueFormat>
    </PerformanceKeys>
    <EndTime>2018-07-09T03:47Z</EndTime>
    <StartTime>2018-07-08T03:47Z</StartTime>
    <Engine>gpdb</Engine>
</DescribeDBInstancePerformanceResponse>
```

JSON format

```
{
    "RequestId":"5E85244A-AB47-46A3-A3AD-5F307DCB407E",
    "DBInstanceId":"gp-xxxxxxxxxxxxxx",
    "PerformanceKeys":[
```

```
        {
          "Key":"MemoryUsage",
          "GroupValues":[
            {
              "Name":"7198315-1530522046144-1",
              "Values":Array[288]
            },
            {
              "Name":"7198315-1530522046144-0",
              "Values":Array[288]
            },
            {
              "Values":Array[288],
              "Name":"master"
            }
          ],
          "Unit":"%",
          "ValueFormat":"mem_usage"
        },
        {
          "Key":"Gpdb_session",
          "GroupValues":[
            {
              "Name":"7198315-1530522046144-1",
              "Values":Array[288]
            },
            {
              "Name":"7198315-1530522046144-0",
              "Values":Array[288]
            },
            {
              "Values":Array[288],
              "Name":"master"
            }
          ],
          "Unit":"int",
          "ValueFormat":"conn_count"
        },
        {
          "Key":"CpuUsage",
          "GroupValues":[
            {
```

```
            {
              "Name":"7198315-1530522046144-1",
              "Values":Array[288]
            },
            {
              "Name":"7198315-1530522046144-0",
              "Values":Array[288]
            },
            {
              "Values":Array[288],
              "Name":"master"
            }
          ],
          "Unit":"%",
          "ValueFormat":"cpu_usage"
        },
        {
          "Key":"Gpdb_IOPS",
          "GroupValues":[
            {
              "Name":"7198315-1530522046144-1",
              "Values":Array[288]
            },
            {
              "Name":"7198315-1530522046144-0",
              "Values":Array[288]
            },
            {
              "Values":Array[288],
              "Name":"master"
            }
          ],
          "Unit":"int",
          "ValueFormat":"data_iops&write_iops&read_iops"
        },
        {
          "Key":"Gpdb_SpaceUsage",
          "GroupValues":[
            {
              "Name":"7198315-1530522046144-1",
              "Values":Array[288]
            },
```

```
            {
              "Name":"7198315-1530522046144-0",
              "Values":Array[288]
            },
            {
              "Values":Array[288],
              "Name":"master"
            }
          ],
          "Unit":"Byte",
          "ValueFormat":"space"
        }
    ],
    "EndTime":"2018-07-09T03:47Z",
    "StartTime":"2018-07-08T03:47Z",
    "Engine":"gpdb"
}
```


2.11.1.8. Database management

2.11.1.8.1. DeleteDatabase

Description

You can call this operation to delete a database from an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DeleteDatabase.
DBInstanceId	String	Yes	The ID of the instance.
DBName	String	Yes	The name of the database.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=DeleteDatabase
&DBName=testdb01
&DBInstanceId=gp-xxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<DeleteDatabaseResponse>
    <RequestId>07F6177E-6DE4-408A-BB4F-0723301340F3</RequestId>
</DeleteDatabaseResponse>
```

JSON format

```
{
  "RequestId":"07F6177E-6DE4-408A-BB4F-0723301340F3"
}
```

2.11.1.8.2. DescribeAccounts

Description

You can call this operation to query the information of a database account.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeAccounts.
AccountName	String	No	The name of the account.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Accounts	List<DBInstanceAccount>	The information of the account.

DBInstanceAccount parameters

Parameter	Type	Description
DBInstanceId	String	The ID of the instance.
AccountName	String	The name of the account.
AccountStatus	String	The statuses of the account are as follows: • 0: indicates that the account is being created. • 1: indicates that the account is being used. • 3: indicates that the account is being deleted.
AccountDescription	String	The description of the account.

Sample requests

```
https://gpdb.example.com/?Action=DescribeAccounts
&DBInstanceId=gp-xxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeAccountsResponse>
      <RequestId>7565770E-7C45-462D-BA4A-8A5396F2CAD1</RequestId>
       <Accounts>
          <DBInstanceAccount>
            <AccountName>testaccount_1</AccountName>
            <DBInstanceId>gp-xxxxxxxxxxxxxx</DBInstanceId>
            <AccountStatus>1</AccountStatus>
            <AccountDescription></AccountDescription>
          <DBInstanceAccount>
       </Accounts>
</DescribeAccountsResponse>
```

JSON format

```
{
   "Accounts": {
    "DBInstanceAccount": [
     {
       "AccountDescription": "",
       "DBInstanceId": "gp-xxxxxxxxxxxxxx",
       "AccountStatus": "1",
       "AccountName": "testaccount_1"
     }
    ]
   },
   "RequestId": "7565770E-7C45-462D-BA4A-8A5396F2CAD1"
 }
```

2.11.1.8.3. ModifyAccountDescription

Description

You can call this operation to modify the description of a database account to help identify the account.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyAccountDescription.
DBInstanceId	String	Yes	The ID of the instance.
AccountName	String	Yes	The name of the account. It must be unique and meet the following requirements: • The name must start with a letter. • The name can contain lowercase letters, digits, and underscores (_). • The name can be up to 16 characters in length. • The name cannot contain reserved keywords.
AccountDescription	String	Yes	Specifies the description of the account. The description must meet the following requirements: • The description must start with a letter. • The description cannot start with http:// or https://. • The description can contain letters, underscores (_), hyphens (-), and digits. • The description must be 2 to 256 characters in length.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ModifyAccountDescription
&DBInstanceId=gp-xxxxxxxxxxxxx
&AccountName=testAccout
&AccountDescription=testAccoutdescribe
&<Common request parameters>
```

Sample responses

XML format

```
<ModifyAccountDescriptionResponse>
      <RequestId>99BBBD5E-B5D8-4FC8-B8BF-FB1A0A38BBA2</RequestId>
</ModifyAccountDescriptionResponse>
```

JSON format

```
{
  "RequestId": "99BBBD5E-B5D8-4FC8-B8BF-FB1A0A38BBA2"
}
```

2.11.1.9. Account management

2.11.1.9.1. CreateAccount

Description

You can call this operation to create an account for a database.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to CreateAccount.

Parameter	Type	Required	Description
DBInstanceId	String	Yes	The ID of the instance.
DatabaseName	String	No	The name of the database.
AccountName	String	Yes	The name of the account.
AccountPassword	String	Yes	The password of the account.
AccountDescription	String	No	The description of the account.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=CreateAccount
&AccountName=testacc02
&AccountPassword=pw1234
&DBInstanceId=gp-xxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<CreateAccountResponse>
      <RequestId>D4D4BE8A-DD46-440A-BFCD-EE31DA81C9DD</RequestId>
</CreateAccountResponse>
```

JSON format

```
{
  "RequestId":"D4D4BE8A-DD46-440A-BFCD-EE31DA81C9DD"
}
```

2.11.1.9.2. ResetAccountPassword

Description

You can call this operation to reset the password for your account. Before calling this operation, make sure that the following conditions are met:

- The instance is in the running state.
- The instance is not locked.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to ResetAccountPassword.
DBInstanceId	String	Yes	The ID of the instance.
AccountName	String	Yes	The name of the account.
AccountPassword	String	Yes	The new password for the account. The password must be 8 to 32 characters in length. The password must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. Special characters include !@#$%^&*()_+-=

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ResetAccountPassword
&AccountName=testaccount_1
&AccountPassword=Testaccount_1
&DBInstanceId=gp-xxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<ResetAccountPasswordResponse>
      <RequestId>187C80FC-75C4-477C-BBF2-A368A36D041C</RequestId>
</ResetAccountPasswordResponse>
```

JSON format

```
{
  "RequestId":"187C80FC-75C4-477C-BBF2-A368A36D041C"
}
```

2.11.1.10. Security management

2.11.1.10.1. DescribeDBInstanceIPArrayList

Description

You can call this operation to query the IP addresses that are allowed to access an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceIPArrayList.
DBInstanceId	String	Yes	The ID of the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Items	List<DBInstanceIPArray>	The IP addresses that are allowed to access the instance.

DBInstanceIPArray parameters

Parameter	Type	Description
DBInstanceIPArrayName	String	The name of the IP address whitelist.
DBInstanceIPArrayAttribute	String	This parameter is null by default. You can use this parameter to distinguish whitelists that have different attributes. The console does not display whitelists that have the attribute.
SecurityIPList	String	The IP addresses listed in the whitelist. You can add up to 1,000 IP addresses to the whitelist. Separate multiple IP addresses with commas (,). The formats are as follows: • 0.0.0.0/0. • 10.23.12.24 (IP addresses). • Classless Inter-Domain Routing (CIDR) blocks, such as 10.23.12.24/24, where /24 indicates the prefix of the CIDR block is 24-bit. You can replace 24 with a value ranging from 1 to 32.

Sample requests

```
https://gpdb.example.com/?Action=DescribeDBInstanceIPArrayList
&DBInstanceId=gp-xxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeDBInstanceIPArrayListResponse>
 <RequestId>CB7AA0BF-BE41-480E-A3DC-C97BF85A391B</RequestId>
 <Items>
  <DBInstanceIPArray>
    <groupName>default</groupName>
     <groupTag></groupTag>
     <securityIPList>127.0.0.1</securityIPList>
  </DBInstanceIPArray>
</DescribeDBInstanceIPArrayListResponse>
```

JSON format

```
{
  "Items":{
    "DBInstanceIPArray":[
      {
        "groupName":"default",
        "groupTag":"",
        "securityIPList":"127.0.0.1"
      }
    ]
  },
  "RequestId":"CB7AA0BF-BE41-480E-A3DC-C97BF85A391B"
}
```

2.11.1.10.2. ModifySecurityIps

Description

You can call this operation to modify the IP addresses that are allowed to access an instance. Before calling this operation, make sure that the following conditions are met:

- The instance is in the running state.
- The instance is not locked.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifySecurityIps.
DBInstanceId	String	Yes	The ID of the instance.
SecurityIps	String	Yes	The IP addresses listed in the whitelist. You can add up to 1,000 IP addresses to the whitelist. Separate multiple IP addresses with commas (,). The formats are as follows: • 0.0.0.0/0. • 10.23.12.24 (IP addresses). • Classless Inter-Domain Routing (CIDR) blocks, such as 10.23.12.24/24, where /24 indicates the prefix of the CIDR block is 24-bit. You can replace 24 with a value ranging from 1 to 32.
DBInstanceIPArrayName	String	No	The name of the whitelist. If you do not enter a name, IP addresses are added to the default whitelist. Note You can create up to 50 whitelists for an instance.

Parameter	Type	Required	Description
DBInstanceIPArrayAttribute	String	No	The attribute of the IP address whitelist. It is null by default. You can use this parameter to distinguish whitelists that have different attributes. The console does not display whitelists that have the `hidden` attribute.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ModifySecurityIps
&DBInstanceId=gp-xxxxxxxxxxxxxx
&SecurityIps=192.168.0.1
&<Common request parameters>
```

Sample responses

XML format

```
<ModifySecurityIpsResponse>
    <RequestId>871C698F-B43D-4D1D-ACD6-DF56B0F89978</RequestId>
</ModifySecurityIpsResponse>
```

JSON format

```
{
 "RequestId":"871C698F-B43D-4D1D-ACD6-DF56B0F89978"
}
```

2.11.1.11. Log management

2.11.1.11.1. DescribeSlowLogRecords

Description

You can call this operation to query slow query logs of a database in an instance over a period of time.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSlowLogRecords.
DBInstanceId	String	Yes	The ID of the instance.
StartTime	String	Yes	The start time of the query. Specify the time in the `YYYY-MM-DDTHH:mmZ` format, such as 2011-06-11T15:00Z.
EndTime	String	Yes	The end time of the query. Specify the time in the `YYYY-MM-DDTHH:mmZ` format, such as 2011-06-11T16:00Z. The end time must be later than the start time.
SQLId	Long	No	The ID of the SQL query.
DBName	String	No	The name of the database.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30
PageNumber	Integer	No	The number of the page to return. Valid values: any non-zero positive integer. Default value: 1

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
Engine	String	The engine of the database.
TotalRecordCount	Integer	The total number of slow SQL queries.
PageNumber	Integer	The number of the page.
PageRecordCount	Integer	The number of slow SQL queries on the current page.
Items	List<SQLSlowRecord>	The details of slow query logs.

SQLSlowRecord parameters

Parameter	Type	Description
HostAddress	String	The IP address of the host that you use to connect to a database.
DBName	String	The name of the database.
SQLText	String	The SQL statement.
QueryTimes	Long	The execution duration of the query. Unit: seconds.
LockTimes	Long	The lock duration of the query. Unit: seconds.
ParseRowCounts	Long	The number of rows that the SQL statement parsed.
ReturnRowCounts	Long	The number of rows that the SQL statement returned.
ExecutionStartTime	String	The beginning of the time range where the statement is executed. It is in the `YYYY-MM-DDTHH:mm:ss Z` format, such as 2011-06-11T15:00:08Z.

Sample requests

```
https://gpdb.example.com/?Action=DescribeSlowLogRecords
&DBInstanceId=gp-xxxxxxxxxxxxxx
&StartTime=2018-07-09T08:00Z
&EndTime=2018-07-09T09:00Z
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeSlowLogRecordsResponse>
  <RequestId>542BB8D6-4268-45CC-A557-B03EFD7AB30A</RequestId>
  <Engine>gpdb</Engine>
  <PageNumber>1</PageNumber>
  <PageRecordCount>1</PageRecordCount>
  <TotalRecordCount>1</TotalRecordCount>
  <Items>
    <SQLSlowRecord>
      <HostAddress>192.168.0.123</HostAddress>
      <DBName>test</DBName>
      <SQLText> update test.zxb set id=0 limit 1</SQLText>
      <QueryTimes>123</QueryTimes>
      <LockTimes>12</LockTimes>
      <ParseRowCounts>125</ParseRowCounts>
      <ReturnRowCounts>1</ReturnRowCounts>
      <ExecutionStartTime>2018-07-09T09:00:08Z</ExecutionStartTime>
    </SQLSlowRecord>
  </Items>
</DescribeSlowLogRecordsResponse>
```

JSON format

```
{
  "RequestId":"542BB8D6-4268-45CC-A557-B03EFD7AB30A",
  "Engine":"gpdb",
  "PageNumber":1,
  "PageRecordCount":1,
  "TotalRecordCount":1,
  "Items":{
    "SQLSlowRecord":[
      {
        "HostAddress":"192.168.0.123",
        "DBName":"test",
        "SQLText":" update test.zxb set id=0 limit 1",
        "QueryTimes":"123",
        "LockTimes":"12",
        "ParseRowCounts":"125",
        "ReturnRowCounts":"1",
        "ExecutionStartTime":"2018-07-09T09:00:08Z"
      }
    ]
  }
}
```


2.11.1.11.2. DescribeSQLCollectorPolicy

Description

You can call this operation to check whether the SQL collection feature is enabled for an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSQLCollectorPolicy.
DBInstanceId	String	Yes	The ID of the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
SQLCollectorStatus	String	• Enabled: specifies whether to enable SQL collection. • Disabled: specifies whether to disable SQL collection.

Sample requests

```
https://gpdb.example.com/?Action=DescribeSQLCollectorPolicy
&DBInstanceId=gp-xxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeSQLCollectorPolicyResponse>
    <RequestId>ABB39CC3-4488-4857-905D-2E4A051D0521</RequestId>
    <SQLCollectorStatus>Enable</SQLCollectorStatus>
</DescribeSQLCollectorPolicyResponse>
```

JSON format

```
{
    "RequestId":"ABB39CC3-4488-4857-905D-2E4A051D0521",
    "SQLCollectorStatus":"Enable"
}
```

2.11.1.11.3. DescribeSQLLogFiles

Description

You can call this operation to query the list of SQL audit log files.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSQLLogFiles.
DBInstanceId	String	Yes	The ID of the instance.
FileName	String	No	The name of the file.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30
PageNumber	Integer	No	The number of the page to return. Valid values: any non-zero positive integer. Default value: 1

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
TotalRecordCount	Integer	The total number of entries.
PageNumber	Integer	The number of the page.
PageRecordCount	Integer	The number of entries on the current page.
Items	List<LogFile>	The array that consists of audit file data.

LogFile parameters

Parameter	Type	Description
FileID	Integer	The ID of an audit log file.

Parameter	Type	Description
LogStatus	String	• NoStart: The database has not started generating audit log files. • Generating: The database is generating audit log files. • Success: The database has generated audit log files. • Failed: The database has failed to generate audit log files.
LogStartTime	String	The beginning of the time range where an audit log starts to record data.
LogEndTime	String	The end of the time range where an audit log stops recording data.
LogDownloadURL	String	The download URL of audit log files. If the download URL is unavailable, an empty string is returned.
LogSize	Long	The size of the audit log file. Unit: Bytes.

Sample requests

```
https://gpdb.example.com/?Action=DescribeSQLLogFiles
&DBInstanceId=gp-xxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeSQLLogFilesResponse>
    <Items></Items>
    <PageNumber>1</PageNumber>
    <TotalRecordCount>0</TotalRecordCount>
    <RequestId>66E164C1-D7F2-4D85-849D-E2883FCFFBA5</RequestId>
    <PageRecordCount>0</PageRecordCount>
</DescribeSQLLogFilesResponse>
```

JSON format

```
{
  "Items":{
    "LogFile":[

    ]
  },
  "PageNumber":1,
  "TotalRecordCount":0,
  "RequestId":"66E164C1-D7F2-4D85-849D-E2883FCFFBA5",
  "PageRecordCount":0
}
```


2.11.1.11.4. DescribeSQLLogRecords

Description

You can call this operation to query the SQL audit logs of an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSQLLogRecords.
DBInstanceId	String	Yes	The ID of the instance.
Database	String	No	The database to be queried. All databases are queried by default.
User	String	No	The username to be queried. All users are queried by default.

Parameter	Type	Required	Description
Form	String	No	• File: generates audit log files. If you set this parameter to File, only common response parameters will be returned. Therefore, you need to call the DescribeSQLLogFiles operation to obtain the download URL of audit log files. • Stream: generates data streams. Default value: Stream.
QueryKeywords	String	No	The keywords that are used for query. Separated multiple keywords with spaces. You can enter up to 10 keywords.
StartTime	String	Yes	The start time of the audit logs to be queried. Specify the time in the `yyyy-MM-ddTHH:mm:ssZ` format.
EndTime	String	Yes	The end time of the audit logs to be queried. Specify the time in the `yyyy-MM-ddTHH:mm:ssZ` format. The end time must be later than the start time.
PageSize	Integer	No	The number of entries to return on each page. Valid values: 30, 50, and 100. Default value: 30
PageNumber	Integer	No	The number of the page to return. Valid values: any non-zero positive integer. Default value: 1

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
TotalRecordCount	Integer	The total number of logs.
PageNumber	Integer	The number of the page.
PageRecordCount	Integer	The number of SQL logs on the current page.
Items	List<SQLRecord>	None

SQLRecord parameters

Parameter	Type	Description
DBName	String	The name of the database.
AccountName	String	The name of the account.
HostAddress	String	The IP address of the client.
SQLText	String	The SQL statement recorded in the log.
TotalExecutionTimes	Long	The time consumed to execute the statement. Unit: microseconds.
ReturnRowCounts	Long	The number of records returned.
ThreadID	String	The ID of the thread.
ExecuteTime	String	The time when the statement is executed. It is in the `yyyy-MM-ddTHH:mm:ssZ` format, for example, 2011-05-30T12:11:20Z.

Sample requests

```
https://gpdb.example.com/?Action=DescribeSQLLogRecords
&DBInstanceId=gp-xxxxxxxxxxxxxx
&StartTime=2018-07-09T04:50:20Z
&EndTime=2018-07-09T08:50:20Z
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeSQLLogRecordsResponse>
  <Items></Items>
  <TotalRecordCount>0</TotalRecordCount>
  <PageNumber>1</PageNumber>
  <RequestId>9B24F29F-BA7F-47A3-838E-C6A993888388</RequestId>
  <PageRecordCount>0</PageRecordCount>
</DescribeSQLLogRecordsResponse>
```

JSON format

```
{
  "Items":{
    "SQLRecord":[
    ]
  },
  "TotalRecordCount":0,
  "PageNumber":1,
  "RequestId":"9B24F29F-BA7F-47A3-838E-C6A993888388",
  "PageRecordCount":0
}
```

2.11.1.11.5. ModifySQLCollectorPolicy

Description

You can call this operation to enable or disable the SQL collection feature for the instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to ModifySQLCollectorPolicy.
DBInstanceId	String	Yes	The ID of the instance.

Parameter	Type	Required	Description
SQLCollectorStatus	String	Yes	• Enabled: specifies whether to enable SQL collection. • Disabled: specifies whether to disable SQL collection.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ModifySQLCollectorPolicy
&DBInstanceId=gp-xxxxxxxxxxxxxx
&SQLCollectorStatus=Enable
&<Common request parameters>
```

Sample responses

XML format

```
<ModifySQLCollectorPolicyResponse>
      <RequestId>4FA1F1D1-50A6-4F60-9A78-5752F2076A53</RequestId>
</ModifySQLCollectorPolicyResponse>
```

JSON format

```
{
  "RequestId":"4FA1F1D1-50A6-4F60-9A78-5752F2076A53"
}
```

2.11.1.12. Network management

2.11.1.12.1. AllocateInstancePublicConnection

Description

You can call this operation to specify the prefix of a public connection string of an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to AllocateInstancePublicConnection.
DBInstanceId	String	Yes	The ID of the instance.
ConnectionStringPrefix	String	Yes	Specifies the connection string that contains the prefix.
Port	String	Yes	Specifies the port number. Valid values: 3200 to 3999.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=AllocateInstancePublicConnection
&DBInstanceId=gp-xxxxxxxxxxxxxx
&ConnectionStringPrefix=gp-bp1v8537p9k010lx6o
&Port=3432
&<Common request parameters>
```

Sample responses

XML format

```
<AllocateInstancePublicConnectionResponse>
    <RequestId>ADD6EA90-EECB-4C12-9F26-0B6DB58710EF</RequestId>
</AllocateInstancePublicConnectionResponse>
```

JSON format

```
{
  "RequestId": "ADD6EA90-EECB-4C12-9F26-0B6DB58710EF"
}
```

2.11.1.12.2. DescribeDBInstanceNetInfo

Description

You can call this operation to query the connection information of an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDBInstanceNetInfo.
DBInstanceId	String	Yes	The ID of the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.
DBInstanceNetInfos	List<DBInstanceNetInfo>	The connection information of the instance.
InstanceNetworkType	String	• Classic: classic network • VPC: Virtual Private Cloud

DBInstanceNetInfo

Parameter	Type	Description
ConnectionString	String	The connection string of DNS.
IPAddress	String	The IP address of the instance.

Parameter	Type	Description
IPType	String	• The type of IP address of a classic network instance. Valid values: Inner and Public. • The type of IP address of a VPC instance. Valid values: Private and Public.
Port	String	The information of the port.
VPCId	String	The ID of the VPC.
VSwitchId	String	The ID of the VSwitch. Multiple IDs are separated with commas (,).

Sample requests

```
https://gpdb.example.com/?Action=DescribeDBInstanceNetInfo
&DBInstanceId=gp-xxxxxxxxxxxxxx
&<Common request parameters>
```

Sample responses

XML format

```
<DescribeDBInstanceNetInfoResponse>
  <instanceNetworkType>Classic</instanceNetworkType>
  <DBInstanceNetInfos>
    <DBInstanceNetInfo>
      <DBInstanceNetType>1</DBInstanceNetType>
      <connectionString>gp-xxxxxxxxxxxxxx.gpdb.rds.example.com</connectionString>
      <ipAddress>127.0.0.1</ipAddress>
      <port>3432</port>
      <userVisible>1</userVisible>
    </DBInstanceNetInfo>
  </DBInstanceNetInfos>
  <RequestId>7565770E-7C45-462D-BA4A-8A5396F2CAD1</RequestId>
</DescribeDBInstanceNetInfoResponse>
```

JSON format

```
{
  "instanceNetworkType":"Classic",
  "DBInstanceNetInfos": {
   "DBInstanceNetInfo": [
    {
      "DBInstanceNetType":"1",
       "connectionString":"gp-xxxxxxxxxxxxx.gpdb.rds.example.com",
       "ipAddress":"127.0.0.1",
       "port":"3432",
       "userVisible":1
    }
   ]
  },
  "RequestId": "7565770E-7C45-462D-BA4A-8A5396F2CAD1"
 }
```


2.11.1.12.3. ModifyDBInstanceConnectionString

Description

You can call this operation to modify the connection string and the port of an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceConnectionString.
DBInstanceId	String	Yes	The ID of the instance.
CurrentConnectionString	String	Yes	The connection string used by the instance.
ConnectionStringPrefix	String	Yes	The connection string to be used by the instance.
Port	String	No	The port to be used by the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ModifyDBInstanceConnectionString
&DBInstanceId=gp-xxxxxxxxxxxxx
&CurrentConnectionString=gp-bp1gjo105888f3b69.gpdb.rds.example.com
&ConnectionStringPrefix=gp-bp1gjo105888f3b69new
&<Common request parameters>
```

Sample responses

XML format

```
<ModifyDBInstanceConnectionStringResponse>
      <RequestId>29B0BF34-D069-4495-92C7-FA6D94528A9E</RequestId>
</ModifyDBInstanceConnectionStringResponse>
```

JSON format

```
{
    "RequestId":"29B0BF34-D069-4495-92C7-FA6D94528A9E"
 }
```

2.11.1.12.4. ModifyDBInstanceNetworkType

Description

You can call this operation to switch the network type of the instance between VPC and classic network.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyDBInstanceNetworkType.
DBInstanceId	String	Yes	The ID of the instance.
InstanceNetworkType	String	Yes	Specifies the type of the network. Valid values: • VPC: Virtual Private Cloud • Classic: classic network
VPCId	String	No	The ID of the VPC.
VSwitchId	String	No	The ID of the VSwitch. If you specify the VPCId parameter, you must also specify this parameter.
PrivateIpAddress	String	No	You can specify the IP address of the VPC to which the VSwitch belongs. If no IP address is specified, the system automatically assigns an IP address based on the VPCId and VSwitchId.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ModifyDBInstanceNetworkType
&DBInstanceId=gp-xxxxxxxxxxxxxx
&InstanceNetworkType=VPC
&<Common request parameters>
```

Sample responses

XML format

```
<ModifyDBInstanceNetworkTypeResponse>
      <RequestId>2d0c35a9-f5da-44ba-852d-741e27b7eb0b</RequestId>
</ModifyDBInstanceNetworkTypeResponse>
```

JSON format

```
{
 "RequestId":"2d0c35a9-f5da-44ba-852d-741e27b7eb0b"
}
```

2.11.1.12.5. ReleaseInstancePublicConnection

Description

You can call this operation to release the public connection string of an instance.

Request parameters

Parameter	Type	Required	Description
<Common request parameters>	-	Yes	For more information, see Common parameters.
Action	String	Yes	The operation that you want to perform. Set the value to ReleaseInstancePublicConnection.
DBInstanceId	String	Yes	The ID of the instance.
CurrentConnectionString	String	Yes	The public connection string of the instance.

Response parameters

Parameter	Type	Description
<Common response parameters>	-	For more information, see Common response parameters.

Sample requests

```
https://gpdb.example.com/?Action=ReleaseInstancePublicConnection
&DBInstanceId=gp-xxxxxxxxxxxxxx
&CurrentConnectionString=gp-xxxxxxxxxxxxxx.gpdb.rds.example.com
&<Common request parameters>
```

Sample responses

XML format

```
<ReleaseInstancePublicConnectionResponse>
      <RequestId>9CEF7037-4158-4A65-BEC7-2A1541F6FE74</RequestId>
</ReleaseInstancePublicConnectionResponse>
```

JSON format

```
{
  "RequestId": "9CEF7037-4158-4A65-BEC7-2A1541F6FE74"
}
```

2.11.1.13. Appendix

2.11.1.13.1. Error codes

2.11.1.13.1.1. Client error codes

Common errors

Error code	Error message	HTTP status code
MissingParameter	The input parameter “parameter name” that is mandatory for processing this request is not supplied.	400
InvalidParameter	The specified parameter “Action or Version” is not valid.	400
InvalidAccessKeyId.NotFound	The Access Key ID provided does not exist in our records.	404
IncompleteSignature	The request signature does not conform to Aliyun standards.	400
IllegalTimestamp	The input parameter “Timestamp” that is mandatory for processing this request is not supplied.	400
InvalidOwnerId	The specified OwnerId is not valid.	400

Error code	Error message	HTTP status code
InvalidOwnerAccount	The specified OwnerAccount is not valid.	400
InvalidOwner	OwnerId and OwnerAccount can't be used at one API access.	400
Throttling	Request was denied due to request throttling.	400
InvalidAction	The specified action is not valid.	403
ActionUnauthorized	The specified action is not available for you.	403
UnsupportedHTTPMethod	This http method not supported.	403
UnsupportedParameter	The parameter "<parameter name>" is not supported.	400
Forbidden.InstanceNotFound	The specified DB instance does not exist.	404
Forbidden.RAM	The user is not authorized to operate the specified resource, or this operation does not support RAM.	403
Forbedden.NotSupportRAM	This action does not support accessed by RAM mode.	403
Forbidden.RiskControl	This operation is forbidden by Aliyun Risk Control system.	403
InsufficientBalance	Your account does not have enough balance.	400
Forbidden.Authentication	This operation is forbidden by Aliyun Realname Authentication system.	403
Invalid<parameter name>.ValueNotSupported	The specified parameter "parameter name" is not valid.	400
Invalid<parameter name>.Malformed	The specified parameter "parameter name n" is not valid.	400
InvalidParameter	The specified parameter "parameter name n" is not valid.	400

Specific errors

Error code	Error message	HTTP status code
InvalidRegionId.NotFound	The DBInstanceId provided does not exist in our records.	404

Error code	Error message	HTTP status code
InvalidSecurityIPList.Duplicate	The Security IP address is not in the available range or occupied.	400
InvalidSecurityIPListLength.Malformed	The security IP address is beyond the available range or is already used.	400
InvalidEngineVersionInRegion.NotAvailable	The EngineVersion in the Region is not available.	403
InvaildEngineInRegion.NotAvailable	The Engine in the Region is not available.	403
InvaildDBInstanceClassInRegion.NotAvailable	The DBInstanceClass in the Region is not available.	403
OperationDenied	The resource is out of usage.	403
RegionUnauthorized	There is no authority to create instance in the specified region.	403
QuotaExceeded.CreateInstance	The quota of create instance exceeds.	403
InvalidDBInstanceId.NotFound	The specified DBInstanceId does not exist.	404
MissingParameter	The input parameters “DBInstanceClass” and “DBInstanceStorage” all blank or no change.	400
OperationDenied.DBInstanceType	The operation is not permitted due to type of instance.	400
OperationDenied.DBInstanceStorageReduce	The operation is not permitted due to reduce storage.	403
OperationDenied.DBInstanceStatus	The operation is not permitted due to instance status.	403
DependencyViolation	The operation is not permitted due to instance mount read only or guard instance.	403
InvalidConnectionStringPrefix.Duplicate	The connection string is not in the available range or occupied.	400
QuotaExceeded.SwitchTime	The quota of switch time exceed.	400
OperationDenied.LockMode	The operation is not permitted due to lock of instance.	403
InvalidSecurityIps.Duplicate	The quota of security ip exceeds.	400

Error code	Error message	HTTP status code
OperationDenied.CurrentEngineVersion	The operation is not permitted due to specified current version.	400
OperationDenied.ReadOnlyDBInstanceLower	The operation is not permitted due to higher read only instance version.	403
OperationDenied.GuardDBInstanceLower	The operation is not permitted due to higher guard instance version.	403
OperationDenied.MasterDBInstanceState	The status of the specified master instance does not support this operation.	403
QuotaExceeded.DBName	The quota of db exceeds.	400
InvalidDBName.Duplicate	The specified DB name is invalid or already exists.	400
InvalidParameter.Keyword	The specified DBName is a reserved keyword.	400
OperationDenied.DBStatus	The status of the database does not support this operation.	403
OperationDenied.DBInstanceEngine	The operation is not permitted due to engine of instance.	403
FTPServiceUnavailable	The service is unavailable now; wait several minutes and try again.	403
QuotaExceeded.Upload	The quota of file exceeds.	403
InvalidFileName.NotCompleted	The specified “FileName” is not completed.	404
InvalidFileName.NotAvailable	The specified “FileName” is not Available.	404
QuotaExceeded.FileSize	The quota of file size exceeds.	403
QuotaExceeded.DBInstanceStorage	The quota of instance storage exceeds.	403
InvalidDBInfo.Malformed	The specified parameter “DBInfo” is not valid or db not exist.	400
OperationDenied.Region	The operation is not permitted due to different region.	403
OperationDenied.Engine	The operation is not permitted due to different engine.	403

Error code	Error message	HTTP status code
OperationDenied.DBInstanceId	The operation is not permitted due to DBInstanceId and SourceDBInstanceId is same.	403
InvalidTaskId.NotFound	The ImportId provided does not exist in our records.	400
OperationDenied.IncorrectTaskStatus	The operation is not permitted due to status of import.	403
InvalidAccountName.keyword	The specified AccountName is a reserved keyword.	400
InvalidAccountName.Duplicate	The specified AccountName already exists.	400
QuotaExceeded.AccountName	The quota of account exceeds.	403
OperationDenied.AccountStatus	The status of the account does not support this operation.	403
InvalidDBName.NotFound	The specified database does not exist.	404
OperationDenied.AccountType	The operation is not permitted due to type of account.	403
OperationDenied.BackupJobExists	You cannot perform this operation; a backup job exists.	403
OperationDenied.NoDatabase	The operation is not permitted due to no database.	403
InvalidStartTimeAndEndTime.Malformed	The EndTime must be later than or equal to the StartTime.	400
OperationDenied.BackupJobExists	You cannot perform this operation; a backup job exists.	403
InvalidBackupId.NotFound	The BackupId provided does not exist in our records.	404
OperationDenied.NotFoundBackup	The operation is not permitted due to no backup.	403
OperationDenied.BackupStatus	The operation is not permitted due to type of backup.	403
OperationDenied.BackupMethod	The operation is not permitted method of backup.	403
OperationDenied.TempDBInstanceExists	You cannot perform this operation; a temp instance exists.	403

Error code	Error message	HTTP status code
Forbidden.Authentication	The operation is forbidden by Aliyun Realname Authentication System.	403
IncorrectDBInstanceConnType	Current DB instance conn type does not support this operation.	404
IncorrecttVpcId.Mismatch	The specified parameter "VpcId" is not valid.	400
IntranetNetTypeNotExists	Current DB instance net type does not support this operation.	404
InvalidDBInstanceName.NotFound	The DBInstanceId provided does not exist in our records.	403
InvalidConnectionMode.ValueNotSupported	The specified parameter “ConnectionMode” is not valid.	400
InvalidConnectionString.Duplicate Specified	connection string already exists in the Aliyun RDS.	403
InvalidConnectionString.Duplicate Specified	connection string or port want to be modified is the same with current net type.	400
InvalidConnectionStringPrefix.Duplicated	The specified connection string already exists.	403
InvalidCurrentConnectionString.NotFound	Specified current connection string doesn’t exist.	400
InvalidDBInstanceId.NotFound	The specified DBInstanceId does not exist.	400
InvalidDBInstanceId.QuotaExceeded	The quota of instance id exceeds.	400
InvalidDBInstanceNetType.NotFound	The Specified DB instance net type is not found.	404
InvalidDBinstanceNetType.ValueNotSupport	The specified parameter “DBinstanceNetType” is not valid.	400
InvalidDBInstanceType.ValueNotSupport	The specified parameter “DBInstanceType” is not valid.	400
InvalidEngineVersion.Malformed	The specified parameter “EngineVersion” is not valid.	400
InvalidInstanceNetworkType.ValueNotSupported	The specified parameter “InstanceNetworkType” is not valid.	400

Error code	Error message	HTTP status code
InvalidParameter	The specified parameter “dbInstanceId” is not valid.	400
InvalidPort.Malformed	Specified port is not valid.	400
InvalidPrivateIpAddress.Duplicated	Specified private IP address is duplicated.	400
InvalidPrivateIpAddress.Mismatch	Specified private IP address is not in the CIDR block of virtual switch.	400
InvalidVPCId.NotFound	The specified connection string or port does not match the current network type.	400
InvalidVSwitchId.Mismatch	Specified instance and virtual switch are not in the same zone.	400
InvalidVSwitchId.NotFound	Specified virtual switch is not found in specified VPC.	400
NetTypeExists	Specified net type already existed.	400
NetTypeExists	Specified public net type already existed.	403
OperationDenied.DBInstanceNetType	The network type of the specified instance does not support this operation.	403
OperationDenied.DBInstanceStatus	The specified connection string or port does not match the current network type.	403
OperationDenied.DBInstanceType	The operation is not permitted due to type of instance.	403
OperationDenied.LockMode	The instance is locked.	403
OperationDenied.Switch	Specified instance cannot be switched.	400
OperationDenied.Switch	Specified instance cannot be switched to VPC.	403
OperationDenied.SwitchToVPC	Specified instance cannot be switched to VPC.	403
OperationDenied	The requested resource is sold out in the specified zone; try other types of resources or other regions and zones.	403
OperationDenied	The vpc cloudinstanceIp is use, please check params.	406
OperationDenied	The vpc service is error, please check params.	400

Error code	Error message	HTTP status code
PARAMETER_ERROR	The vpc request parameter may not be null.	406
PARAMETER_MUST_NOT_NULL	The parameter must not be null.	406
PublicConnectionExists	PublicConnection exists.	403
bpcIzNoNotEqualsRdsMultIzNo	Specified vpc IzNo not equal rds IzNo.	400
IncorrectDBInstanceState	CurrentDB instance state does not support this operation.	403
IncorrectDBInstanceType	CurrentDB instance type does not support this operation.	400
IncorrectDBInstanceLockMode	CurrentDB instance lock mode does not support this operation.	400
ParamNotSupportedForCurrentVersion	Parameteris not supported for current version.	400
InvalideStatus.Format	MigrateTask Status is not valid.	400
EngineVersionNotSupported	EngineVersion specified cannot be replicate with the source DB Instance.	400
EngineNotSupported	Engine specified cannot be supported the operation.	400
ConnectionModeNotSupported	ConnectionMode specified cannot be replicate with the source DB Instance.	400
InvalidConfigurationValue.Malformed	Specified ConfigurationValue is not valid.	403
InvalidConfigurationValueStatus.Malformed	Specified ProxyConfigurationValue (status) is not valid.	403
InvalidConfigurationValueOrther.Malformed	Specified ProxyConfigurationValue (check_interval_seconds or max_failed_login_attempts or blocking_seconds) is not valid.	403
ProxyConnectionPersistExists	Specified same ProxyConnectionPersist already exists.	400
ProxyConnectionPersist.NotFound	Specified same ProxyConnectionPersist already exists.	400
ProxyConnectionPersist.NotFound	Specified ProxyConnectionPersist is not found.	400

Error code	Error message	HTTP status code
ProxyConnectionPersistParametersInvalid	ProxyConnectionPersist parameter out of range	400
InvalidConfigValue	ProxyConnectionPersist parameter config table not exits or data error.	400
InvalidDBInstance.NotFound	Specified instance does not exist or not support.	400
ProxyConnectionPersist.NotFound	Specified ProxyConnectionPersist is not found.	400
ProxyConnectionPersistParametersInvalid	ProxyConnectionPersist parameter out of range.	400
InvalidConfigValue	parameter config table not exits or data error.	400

2.11.1.13.1.2. Server error codes

Error code	Error message	HTTP status code
ServiceUnavailable	The request has failed due to a temporary failure of the server.	503
InternalError	The request processing has failed due to some unknown error, exception or failure.	500

2.11.1.13.2. Instance types

Instance types

Instance type	vCPU	Memory (MB)	Storage space (GB)	Storage space (Mbit/s)	Disk type
gpdb.group.segsdx1	1	8,192	80	150	SSD
gpdb.group.segsdx2	2	16,384	160	300	SSD
gpdb.group.segsdx16	16	131,072	1,280	2,400	SSD

2.11.1.13.3. Performance parameters

Performance parameters

API parameter	Description
Gpdb_IOPS	The input/output operations per second (IOPS) of the instance. It is in the data_iops&write_iops&read_iops format.
IOPSUsage	The IOPS usage rate of the instance.
CpuUsage	The CPU utilization of the instance.
ConnectionUsage	The connection usage rate of the instance.
Gpdb_session	The number of connections to the instance.
Gpdb_SpaceUsage	The disk usage of the instance. Unit: MB. It is in the ins_size&data_size&log_size&other_size format.
DiskUsage	The disk usage rate of the instance.
Gpdb_BPS	The bytes per second (BPS) size of the instance. Unit: byte. It is in the data_bps&write_bps&read_bps format.
BPSUsage	The BPS usage rate of the instance.
MemoryUsage	The memory usage rate of the instance.
Gpdb_memory	The memory usage of the instance. Unit: MB.

2.11.1.13.4. Instance states

Instance states

State	Description
Creating	The instance is being created.
Running	The instance is in the running state.
Deleting	The instance is being deleted.
Rebooting	The instance is being restarted.
DBInstanceClassChanging	The instance specifications are being changed.
Transfering	The instance is being migrated.
EngineVersionUpgrading	The engine version is being upgraded.
TransferingToOtherInstance	The data is being migrated to other instances of AnalyticDB for PostgreSQL.
GuardDBInstanceCreating	The disaster recovery instance is being created.

State	Description
Restoring	The instance is being restored from the backup.
Importing	The data is being imported.
ImportingFromOtherInstance	The data is being imported from other instances of AnalyticDB for PostgreSQL.
DBInstanceNetTypeChanging	The network type is being changed.
GuardSwitching	The instance is undergoing disaster recover failover.

2.11.1.13.5. Terms

Terms

Term	Full name	Description
DBInstance	database instance	A database service process that takes up physical memory independently. You can configure different memory size and disk space. The memory size determines the performance of the instance, such as the IOPS and connections.
DBInstanceId	database instance ID	A globally unique name that identifies an instance.
Group	compute group	A compute group is the minimum computing and resource storage unit of an AnalyticDB for PostgreSQL database that you can purchase.
DBInstanceClass	group instance class	The group types are as follows: • **gpdb.group.segsdx1**: 1 vCPU, 8 GB of memory, and 80 GB of SSD storage space. • **gpdb.group.segsdx2**: 2 vCPUs, 16 GB of memory, and 160 GB of SSD storage space. • **gpdb.group.segsdx16**: 16 vCPUs, 128 GB of memory, and 1.28 TB of SSD storage space. In addition to a segment, each type of compute group has a mirror node that has the same specifications as the segment.

Term	Full name	Description
DBInstanceGroupCount	group count	The number of compute groups indicates the number of AnalyticDB for PostgreSQL groups in the instance that you have purchased. For example: If the value of DBInstanceClass is gpdb.group.segsdx2, the instance has two compute groups. Total available resources: 4 vCPUs, 32 GB of memory, and 320 GB of SSD storage space. For resource and performance reasons, the valid value of DBInstanceGroupCount strictly corresponds to DBInstanceClass: • gpdb.group.segsdx1: 2 • gpdb.group.segsdx2: 2, 4, and 8 • gpdb.group.segsdx16: 2 and 4
DB Account	database account	An account identifies the access permissions of a database. A database can be created with multiple accounts, and an account can be associated with multiple databases.
AccountName	database account name	The name of a database account identifies the account. The name must be unique among all the database accounts that are in the same instance.
Region	region	The region indicates the data center in the specified region.

2.11.2. SDK reference

2.11.2.1. Java SDK

2.11.2.1.1. Quick start

This topic describes how to obtain and use the *AnalyticDB for PostgreSQL* Java SDK.

Preparation

- You must have an Apsara Stack account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the Java SDK For more information about how to view and obtain your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.
- For more information about how to obtain the service endpoint, see Obtain an endpoint.

- The Apsara Stack Java SDK supports JDK 1.6 and later.

Installation

If you use Apache Maven to manage Java projects, you only need to import the JAR file to the *pom.xml* file of the project.

To use the SDK of a service, you must install the service SDK and the SDK core library.

The version of the SDK core library is 3.7.1, and the version of the *AnalyticDB for PostgreSQL* SDK is *3.7.1*.

```
<dependencies>
 <dependency>
  <groupId>com.aliyun</groupId>
  <artifactId>aliyun-java-sdk-core</artifactId>
  <version>3.7.1</version>
  <scope>system</scope>
  <systemPath>${project.basedir}/lib/aliyun-java-sdk-core-3.7.1.jar</systemPath>
 </dependency>
</dependencies>
```

Usage

The following code provides an example of how to use the Java SDK:

1. Create and initialize a DefaultAcsClient instance.
2. Create an API request and configure the parameters.
3. Initiate the request and handle the response or exception.

```
import com.example.CommonRequest;
import com.example.CommonResponse;
import com.example.DefaultAcsClient;
import com.example.exceptions.ClientException;
import com.example.exceptions.ServerException;
import com.example.http.FormatType;
import com.example.http.MethodType;
import com.example.profile.DefaultProfile;
import com.example.profile.IClientProfile;

public class CommonTest {
    private static final String regionId = "your-region-id";
    private static final String userAccessKeyId = "your-access-key-id";
    private static final String userAccessKeySecret = "your-access-key-secret";
    private static final String crEndpointDomain = "cr-endpoint-domain";

    public static void main(String[] args) throws Exception {
```

```
        // Create and initialize a DefaultAcsClient instance.
        IClientProfile profile = DefaultProfile.getProfile(regionId, userAccessKeyId, userAccessKeySecre
t);
        DefaultProfile.addEndpoint(regionId, regionId, "cr", crEndpointDomain);
        DefaultAcsClient client = new DefaultAcsClient(profile);

        // Create an API request and configure the parameters.
        CommonRequest request = new CommonRequest();
        request.setDomain("cr.cn-hangzhou.example.com");
        request.setVersion("2016-06-07");
        request.setUriPattern("/users");
        request.setMethod(MethodType.PUT);
        String content = "{\"User\":{\"Password\":\"As123456\"}}\n";
        request.setHttpContent(content.getBytes(),"UTF-8", FormatType.JSON);

        try {
            CommonResponse response = client.getCommonResponse(request);
            System.out.println(response.getData());
        } catch (ServerException e) {
            e.printStackTrace();
        } catch (ClientException e) {
            e.printStackTrace();
        }
    }

}
```

2.11.2.1.2. Use the Java SDK

2.11.2.1.2.1. Install the Java SDK

This topic describes how to install and call the Java SDK of *AnalyticDB for PostgreSQL*.

The Apsara Stack Java SDK supports JDK V1.6 and later. You can import JAR files to install the JDK.

Click here to download JAR files of *AnalyticDB for PostgreSQL*.

If you are using Eclipse or IntelliJ as the integrated development environment, install the *AnalyticDB for PostgreSQL* Java SDK by importing the JAR files.

The installation methods are as follows:

- Use Eclipse

  Complete the following steps to install the AnalyticDB for PostgreSQL Java SDK in Eclipse projects:

i. Copy the downloaded `aliyun-java-sdk-gpdb-version.jar` file to your project folder.

ii. Open your project in Eclipse, right-click the project, and choose **Properties** from the shortcut menu.

iii. In the dialog box that appears, choose **Java Build Path** > **Libraries** > **Add JARs** to add the downloaded JAR file.

iv. Click **Apply and Close**.

- Use IntelliJ

  Complete the following steps to install the Apsara Stack Java SDK in IntelliJ projects:

  i. Copy the downloaded `aliyun-java-sdk-gpdb-version.jar` file to your project folder.

  ii. Open your project in IntelliJ. In the menu bar, choose **File** > **Project Structure**.

  iii. Click **Apply**, and then click **OK**.

2.11.2.1.2.2. Configure authentication credentials

When using Apsara Stack SDKs to access Apsara Stack services, you must provide an Apsara Stack account for authentication.

The Java SDK supports authentication through an AccessKey pair. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

If you want to use your AccessKey pair to access Apsara Stack, you must configure the AccessKey pair as a credential when you initialize the client.

> **Notice** Do not disclose any code that may contain your AccessKey pair. For example, do not commit the code to public GitHub projects. Otherwise, your Apsara Stack account may be compromised.

```
DefaultProfile profile = DefaultProfile.getProfile(
  "<your-region-id>",        // The ID of the region where your instance is located.
  "<your-access-key-id>",    // The AccessKey ID of your account.
  "<your-access-key-secret>"); // The AccessKey Secret of your account.
```

2.11.2.1.2.3. Initiate a request

This topic describes how to initiate a request by calling the Java SDK of *AnalyticDB for PostgreSQL*.

Procedure

1. Create an AcsClient instance.

   ```
   IAcsClient client = new DefaultAcsClient(profile);
   ```

2. Create a request.

   The naming convention for requests is `${apiName}Request`. ${apiName} indicates the API operation name, such as *DescribeDBInstances*.

When the SDKs of multiple services are used, different requests may have the same name. Differentiate the requests by SDK package.

```
DescribeDBInstancesRequest request = new DescribeDBInstancesRequest();
request.setPageSize(10);
```

3. Initiate a request and handle the response.

```
DescribeDBInstancesResponse response;
try {
   response = client.getAcsResponse(request);
   for (DescribeDBInstancesResponse.Instance instance:response.getInstances()) {
      System.out.println(instance.getPublicIpAddress());
   }
} catch (ServerException e) {
   e.printStackTrace();
} catch (ClientException e) {
   e.printStackTrace();
}
```

All returned fields are deserialized into the response. You can call `response.getXXX()` to obtain the response fields.

```
instanceStatus := response.getStatus()
```

However, if an exception occurs or if you require the original HTTP response, you can use `doAction()` to obtain the original response.

```
HttpResponse response = client.doAction(request);
```

2.11.2.1.2.4. Troubleshooting

If an error occurs on the server side or SDK side, the Apsara Stack Java SDK returns the corresponding exception message. An exception message contains the detailed error information, namely the error code and the error message.

Generally, you are not required to handle the errors returned by the Apsara Stack Java SDK. You are only required to handle the errors on the server side according to the error message.

- `ServerException` is the error message on the server side.
- `ClientException` is the error message on the SDK side.

For example, if the following error occurs, modify the ID of AccessKey according to the detailed error message.

```
com.aliyuncs.exceptions.ClientException: InvalidAccessKeyId.NotFound : Specified access key is not found.
```

To handle the errors returned by the Apsara Stack Java SDK, see the following code example for reference:

```
try {
    FooResponse response = client.getAcsResponse(request);
    // Handle the response.
    // ...
}catch (ServerException e){
    // Add your own error handling logic here.
    // For example, print the detailed error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
    // If the problem is tricky, open a ticket and provide the RequestId for us.
    System.out.println("ResponseId=" + e.getRequestId());
}catch (ClientException e){
    // Add your own error handling logic here.
    // For example, print the detailed error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
}
```

2.11.2.1.2.5. Common errors

This topic describes the common errors when you use Java SDK and how to troubleshoot the problems based on the corresponding causes and solutions.

Error code	Error message	Cause	Solution
SDK.CanNotResolveEndpoint	Can not resolve endpoint, please check the user guide	The SDK cannot automatically obtain the endpoint of the called service in the specified region.	Check whether the provided region ID and endpoint are correct. After obtaining the correct endpoint, use the following code to set the endpoint: `DefaultProfile.addEndpoint("your-region-id", "your-region-id", "product", "endpoint"");`

Error code	Error message	Cause	Solution
SDK.JsonUnmarshalError	Failed to unmarshal response	The SDK response fails to be deserialized. In most cases, the cause is that the structure of the response received by the SDK does not conform to the API metadata, such as mismatched fields or incorrect formatting.	You can use the client.doAction(request) method to obtain the original HTTP response.
SDK.TimeoutError	The request timed out 4 times (3 for retry), perhaps we should have the threshold raised a little?	The request has timed out and all retry attempts have failed.	In scenarios such as poor network quality, we recommend that you prolong the timeout period or increase the maximum number of retries.
SDK.ServerError:InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The API only accepts HTTPS requests and does not accept HTTP requests.	You can add the following code to the request before it is sent: request.setProtocol(ProtocolType.HTTPS)

2.11.2.2. Python SDK

2.11.2.2.1. Quick start

This topic describes how to obtain and use the *AnalyticDB for PostgreSQL* Python SDK.

Preparation

- You must have an Apsara Stack account and an AccessKey pair (AccessKey ID and AccessKey Secret) to use the Python SDK. For more information about how to view and obtain your AccessKey pair in the Apsara Stack console, see Obtain an AccessKey pair.

- For more information about how to obtain the service endpoint, see Obtain an endpoint.

Install the Python SDK

To install the Python SDK, perform the following operations:

1. Install the SDK core library.
   - If you are using Python V2.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core
     ```

   - If you are using Python V3.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core-v3
     ```

2. Install the *AnalyticDB for PostgreSQL* SDK.

   The following code shows how to install the AnalyticDB for PostgreSQL SDK:

   ```
   pip install aliyun-python-sdk-rds
   ```

Usage

The following code provides an example of how to use the Python SDK:

1. Create a client instance. When you create the client instance, you must obtain the region ID, AccessKey ID, and AccessKey Secret.
2. Create an API request and configure the parameters.
3. Initiate the request and handle the response or exception.

```
from aliyunsdkcore import client
from aliyunsdkgpdb.request.v20160101 import DescribeDBInstancesRequest

# global config
region_id = 'xxxxx'
secret_id = 'xxxxx'
secret_key = 'xxxxx'

# product config
product_name = 'AnalyticDB for PostgreSQL'

# setup request
request = DescribeDBInstancesRequest.DescribeDBInstances()

# get response
response = clt.do_action_with_exception(request)

print response
```

2.11.2.2.2. Use the Python SDK

2.11.2.2.2.1. Install the Python SDK

This topic describes how to install and use the *AnalyticDB for PostgreSQL* Python SDK.

The Python SDK supports Python V2.6.x, 2.7.x, 3.x, and later. The following installation methods are supported:

- Use pip (recommended)

  Run the following commands to install the Python SDK by using pip:

  ```
  pip install aliyun-python-sdk-core # Install the Apsara Stack SDK core library.
  pip install aliyun-python-sdk-gpdb # Install the AnalyticDB for PostgreSQL SDK.
  ```

  > **Note** If you are using Python V3.x, use the `pip install aliyun-python-sdk-core-v3` command instead of the `pip install aliyun-python-sdk-core` command.

- Use GitHub

  Run the following commands to install the Python SDK by using GitHub:

  ```
  git clone https://github.com/aliyun/aliyun-openapi-python-sdk.git
  # Install the SDK core library.
  cd aliyun-python-sdk-core
  python setup.py install
  # Install the AnalyticDB for PostgreSQL SDK.
  cd aliyun-python-sdk-gpdb
  python setup.py install
  ```

- Use the source code

  i. Download the SDK package and decompress it.

  ii. You can use one of the following methods to install the SDK package:

  - Modify the sys.path variable and add the directory that you need to search for. It is the directory where the SDK package has been decompressed to. Example:

    ```
    >>> import sys
    >>> sys.path.append('/Users/michael/my_py_scripts')
    ```

    > **Note** This modification takes effect only when the instance is running.

  - Configure the PYTHONPATH environment variable and add the directory where you need to decompress the SDK package to. The content of this environment variable is automatically added to the module search directory.

    The configuration of the environment variable PYTHONPATH is similar to that of the environment variable Path.

- Place the decompressed SDK package in the project. The Python SDK is now available to be used in your project.

2.11.2.2.2.2. Configure authentication credentials

When using Apsara Stack SDKs to access Apsara Stack services, you must provide an Apsara Stack account for authentication.

The Python SDK supports authentication through an AccessKey pair. For more information about how to obtain an AccessKey pair, see Obtain an AccessKey pair.

If you want to use your AccessKey pair to access Apsara Stack, you must configure the AccessKey pair as a credential when you initialize the client.

> **Notice** Do not disclose any code that may contain your AccessKey pair. For example, do not commit the code to public GitHub projects. Otherwise, your Apsara Stack account may be compromised.

```
clt = client.AcsClient(secret_id, secret_key, region_id)
```

2.11.2.2.2.3. Initiate a request

This topic describes how to initiate a request by calling the Python SDK of *AnalyticDB for PostgreSQL*.

Procedure

1. Import the SDK of the service.

```
 from aliyunsdkcore import client
from aliyunsdkgpdb.request.v20160101
import DescribeDBInstancesRequest
```

2. Create an AcsClient instance.

```
client = AcsClient(
   "<your-access-key-id>",
   "<your-access-key-secret>",
   "<your-region-id>"
 );
```

3. Create a request and configure the required parameters.

```
request = DescribeDBInstancesRequest.DescribeDBInstances()
```

4. Initiate an API request and display the response.

```
response = client.do_action_with_exception(request)
 print response
```

2.11.2.2.2.4. Set HTTPS requests

The Python SDK allows you to make API requests over HTTP and HTTPS.

When using the Python SDK, you can specify a default protocol (HTTP or HTTPS) for requests to different services, or set a global protocol for all requests.

> **Note** The default HTTP or HTTPS protocol for each service takes precedence over the global protocol.

Add OpenSSL support

The HTTPS protocol for Python SDK is supported by the OpenSSL of Python. To send HTTPS requests by using the Python SDK, you must add OpenSSL support in Python.

Run the `python -c "import ssl"` command to check whether your Python environment supports OpenSSL. If the error message `ImportError: No module named ssl` is not displayed, OpenSSL is supported.

If OpenSSL is not supported, run the following command to install OpenSSL:

```
pip install pyopenssl
```

Specify the HTTP or HTTPS protocol for a request

The following example shows how to specify the HTTPS protocol for a request:

```
request = DescribeDBInstancesRequest.DescribeDBInstances()
request.set_protocol_type("https")
# Valid values: "https" and "http".
```

Set a global protocol for all requests

The following example shows how to set a default global protocol for all requests:

```
import aliyunsdkcore.request
aliyunsdkcore.request.set_default_protocol_type("https")
# Create a request and call client.do_action_with_exception() to send the request.
```

2.11.2.2.2.5. Troubleshooting

If an error occurs on the server side or SDK side when you use the Python SDK, the Python SDK returns the corresponding exception message. An exception message contains the detailed error information, namely the error code and the error message.

Generally, you are not required to handle the errors returned by the Python SDK. You are only required to handle the errors on the server side according to the error message.

- `ServerException` is the error message on the server side.
- `ClientException` is the error message on the SDK side.

For example, if the following error occurs, modify the ID of AccessKey according to the detailed error message.

```
aliyunsdkcore.acs\_exception.exceptions.ServerException: HTTP Status: 404 Error:InvalidAccessKeyId.N
otFound Specified access key is not found.
```

To handle the errors returned by the Python SDK, see the following code example for reference:

```
try:
    response = client.do_action_with_exception(request)
except ServerException as e:
    # Add your own error handling logic here.
    # For example, print the detailed error message.
    print e.get_http_status()
    print e.get_error_code()
    print e.get_error_msg()
```

2.11.2.2.2.6. Common errors

This topic lists the causes and solutions for some common errors you may experience when you use the SDK.

Error code	Error message	Cause	Solution

`SDK.InvalidRegionId`	`Can not find endpoint to access.`	The error message returned because the SDK failed to automatically obtain the endpoint of the requested service in the specified region.	Check whether the specified region ID and endpoint are correct. After you have obtained the endpoint, you can run the following code to set the endpoint:
			`from aliyunsdkcore.profile import region_provider`
			`region_provider.modify_point('product_name', 'region_id', 'endpoint')`

`SDK.TimeoutError`	—	The error message returned because the request timed out and all retries failed.	In low network quality scenarios, we recommend that you increase the timeout period or the maximum number of retries.

Error code	Error message	Cause	Solution
SDK.ServerError: InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The error message returned because you made an HTTP request. The API only accepts HTTPS requests.	Before you send a request, add the following code: request.set_protocol_type('https')

2.11.2.3. Obtain an AccessKey pair

You can obtain the AccessKey pair on the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**.

   The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.11.2.4. Obtain an endpoint

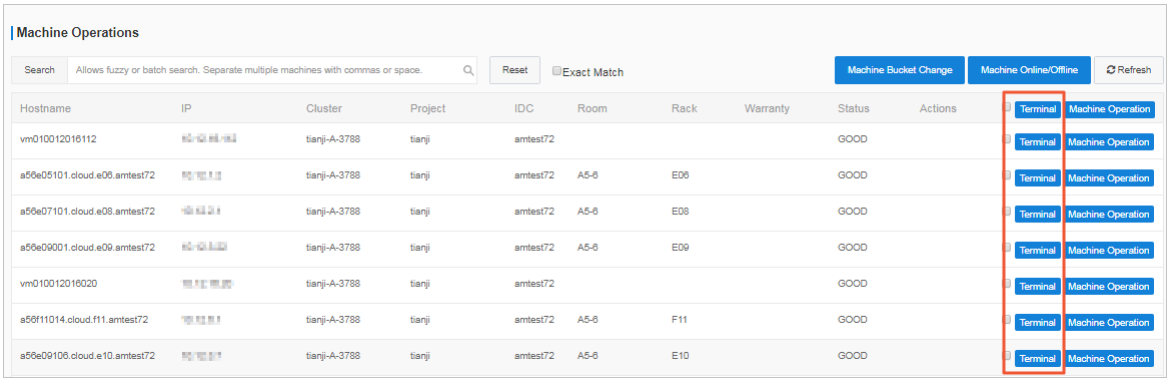
You can obtain the product endpoint in Apsara Stack Operations.

Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms** > **Apsara Stack Operations** > **Log on to Apsara Stack Operations**

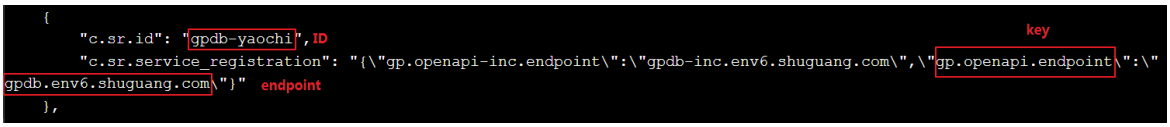
in *Operations Guide* .

2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. Choose **Operations** > **Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the command **curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration"** to obtain JSON data.

7. You can find the endpoint of *AnalyticDB for PostgreSQL* by using the ID (*gpdb-yaochi*) and key value (*gp.openapi.endpoint*) of the *AnalyticDB for PostgreSQL* service.



2.12. Data Transmission Service (DTS)

2.12.1. API reference

2.12.1.1. Call OpenAPI

2.12.1.1.1. API overview

This topic describes the APIs that DTS OpenAPI supports.

Data migration APIs

API	Description
ConfigureMigrationJob	Configures a migration task.
StartMigrationJob	Starts or restarts a migration task.
SuspendMigrationJob	Suspends a migration task.
StopMigrationJob	Stops a migration task.
DeleteMigrationJob	Deletes a migration task.
DescribeMigrationJobStatus	Queries the status of a migration task.
DescribeMigrationJobDetail	Queries the details of a migration task.
DescribeMigrationJobs	Queries the list of migration tasks.

Data synchronization APIs

API	Description
CreateSynchronizationJob	Purchases a synchronization instance.
ConfigureSynchronizationJob	Configures a synchronization task.
StartSynchronizationJob	Starts a synchronization task.
SuspendSynchronizationJob	Suspends a synchronization task.
DeleteSynchronizationJob	Deletes a synchronization task.
ModifySynchronizationObject	Modifies the list of objects to be synchronized.
DescribeObjectModifyStatus	Queries the modification status of the list of objects to be synchronized.
DescribeSynchronizationJobStatus	Queries the running status of a synchronization task.
DescribeSynchronizationJobs	Queries the list of synchronization tasks.

API	Description
DescribeInitializationStatus	Queries the initialization status of a synchronization task.

Data subscription APIs

API	Description
CreateSubscriptionInstance	Purchases a subscription channel.
ConfigureSubscriptionInstance	Configures a subscription channel.
StartSubscriptionInstance	Starts a subscription task.
DeleteSubscriptionInstance	Releases a subscription channel.
DescribeSubscriptionInstanceStatus	Queries the status of a subscription channel.
DescribeSubscriptionInstances	Queries the list of subscription instances.
ModifySubscriptionObject	Modifies the list of objects to be subscribed.
ModifyConsumptionTimestamp	Modifies the consumption checkpoint.

2.12.1.2. Data migration APIs

2.12.1.2.1. ConfigureMigrationJob

2.12.1.2.1.1. Overview

You can call this operation to configure a data migration task, including the source and destination instances and the objects to be migrated.

Before a migration task is started, you can call this operation repetitively to modify task configurations.

2.12.1.2.1.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ConfigureMigrationJob.
MigrationJobId	String	Yes	The migration task ID.
MigrationJobName	String	No	The migration task name.

Name	Type	Required	Description
SourceEndpoint.InstanceType	String	Yes	The type of the source instance specified in the migration task. Valid values: • RDS: an RDS instance • ECS: a user-created database in ECS • LocalInstance: a user-created database in a local IDC • MongoDB: an ApsaraDB for MongoDB instance
SourceEndpoint.Region	String	Yes	The region of the source instance. If it is a user-created database, you can select the region geologically nearest to the user-created IDC. Valid values: • cn-hangzhou: Alibaba Cloud in Hangzhou • cn-shanghai: Alibaba Cloud in Shanghai • cn-qingdao: Alibaba Cloud in Qingdao • cn-beijing: Alibaba Cloud in Beijing • cn-zhangbei: Alibaba Cloud in Zhangbei • cn-shenzhen: Alibaba Cloud in Shenzhen • cn-hongkong: Alibaba Cloud in Hong Kong • us-west-1: Alibaba Cloud in Western US • us-east-1: Alibaba Cloud in Eastern US • ap-southeast-1: Alibaba Cloud in Singapore • cn-hangzhou-finance-1: Finance Cloud in Hangzhou • cn-qingdao-finance-1: Finance Cloud in Qingdao • cn-shanghai-finance-1: Finance Cloud in Shanghai • cn-shenzhen-finance-1: Finance Cloud in Shenzhen • me-east-1: Alibaba Cloud in Dubai • en-central-1: Alibaba Cloud in Frankfurt
SourceEndpoint.InstanceId	String	No	The source instance ID. • When the value of SourceEndpoint.InstanceType is RDS, this value is an RDS instance ID. • When the value of SourceEndpoint.InstanceType is ECS, this value is an ECS instance ID. • When the value of SourceEndpoint.InstanceType is MongoDB, this value is an ApsaraDB for MongoDB instance ID.
SourceEndpoint.EngineName	String	No	The database type of the source instance. This parameter is required when the value of SourceEndpoint.InstanceType is not RDS. Valid values: MySQL, SQLServer, PostgreSQL, Oracle, MongoDB, and Redis.

Name	Type	Required	Description
SourceEndpoint.IP	String	No	The connection address of the source instance. This parameter is required when the source instance is a user-created database.
SourceEndpoint.Port	String	No	The listening port of the source instance. This parameter is required when the source instance is a user-created database.
SourceEndpoint.OracleSID	String	No	The Oracle SID when the source instance is an Oracle database.
SourceEndpoint.DatabaseName	String	No	The database name of the source instance used for establishing a connection when the source instance is a PostgreSQL or MongoDB database.
SourceEndpoint.UserName	String	Yes	The username to access the source instance.
SourceEndpoint.Password	String	Yes	The password to access the source instance.
SourceEndpoint.OwnerID	String	Yes	The UID of the Apsara Stack tenant account of the source instance. This parameter is required when the source instance is an RDS instance and uses a different Apsara Stack tenant account from that of the destination instance.
SourceEndpoint.Role	String	Yes	The authorization role granted by the Apsara Stack tenant account of the source instance to the Apsara Stack tenant account of the destination instance. This parameter is required when the source instance is an RDS instance and uses a different Apsara Stack tenant account from that of the destination instance. For the permissions required by this role and authorization method, see Cross-account migration and synchronization.
DestinationEndpoint.InstanceType	String	Yes	The type of the destination instance specified in the migration task. Valid values: • RDS: an RDS instance • ECS: a user-created database on ECS • LocalInstance: a user-created database in a local IDC • MongoDB: an ApsaraDB for MongoDB instance • Redis: a KVStore for Redis instance

Name	Type	Required	Description
DestinationEndpoint.Region	String	Yes	The region of the destination instance. If it is a user-created database, you can select the region geologically nearest to the user-created IDC. Valid values: • cn-hangzhou: Alibaba Cloud in Hangzhou • cn-shanghai: Alibaba Cloud in Shanghai • cn-qingdao: Alibaba Cloud in Qingdao • cn-beijing: Alibaba Cloud in Beijing • cn-zhangbei: Alibaba Cloud in Zhangbei • cn-shenzhen: Alibaba Cloud in Shenzhen • cn-hongkong: Alibaba Cloud in Hong Kong • us-west-1: Alibaba Cloud in Western US • us-east-1: Alibaba Cloud in Eastern US • ap-southeast-1: Alibaba Cloud in Singapore • cn-hangzhou-finance-1: Finance Cloud in Hangzhou • cn-qingdao-finance-1: Finance Cloud in Qingdao • cn-shanghai-finance-1: Finance Cloud in Shanghai • cn-shenzhen-finance-1: Finance Cloud in Shenzhen • me-east-1: Alibaba Cloud in Dubai • en-central-1: Alibaba Cloud in Frankfurt
DestinationEndpoint.InstanceID	String	No	The destination instance ID. • When the value of DestinationEndpoint.InstanceType is RDS, this value is an RDS instance ID. • When the value of DestinationEndpoint.InstanceType is ECS, this value is an ECS instance ID. • When the value of DestinationEndpoint.InstanceType is MongoDB, this value is an ApsaraDB for MongoDB instance ID. • When the value of DestinationEndpoint.InstanceType is Redis, this value is a KVStore for Redis instance ID.
DestinationEndpoint.EngineName	String	No	The database type of the destination instance. This parameter is required when the destination instance is a user-created database. Valid values: MySQL, SQL Server, PostgreSQL, PPAS, MongoDB, and Redis.
DestinationEndpoint.IP	String	No	The connection address of the destination instance. This parameter is required when the destination instance is a user-created database.
DestinationEndpoint.Port	String	No	The listening port of the destination instance. This parameter is required when the destination instance is a user-created database.

Name	Type	Required	Description
DestinationEndpoint.DatabaseName	String	No	The database name of the destination instance used for establishing a connection. This parameter is required when the destination instance is a PostgreSQL, PPAS, or MongoDB database.
DestinationEndpoint.UserName	String	Yes	The username to access the destination instance.
DestinationEndpoint.Password	String	Yes	The password to access the destination instance.
MigrationMode.StructureIntialization	Boolean	Yes	Indicates whether the migration task performs schema migration. Valid values: • true: yes • false: no
MigrationMode.DataIntialization	Boolean	Yes	Indicates whether the migration task performs full data migration. Valid values: • true: yes • false: no
MigrationMode.DataSynchronization	Boolean	Yes	Indicates whether the migration task performs incremental data synchronization. Valid values: • true: yes • false: no
MigrationObject	List	Yes	The objects to be migrated. For more information, see MigrationObject parameter definitions.

2.12.1.2.1.3. MigrationObject parameter definitions

The MigrationObject parameters are defined as JSON strings. Certain regular expressions can be used in the object configuration.

The MigrationObject parameter definitions are as follows:

```
MigrationObject:{
    DBName:'The name of the database to be migrated',
    NewDBName:"The mapped name of the database to be migrated in the destination instance"
    SchemaName:'The name of the schema to be migrated',
    NewSchemaName:'The mapped name of the schema to be migrated in the destination instance',
    TableIncludes:[{
        TableName: 'The name of the table to be migrated',
        NewTableName:'The mapped name of the table to be migrated in the destination instance',
        FilterCondition:'where condition',
        ColumnIncludes:[{
            ColumnName:'The name of the column that needs to be migrated in the table',
            NewColumnName:'The mapped name of the column that needs to be migrated in the destin
ation instance'
        }]
        ColumnExcludes:[{
            ColumnName:'The name of the column that does not need to be migrated in the table'
        }]
    }]
    TableExcludes:[{                    — The table that does not need to be migrated
        TableName:'The name of the table that does not need to be migrated in the database'
    }]
}
```

SchemaName and NewSchemaName are applicable only to SQLServer. DBName and NewDBName are used to specify the names of other databases.

If you only specify DBName but do not specify lower levels of objects, all objects in the database are migrated.

If you specify DBName and some lower levels of objects, the objects that are not specified are not migrated by default.

You can use the following regular expressions to define different object names:

- A period (.) matches any single character except '\r\n'.
- An asterisk (*) matches zero or more occurrences of a subexpression which occurs before. h.*llo matches strings such as hllo and heeeello.
- A question mark (?) matches zero or one occurrence of a subexpression which occurs before. h.?llo matches hllo and hello, but not haello.
- The [characters] character set matches any character included in the braces. For example, h[aello] matches hallo and hello.
- The [^characters] negative character set does not match any character included in the braces. For example, h[^ae]llo matches hcllo and hdllo, but not hallo or hello.
- The [character1-character2] character range matches any character included in the range from character1 to character2, such as [0-9] and [a-z].

2.12.1.2.1.4. Response parameters

Name	Type	Description
Common response parameters	-	The request ID.

2.12.1.2.1.5. Example

The following example shows how to use the Java SDK to configure a migration task.

```
private static void configureMigrationJob(String MigrationJobId){
    String MigrationJobName="jiangliutest";
    /*Source Endpoint*/
    String SourceEndpoint_InstanceType="RDS";
    String SourceEndpoint_Region="cn-hangzhou";
    String SourceEndpoint_InstanceId="rm-xxxxxxxxxxxxxxxxx";
    String SourceEndpoint_UserName="*******";
    String SourceEndpoint_Password="*******";
    /*Destination Endpoint*/
    String DestinationEndpoint_InstanceType="RDS";
    String DestinationEndpoint_InstanceId="rm-xxxxxxxxxxxxxxxxx";
    String DestinationEndpoint_UserName="******";
    String DestinationEndpoint_Password="******";
    Boolean MigrationMode_StructureIntialization=true;
    Boolean MigrationMode_DataIntialization=true;
    Boolean MigrationMode_DataSynchronization=true;
    String MigrationObject="[{\"DBName\":\"jiangliutest\",\"NewDBName\":\"jiangliutest\","
        + "\"TableIncludes\":[{\"TableName\":\"t1\",\"NewTableName\":\"t1\"}]}]";
    ConfigureMigrationJobRequest request = new ConfigureMigrationJobRequest();
    request.setMigrationJobId(MigrationJobId);
    request.setMigrationJobName(MigrationJobName);
    request.setSourceEndpointRegion(SourceEndpoint_Region);
    request.setSourceEndpointInstanceType(SourceEndpoint_InstanceType);
    request.setSourceEndpointInstanceID(SourceEndpoint_InstanceId);
    request.setSourceEndpointUserName(SourceEndpoint_UserName);
    request.setSourceEndpointPassword(SourceEndpoint_Password);
    request.setDestinationEndpointInstanceType(DestinationEndpoint_InstanceType);
    request.setDestinationEndpointInstanceID(DestinationEndpoint_InstanceId);
    request.setDestinationEndpointUserName(DestinationEndpoint_UserName);
    request.setDestinationEndpointPassword(DestinationEndpoint_Password);
    request.setMigrationModeStructureIntialization(MigrationMode_StructureIntialization);
    request.setMigrationModeDataIntialization(MigrationMode_DataIntialization);
    request.setMigrationModeDataSynchronization(MigrationMode_DataSynchronization);
```

```
    request.setMigrationObject(MigrationObject);
    try {
        ConfigureMigrationJobResponse response = client.getAcsResponse(request);
        System.out.println("Configure "+ MigrationJobId+ " Succeed");
    } catch (Exception e) {
        // TODO: handle exception
        System.out.println("Configure "+MigrationJobId + " Failed!") ;
        System.out.println(e.toString());
    }
}
```

2.12.1.2.2. CreateMigrationJob

2.12.1.2.2.1. Overview

You can call this operation to purchase a database migration instance. After the purchase, you need to call the ConfigureMigrationJob operation to configure a migration task.

2.12.1.2.2.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateMigrationJob.
Region	String	Yes	The region of the migration instance. Valid values: • cn-hangzhou: Alibaba Cloud in Hangzhou • cn-shanghai: Alibaba Cloud in Shanghai • cn-qingdao: Alibaba Cloud in Qingdao • cn-beijing: Alibaba Cloud in Beijing • cn-zhangbei: Alibaba Cloud in Zhangbei • cn-shenzhen: Alibaba Cloud in Shenzhen • cn-hongkong: Alibaba Cloud in Hong Kong • us-west-1: Alibaba Cloud in Western US • us-east-1: Alibaba Cloud in Eastern US • ap-southeast-1: Alibaba Cloud in Singapore • cn-hangzhou-finance-1: Finance Cloud in Hangzhou • cn-qingdao-finance-1: Finance Cloud in Qingdao • cn-shanghai-finance-1: Finance Cloud in Shanghai • cn-shenzhen-finance-1: Finance Cloud in Shenzhen • me-east-1: Alibaba Cloud in Dubai • en-central-1: Alibaba Cloud in Frankfurt

Name	Type	Required	Description
MigrationJobClass	String	Yes	The migration task type. Valid values: small, medium, and large. For the testing performance of each instance type, see Data migration types.
ClientToken	String	No	The token used to ensure the idempotence of the request. It can be any string.
OwnerID	String	No	If a RAM user is used to call this operation, the value of OwnerID is the UID of the Apsara Stack tenant account to which this RAM user belongs.

2.12.1.2.2.3. Response parameters

Name	Type	Description
MigrationJobId	String	The migration task ID.

2.12.1.2.2.4. Examples

The following code provides an example of how to use the Java SDK to purchase a migration instance.

```
private static String createMigrationJob(String region,String migrationJobClass) {
        CreateMigrationJobRequest request=new CreateMigrationJobRequest();
        request.setRegion("cn-hangzhou");
        request.setMigrationJobClass("small");
        try {
           CreateMigrationJobResponse response = client.getAcsResponse(request);
           String MigrationJobId = response.getMigrationJobId();
           System.out.println("Create Migration Job succeed. The Migration Job Id is "+MigrationJobId);
           return MigrationJobId;
        } catch (Exception e) {
           // TODO: handle exception
           System.out.println("Create Migration Job failed!" +e.toString());
           return null;
        }
    }
```

2.12.1.2.3. DeletetMigrationJob

2.12.1.2.3.1. Overview

You can call this operation to delete a migration task regardless of its status. After a migration task is deleted, you cannot query or manage it through OpenAPI or the console.

2.12.1.2.3.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeletetMigrationJob.
MigrationJobId	String	Yes	The migration task ID.

2.12.1.2.3.3. Response parameters

Name	Type	Description
Common response parameters	-	The request ID.

2.12.1.2.3.4. Examples

The following code provides an example of how to use the Java SDK to delete a migration task.

```
private static void deleteMigrationJob(String MigrationJobId) {
      DeleteMigrationJobRequest request = new DeleteMigrationJobRequest();
      DeleteMigrationJobResponse response = new DeleteMigrationJobResponse();
      request.setMigrationJobId(MigrationJobId);
      try {
         response = client.getAcsResponse(request);
         System.out.println("Delete Migration Job "+MigrationJobId+" Succeed!") ;
      } catch (Exception e) {
         // TODO: handle exception
         System.out.println("Delete Migration Job "+MigrationJobId+" Failed!") ;
         System.out.println(e.toString());
      }
   }
```

2.12.1.2.4. DescribeMigrationJobDetail

2.12.1.2.4.1. Overview

When a migration task is in the Migrating, MigrationFailed, Suspending, or Finished status, you can call this operation to query data migration details, including the migration status and progress of each object.

2.12.1.2.4.2. Request parameters

Description	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeMigrationJobDetail.
MigrationJobId	String	Yes	The migration task ID.
MigrationMode.StructureInitialization	Boolean	No	The schema migration details.
MigrationMode.DataInitialization	Boolean	No	The full data migration details.
MigrationMode.DataSynchronization	Boolean	No	The incremental data migration details.
PageSize	Integer	No	• The number of records on each page. Valid values: 30, 50, and 100. Default value: 30. • This parameter is required when only one of these three parameters is set to true: MigrationMode.StructureInitialization, MigrationMode.DataInitialization, and MigrationMode.DataSynchronization.

Description	Type	Required	Description
PageNum	Integer	No	• The page number. It must be greater than 0 and smaller than or equal to the maximum value of Integer. Default value: 1. • This parameter is required when only one of these three parameters is set to true: MigrationMode.StructureInitialization, MigrationMode.DataInitialization, and MigrationMode.DataSynchronization.

2.12.1.2.4.3. Response parameters

Name	Type	Description
StructureInitializationDetails	List	The schema migration details. For more information, see StructureInitializationDetail parameter definitions.
DataInitializationDetails	List	The full data migration details. For more information, see DataInitializationDetail parameter definitions.
DataSynchronizationDetails	List	The incremental data migration details. For more information, see DataSynchronizationDetail parameter definitions.

2.12.1.2.4.4. StructureInitializationDetail parameter definitions

Name	Type	Description
ObjectName	String	The name of the object to be migrated.

Name	Type	Description
ObjectType	String	The type of the object to be migrated. Valid values: Table, Constraint, Index, View, MaterializeView, Type, Synonym, Trigger, Function, Procedure, Package, Default, Rule, and Plan Guide.
SourceOwnerDBName	String	The name of the source database from which the object is to be migrated.
DestinationOwnerDBName	String	The schema of the destination database to which the object is to be migrated.
Status	String	The migration status of the object to be migrated.
ErrorMessage	String	The reason why the object failed to be migrated.
ObjectDefinition	String	The schema definition of the object to be migrated.
Constraints	List	Constraints in which the object to be migrated participates. Constraints are active only when the object to be migrated is a table. The list of constraints includes indexes and foreign keys.

2.12.1.2.4.5. DataInitializationDetail parameter definitions

Name	Type	Description
TableName	String	The name of the table to be migrated.
SourceOwnerDBName	String	The name of the source database from which the table is to be migrated.
DestinationOwnerDBName	String	The name of the destination database to which the table is to be migrated.
Status	String	The migration status of the table.

Name	Type	Description
ErrorMessage	String	The reason why the table failed to be migrated.
TotalRowNum	String	The total number of records to be migrated in the table.
FinishRowNum	String	The number of records that have been migrated in the table.
UsedTime	String	The time that has been spent on migrating the table. Unit: second.

2.12.1.2.4.6. DataSynchronizationDetail parameter definitions

Name	Type	Description
TableName	String	The name of the table to be migrated.
SourceOwnerDBName	String	The name of the source database from which the table is to be migrated.
DestinationOwnerDBName	String	The name of the destination database to which the table is to be migrated.
Status	String	The migration status of the table to be migrated.
ErrorMessage	String	The reason why the table failed to be migrated.

2.12.1.2.4.7. Examples

The following code provides an example of how to use the Java SDK to query migration task details.

```
private static void describeMigrationJobDetail(String MigrationJobId) {
    DescribeMigrationJobDetailRequest request = new DescribeMigrationJobDetailRequest();
    request.setMigrationJobId(MigrationJobId);
    request.setMigrationModeStructureInitialization(true);
    request.setMigrationModeDataInitialization(true);
    request.setMigrationModeDataSynchronization(true);
    try {
```

```
    try {
        DescribeMigrationJobDetailResponse response = client.getAcsResponse(request);
        System.out.println("Get Migration Detail of Migration Job " +MigrationJobId+" Succeed!") ;
        List<StructureInitializationDetail> struInitDetails= response.getStructureInitializationDetailList();
        System.out.println("Structure Initialization Detail:");
        for (int i = 0; i < struInitDetails.size(); i++) {
            String objectName=struInitDetails.get(i).getObjectName();
            String SrcDBName=struInitDetails.get(i).getSourceOwnerDBName();
            String DestDBName = struInitDetails.get(i).getDestinationOwnerDBName();
            String Status=struInitDetails.get(i).getStatus();
            String errorMsg=struInitDetails.get(i).getErrorMessage();
            System.out.println("ObjectName:"+objectName+"; SRCDBName:"+SrcDBName+"; DESTDBName:"
                    +DestDBName+"; Status:"+Status+"errorMsg:"+errorMsg);
        }
        List<DataInitializationDetail> dataInitDetails = response.getDataInitializationDetailList();
        System.out.println("Data Initialization Detail:");
        for (int i = 0; i < dataInitDetails.size(); i++) {
            String tblName=dataInitDetails.get(i).getTableName();
            String tbl_srcDBName=dataInitDetails.get(i).getSourceOwnerDBName();
            String tbl_destDBName=dataInitDetails.get(i).getDestinationOwnerDBName();
            String dataInitStatus=dataInitDetails.get(i).getStatus();
            String dataInitSumRows=dataInitDetails.get(i).getTotalRowNum();
            String dataInitFinishRows=dataInitDetails.get(i).getFinishRowNum();
            String dataUsedTime=dataInitDetails.get(i).getMigrationTime();
            String dataInitErrMSG = dataInitDetails.get(i).getErrorMessage();
            System.out.println("TableName:"+tblName+"; SRCDBName:"+tbl_srcDBName
                    +"; DESTDBName:"+tbl_destDBName+"; SumRows:"+dataInitSumRows+"; FinishRows"
                    +"; UsedTime:"+dataUsedTime+"; ErrorMSG:"+dataInitErrMSG);
        }
        List<DataSynchronizationDetail> dataSyncDetails = response.getDataSynchronizationDetailList()
;
        System.out.println("Data Synchronization Detail");
        for (int i = 0; i < dataSyncDetails.size(); i++) {
            String dataSyncTblName=dataSyncDetails.get(i).getTableName();
            String dataSyncSRCDBName=dataSyncDetails.get(i).getSourceOwnerDBName();
            String dataSyncDESTDBName = dataSyncDetails.get(i).getDestinationOwnerDBName();
            String dataSyncStatus = dataSyncDetails.get(i).getStatus();
            String dataSyncErrMsg = dataSyncDetails.get(i).getErrorMessage();
            System.out.println("TableName:"+dataSyncTblName+"; SRCDBName:"+dataSyncSRCDBName
                    +"; DESTDBName:"+dataSyncDESTDBName+"; Status:"+dataSyncStatus+"; ErrorMSG:"+dat
aSyncErrMsg);
        }
```

```
    } catch (Exception e) {
        // TODO: handle exception
        System.out.println("Get Migration Detail of Migration Job " +MigrationJobId+" Failed!") ;
        System.out.println(e.toString());
    }
}
```

2.12.1.2.5. DescribeMigrationJobStatus

2.12.1.2.5.1. Overview

You can call this operation to query the data migration status regardless of the migration task status. You can query the overall migration status of the task, the migration status of each migration stage (schema migration, full data migration, and incremental data migration), and the precheck status.

2.12.1.2.5.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeMigrationJobStatus.
MigrationJobId	String	Yes	The migration task ID.

2.12.1.2.5.3. Response parameters

Name	Type	Description
MigrationJobId	String	The ID of the migration task.
MigrationJobName	String	The name of the migration task.
PayType	String	The billing method.
MigrationJobClass	String	The type of the migration instance.
SourceEndpoint	Endpoint	The IP address for connecting to the source instance. For more information, see the parameter definition in section 1.2.5.4.

Name	Type	Description
DestinationEndpoint	Endpoint	The IP address for connecting to the destination instance. For more information, see the parameter definition in section 1.2.5.4.
MigrationMode	MigrationMode	The migration type. For more information, see the parameter definition in section 1.2.5.5.
MigrationObjects	List	The objects to be migrated.
MigrationJobStatus	String	The status of the migration task. Valid values: • NotStarted: The migration task is not started. • Prechecking: The migration task is being prechecked. • PrecheckFailed: The precheck fails. • Migrating: Data is being migrated. • Suspending: The migration task is suspended. • MigrationFailed: The migration task fails. • Finished: The migration task is complete.
PrecheckStatus	PrecheckStatus	The precheck status including the check progress and the specific state. For more information, see the parameter definition in section 1.2.5.6.
StructureInitializationStatus	StructureInitializationStatus	The status of schema migration including the migration progress and the specific state. For more information, see the parameter definition in section 1.2.5.8.
DataInitializationStatus	DataInitializationStatus	The status of full data migration including the migration progress and the specific state. For more information, see the parameter definition in section 1.2.5.9.

Name	Type	Description
DataSynchronizationStatus	DataSynchronizationStatus	The status of incremental data migration including the migration progress and the specific state. For more information, see the parameter definition in section 1.2.5.10.

2.12.1.2.5.4. Endpoint parameter definitions

Name	Type	Description
InstanceType	String	The instance type.
Region	String	The region of the source instance.
InstanceId	String	The instance ID.
EngineName	String	The database type.
IP	String	The database connection address.
Port	String	The listening port of the database.
UserName	String	The username to access the database.
OracleSID	String	The Oracle SID.
DatabaseName	String	The database name.

2.12.1.2.5.5. MigrationMode parameter definitions

Name	Type	Description
StructureInitialization	String	Indicates whether to perform schema migration.
DataInitialization	String	Indicates whether to perform full data migration.
DataSynchronization	String	Indicates whether to perform incremental data migration.

2.12.1.2.5.6. PrecheckStatus parameter definitions

Name	Type	Description
Status	String	The precheck status.
Percent	String	The precheck progress. Unit: %.
Detail	List	The check details of each precheck item. For more information, see CheckItem parameter definitions.

2.12.1.2.5.7. CheckItem parameter definitions

Name	Type	Description
ItemName	String	The check item name.
CheckStatus	String	The check status. Valid values: • NotStarted • Checking • Failed • Finished
ErrorMessage	String	The cause of the error.
RepairMethod	String	The repair method.

2.12.1.2.5.8. StructureInitializationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Progress	String	The number of tables that have been migrated.

2.12.1.2.5.9. DataInitializationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Progress	String	The number of tables that have been migrated.

2.12.1.2.5.10. DataSynchronizationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Delay	String	The migration latency.

2.12.1.2.5.11. Examples

The following code provides an example of how to use the Java SDK to query the status of a migration task.

```
private static void describeMigrationJobStatus(String MigrationJobId){
    DescribeMigrationJobStatusRequest request = new DescribeMigrationJobStatusRequest();
    request.setMigrationJobId(MigrationJobId);
    try {
```

```
        DescribeMigrationJobStatusResponse response = client.getAcsResponse(request);
        System.out.println("Get Status of Migration Job "+MigrationJobId+" Succeed!") ;
        String JobStatus=response.getMigrationJobStatus();
        /*Get the basic information of the migration job*/
        System.out.println("MigrationJobName:"+response.getMigrationJobName()
            +"MigrationJobId:"+response.getMigrationJobId()
            +"MigrationObjects:"+response.getMigrationObject()
            +"; MigrationMode.StructureInitialization:" + response.getMigrationMode().getStructureInitia
lization()
            +"; MigrationMode.DataInitialization:"+response.getMigrationMode().getDataInitialization()
            +"; MigrationMode.DataSynchronization:"+response.getMigrationMode().getDataSynchroniz
ation()
            +"; MigrationJobStatus:"+response.getMigrationJobStatus());
        /*Get the source endpoint of the migration job*/
        System.out.println("SourceEndpoint.InstanceType:"+response.getSourceEndpoint().getInstanceT
ype()
            +"; SourceEndpoint.InstanceId:"+response.getSourceEndpoint().getInstanceId()
            +"; SourceEndpoint.EngineName:"+response.getSourceEndpoint().getEngineName()
            +"; SourceEndpoint.IP:"+response.getSourceEndpoint().getIP()
            +"; SourceEndpoint.Port"+response.getSourceEndpoint().getPort()
            +"; SourceEndpoint.UserName:"+response.getSourceEndpoint().getUserName()
            +"; SourceEndpoint.DatabaseName:"+response.getSourceEndpoint().getDatabaseName()
            +"; SourceEndpoint.OracleSID:"+response.getSourceEndpoint().getOracleSID());
        /*Get the destination endpoint of the migration job*/
        System.out.println("DestinationEnpoint.InstanceType:"+response.getDestinationEndpoint().getIn
stanceType()
            +"DestinationEndpoint.InstanceId:"+response.getDestinationEndpoint().getInstanceId()
            +"DestinationEndpint.EngineName:"+response.getDestinationEndpoint().getEngineName()
            +"DestinationEndpoint.IP:"+response.getDestinationEndpoint().getIP()
            +"DestinationEndpoint:Port:"+response.getDestinationEndpoint().getPort()
            +"DestinationEndpoint.UserName:"+response.getDestinationEndpoint().getUserName()
            +"DestinationEndpoint.DatabaseName"+response.getDestinationEndpoint().getDatabaseNa
me()
            +"DestinationEndpoint.OracleSID:"+response.getDestinationEndpoint().getOracleSID());
        /*Get Status of Precheck*/
        try {
          com.aliyuncs.dts.model.v20160801. DescribeMigrationJobStatusResponse.PrecheckStatus prech
eckStatus = response.getPrecheckStatus();
          System.out.println("Get  Precheck Status of Migration Job "+MigrationJobId +" Succeed!") ;
          System.out.println("Precheck Status:"+ precheckStatus.getStatus()+";Precheck Percent:"+prec
heckStatus.getPercent());
```

```
            List<CheckItem> checkItems = precheckStatus.getDetail();
            for (int i = 0; i < checkItems.size(); i++) {
               String checkItem=checkItems.get(i).getItemName();
               String checkStatus = checkItems.get(i).getCheckStatus();
               String repairMethod = checkItems.get(i).getRepairMethod();
               String errorMessage =checkItems.get(i).getErrorMessage();
               System.out.println("CheckItem:"+checkItem+"; CheckStatus:"+checkStatus
                     +"errorMessage:"+errorMessage+"; repairMethod:"+repairMethod);
            }
         } catch (Exception e) {
            // TODO: handle exception
            System.out.println("Get  Precheck Status of Migration Job "+MigrationJobId +" Failed!") ;
            System.out.println(e.toString());
         }
         /*Get Status of Structure Migration*/
         try {
            StructureInitializationStatus strucInitStatus = new StructureInitializationStatus();
            strucInitStatus = response.getStructureInitializationStatus();
            String status = strucInitStatus.getStatus();
            String percent = strucInitStatus.getPercent();
            String progress = strucInitStatus.getProgress();
            String errorMsg = strucInitStatus.getErrorMessage();
            System.out.println("Get Structure Initialization Status of Migration Job " +MigrationJobId+" Succ
eed!") ;
            System.out.println("Status:"+status+";percent:"+percent+"; progress:"+progress+"; errorMsg:
"+errorMsg);
         } catch (Exception e) {
            // TODO: handle exception
            System.out.println("Get Structure Initialization Status of Migration Job " +MigrationJobId+" Faile
d!") ;
            System.out.println(e.toString());
         }
         /*Get Status of Data Migration*/
         try {
            DataInitializationStatus dataInitStatus = new DataInitializationStatus();
            dataInitStatus = response.getDataInitializationStatus();
            String datainitstatus=dataInitStatus.getStatus();
            String datainitpercent = dataInitStatus.getPercent();
            String datainitprogress = dataInitStatus.getProgress();
            String datainiterrormsg = dataInitStatus.getErrorMessage();
            System.out.println("Get Data Initialization Status of Migration Job " +MigrationJobId+" Succeed!"
```

```
) ;
            System.out.println("Status:"+datainitstatus+";percent:"+datainitpercent+"; progress:"+datainitprogress+"; errorMsg:"+datainiterrormsg);
          } catch (Exception e) {
            // TODO: handle exception
             System.out.println("Get Data Initialization Status of Migration Job " +MigrationJobId+" Failed!") ;
             System.out.println(e.toString());
          }
          /*Get Status of Data Synchronization*/
          try {
            DataSynchronizationStatus dataSyncStatus = new DataSynchronizationStatus();
            dataSyncStatus = response.getDataSynchronizationStatus();
            String datasynstatus=dataSyncStatus.getStatus();
            String datasyncpercent=dataSyncStatus.getPercent();
            String datasyncdelay=dataSyncStatus.getDelay();
            String datasyncerrormsg=dataSyncStatus.getErrorMessage();
            System.out.println("Get Data Synchronization Status of Migration Job " +MigrationJobId+" Succeed!") ;
            System.out.println("Status:"+datasynstatus+";percent:"+datasyncpercent+"; delay:"+datasyncdelay+"; errorMsg:"+datasyncerrormsg);
          } catch (Exception e) {
            // TODO: handle exception
            System.out.println("Get Data Synchronization Status of Migration Job " +MigrationJobId+" Failed!") ;
            System.out.println(e.toString());
          }
      } catch (Exception e) {
          // TODO: handle exception
          System.out.println("Get Status of Migration Job "+MigrationJobId+" Failed");
          System.out.println(e.toString());
      }
   }
```

2.12.1.2.6. StartMigrationJob

2.12.1.2.6.1. Overview

You can call this operation to start a migration task. When a migration task is in the NotStarted or MigrationFailed status, you can call this operation to start or restart it.

2.12.1.2.6.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to StartMigrationJob.
MigrationJobId	String	Yes	The migration task ID.

2.12.1.2.6.3. Response parameters

Name	Type	Description
<Common response parameters>	-	The request ID.

2.12.1.2.6.4. Examples

The following code provides an example of how to use the Java SDK to start a migration task.

```
private static void startMigrationJob(String MigrationJobId){
    StartMigrationJobRequest request = new StartMigrationJobRequest();
    request.setMigrationJobId(MigrationJobId);
    try {
       StartMigrationJobResponse response = client.getAcsResponse(request);
       System.out.println("Start "+MigrationJobId+" Succeed");
    } catch (Exception e) {
       // TODO: handle exception
       System.out.println("Start "+MigrationJobId + " Failed");
       System.out.println(e.toString());
    }
  }
```

2.12.1.2.7. StopMigrationJob

2.12.1.2.7.1. Overview

You can call this operation to stop a migration task when it is in the **Migrating** status.

> **Note** You cannot start a task that has been stopped.

2.12.1.2.7.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to StopMigrationJob.
MigrationJobId	String	Yes	The migration task ID.

2.12.1.2.7.3. Response parameters

Name	Type	Description
<Common response parameters>	-	The request ID.

2.12.1.2.7.4. Examples

The following code provides an example of how to use the Java SDK to stop a migration task.

```
private static void stopMigrationJob(String MigrationJobId) {
      StopMigrationJobRequest request = new StopMigrationJobRequest();
      try {
         request.setMigrationJobId(MigrationJobId);
         StopMigrationJobResponse response = client.getAcsResponse(request);
         System.out.println("Stop Migration Job "+MigrationJobId+" Succeed!") ;
      } catch (Exception e) {
         // TODO: handle exception
         System.out.println("Stop Migration Job "+MigrationJobId+" Failed!") ;
         System.out.println(e.toString());
      }
   }
```

2.12.1.2.8. SuspendMigrationJob

2.12.1.2.8.1. Overview

You can call this operation to suspend a migration task when it is in the Migrating status. Note that if a task has been suspended for more than 6 hours after it enters the incremental data migration stage, you may fail to restart it through the StartMigrationJob operation.

2.12.1.2.8.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to SuspendMigrationJob.
MigrationJobId	String	Yes	The migration task ID.

2.12.1.2.8.3. Response parameters

Name	Type	Description
<Common response parameters>	-	The request ID.

2.12.1.2.8.4. Examples

The following code provides an example of how to use the Java SDK to suspend a migration task.

```
private static void suspendMigrationJob(String MigrationJobId){
      SuspendMigrationJobRequest request = new SuspendMigrationJobRequest();
      request.setMigrationJobId(MigrationJobId);
      try {
         SuspendMigrationJobResponse response = client.getAcsResponse(request);
         System.out.println("Suspend "+ MigrationJobId + " Succeed");
      } catch (Exception e) {
         // TODO: handle exception
         System.out.println("Suspend "+MigrationJobId +"Failed");
         System.out.println(e.toString());
      }
   }
```

2.12.1.3. Data subscription APIs

2.12.1.3.1. ConfigureSubscriptionInstance

2.12.1.3.1.1. Overview

You can call this operation to modify the configurations of a change tracking task, such as instance connection details and objects for change tracking. You can call this operation multiple times to modify the configurations of a task before the task is started. Only the changes of RDS for MySQL instances can be tracked.

2.12.1.3.1.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ConfigureSubscriptionInstance.
SubscriptionInstanceId	String	Yes	The ID of the subscription channel to be configured.
SubscriptionInstanceName	String	No	The name of a subscription channel that can distinguish it from other subscription channels.
SourceEndpoint.InstanceType	String	No	The type of the subscription instance. Valid value: RDS. Default value: RDS.
SourceEndpoint.InstanceId	String	Yes	The RDS instance ID.
SubscriptionDataType.DDL	Boolean	Yes	Indicates whether to subscribe to schema updates made through DDL. Valid values: true (yes) and false (no). Default value: true.
SubscriptionDataType.DML	Boolean	Yes	Indicates whether to subscribe to data updates made through DML. Valid values: true (yes) and false (no). Default value: true.
SubscriptionObjects	List	Yes	The listening port of the source instance. This parameter is required when the source instance is a user-created database. For more information, see SubscriptionObject parameter definitions.

2.12.1.3.1.3. SubscriptionObject parameter definitions

The SubscriptionObject parameters are defined as JSON strings. Certain regular expressions can be used in the object configuration.

The SubscriptionObject parameter definitions are as follows:

```
SubscriptionObject:{
    DBName:"The name of the database to be subscribed",
    TableIncludes:[{
        TableName: "The name of the table to be migrated"
    }]
}
```

SubscriptionObject indicates the whitelist of objects to be subscribed.

You can use the following regular expressions to define different object names:

- A period (.) matches any single character except '\r\n'.
- An asterisk (*) matches zero or more occurrences of a subexpression which occurs before. h.*llo matches strings such as hllo and heeeello.
- A question mark (?) matches zero or one occurrence of a subexpression which occurs before. h.?llo matches hllo and hello, but not haello.
- The [characters] character set matches any character included in the braces. For example, h[aello] matches hallo and hello.
- The [^characters] negative character set does not match any character included in the braces. For example, h[^ae]llo matches hcllo and hdllo, but not hallo or hello.
- The [character1-character2] character range matches any character included in the range from character1 to character2, such as [0-9] and [a-z].

2.12.1.3.1.4. Response parameters

Name	Type	Description
RequestId	String	The GUID of the request.
Success	String	Indicates whether the request is successful. Valid values: true and false.
ErrCode	String	The error code.
ErrMessage	String	The detailed error message.

2.12.1.3.1.5. Example

This topic describes how to use the Java SDK to configure a migration task.

```
private static void configureSbeJob(String MigrationJobId){
    String MigrationJobName="jiangliutest";
    /*Source Endpoint*/
    String SourceEndpoint_InstanceId="rm-xxxxxxxxxxxxxxxxx";
    String SourceEndpoint_InstanceType="rds";
    Boolean MigrationMode_SubscriptionDataTypeDML=true;
    Boolean MigrationMode_SubscriptionDataTypeDDL=true;
    String MigrationObjects="[{\"DBName\":\"jiangliutest\","
        + "\"TableIncludes\":[{\"TableName\":\"t1\"}]}]";
    ConfigureSubscriptionInstanceRequest request = new ConfigureSubscriptionInstanceRequest();
    request.setMigrationJobId(MigrationJobId);
    request.setMigrationJobName(MigrationJobName);
    request.setSubscriptionInstanceId(jobId);
    request.setSubscriptionDataTypeDDL(MigrationMode_SubscriptionDataTypeDDL);
    request.setSubscriptionDataTypeDML(MigrationMode_SubscriptionDataTypeDML);
    request.setSourceEndpointInstanceType(SourceEndpoint_InstanceType);
    request.setSourceEndpointInstanceID(SourceEndpoint_InstanceId);
    request.setMigrationObject(MigrationObjects);
    try {
       ConfigureSubscriptionInstanceResponse response = client.getAcsResponse(request);
       System.out.println("Configure "+ MigrationJobId+ " Succeed");
    } catch (Exception e) {
       // TODO: handle exception
       System.out.println("Configure "+MigrationJobId + " Failed!") ;
       System.out.println(e.toString());
    }
  }
```

2.12.1.3.2. CreateSubscriptionInstance

2.12.1.3.2.1. Overview

You can call this operation to purchase a database incremental subscription instance. After the purchase, you need to call the ConfigureSubscriptionInstance operation to configure a subscription task.

2.12.1.3.2.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateSubscriptionInstance.

Name	Type	Required	Description
Region	String	Yes	The region of the subscription instance. Valid values: • cn-hangzhou: Alibaba Cloud in Hangzhou • cn-shanghai: Alibaba Cloud in Shanghai • cn-qingdao: Alibaba Cloud in Qingdao • cn-beijing: Alibaba Cloud in Beijing • cn-zhangbei: Alibaba Cloud in Zhangbei • cn-shenzhen: Alibaba Cloud in Shenzhen • cn-hongkong: Alibaba Cloud in Hong Kong • us-west-1: Alibaba Cloud in Western US • us-east-1: Alibaba Cloud in Eastern US • ap-southeast-1: Alibaba Cloud in Singapore • cn-hangzhou-finance-1: Finance Cloud in Hangzhou • cn-qingdao-finance-1: Finance Cloud in Qingdao • cn-shanghai-finance-1: Finance Cloud in Shanghai • cn-shenzhen-finance-1: Finance Cloud in Shenzhen • me-east-1: Alibaba Cloud in Dubai • en-central-1: Alibaba Cloud in Frankfurt
ClientToken	String	No	The token used to ensure the idempotence of the request. It can be any string.
OwnerID	String	No	If a RAM user is used to call this operation, the value of OwnerID is the UID of the Apsara Stack tenant account to which this RAM user belongs.

2.12.1.3.2.3. Response parameters

Name	Type	Description
SubscriptionInstanceId	String	The subscription channel ID. This is the GUID of a subscription channel.

2.12.1.3.2.4. Examples

The following code provides an example of how to use the Java SDK to purchase a migration instance.

```
private String create() throws Exception {
      CreateSubscriptionInstanceRequest request = new CreateSubscriptionInstanceRequest();
      request.setRegion("cn-hangzhou");
      request.setPayType("postpaid");
      CreateSubscriptionInstanceResponse response = client.getAcsResponse(request);
      if(response == null){
         throw new Exception("create fail");
      }
      System.out.println("CreateSubscriptionInstanceRequest, result :"+response.getSubscriptionInstanc
eId());
      return response.getSubscriptionInstanceId();
   }
```

2.12.1.3.3. DeleteSubscriptionInstance

2.12.1.3.3.1. Overview

You can call this operation to delete a subscription channel regardless of its status. After a subscription task is deleted, you cannot query or manage it through OpenAPI or the console.

2.12.1.3.3.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteSubscriptionInstance.
SubscriptionInstanceId	String	Yes	The ID of the subscription channel to be released.

2.12.1.3.3.3. Response parameters

Name	Type	Description
RequestId	String	The GUID of the request.
Success	String	Indicates whether the request is successful. Valid values: true and false.
ErrCode	String	The error code.

Name	Type	Description
ErrMessage	String	The detailed error message.

2.12.1.3.3.4. Examples

The following code provides an example of how to use the Java SDK to delete a subscription task.

```
private static void deleteMigrationJob(String MigrationJobId) {
      DeleteMigrationJobRequest request = new DeleteMigrationJobRequest();
      DeleteMigrationJobResponse response = new DeleteMigrationJobResponse();
      request.setMigrationJobId(MigrationJobId);
      try {
         response = client.getAcsResponse(request);
         System.out.println("Delete Migration Job "+MigrationJobId+" Succeed!") ;
      } catch (Exception e) {
         // TODO: handle exception
         System.out.println("Delete Migration Job "+MigrationJobId+" Failed!") ;
         System.out.println(e.toString());
      }
   }
```

2.12.1.3.4. DescribeSubscriptionInstances

2.12.1.3.4.1. Overview

You can call this operation to query the list of subscription channels that your Apsara Stack tenant account has access to. Data subscription channels in any status are returned.

2.12.1.3.4.2. Request parameters

Description	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSubscriptionInstances.
PageSize	Integer	No	The number of records on each page. Valid values: 30, 50, and 100. Default value: 30.

Description	Type	Required	Description
PageNum	Integer	No	The page number. It must be greater than 0 and smaller than or equal to the maximum value of Integer. Default value: 1.

2.12.1.3.4.3. Response parameters

Name	Type	Description
SubscriptionInstances	List	The subscription channel details. For more information, see DescribeSubscriptionInstanceStatus.
PageNumber	Integer	The page number.
TotalRecrodCount	Integer	The total number of records.
PageRecordCount	Integer	The number of records on the page.

2.12.1.3.4.4. Examples

The following code provides an example of how to use the Java SDK to query the list of subscription instances.

```
public List<SubscriptionInstance> list(String jobName) throws ClientException {
    DescribeSubscriptionInstancesRequest request = new DescribeSubscriptionInstancesRequest();
    request.setPageNum(1);
    request.setPageSize(20);
    if(jobName! =null) {
       request.setSubscriptionInstanceName(jobName);
    }
    DescribeSubscriptionInstancesResponse response = client.getAcsResponse(request);
    System.out.println("page no: "+response.getPageNumber());
    System.out.println("page size: "+response.getPageRecordCount());
    System.out.println("size: "+ response.getSubscriptionInstances().size());
    return response.getSubscriptionInstances();
  }
```

2.12.1.3.5. DescribeSubscriptionInstanceStatus

2.12.1.3.5.1. Overview

You can call this operation to query the status of a subscription channel regardless of the subscription task status. You can query the channel configuration information, channel status, and downstream consumption status.

2.12.1.3.5.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSubscriptionInstanceStatus.
SubscriptionInstanceId	String	Yes	The subscription channel ID.

2.12.1.3.5.3. Response parameters

Name	Type	Description
SubscriptionInstanceId	String	The subscription channel ID.
SubscriptionInstanceName	String	The subscription channel name.
PayType	String	The billing method.
SourceEndpoint	Endpoint	The endpoint to access the source instance specified in the subscription task. For more information, see Endpoint parameter definitions.
SubscriptionDataType.DDL	Boolean	Indicates whether the data to be subscribed contains schema updates made through DDL. Valid values: true (yes) and false (no).
SubscriptionDataType.DML	Boolean	Indicates whether the data to be subscribed contains data updates made through DML. Valid values: true (yes) and false (no).
SubscriptionObjects	List	The objects to be subscribed, listed in a SubscriptionObject array. For more information, see SubscriptionObject parameter definitions.
Status	String	The subscription channel status. Valid values: NotStarted, Prechecking, PrecheckFailed, Starting, Normal, and Abnormal.
ErrorMessage	String	The cause of the channel error.

Name	Type	Description
ConsumptionCheckpoint	String	The consumption checkpoint of the downstream SDK connected to the subscription channel. The date format follows the ISO8601 standard. It is in the UTC format of YYYY-MM-DDThh:mm:ssZ. For example, 2017-08-15T12:00:00Z (or 20:00:00, August 15, 2017, China Standard Time).
BeginTimestamp	String	The start time of the timestamp range of the data stored in the subscription channel. The date format follows the ISO8601 standard. It is in the UTC format of YYYY-MM-DDThh:mm:ssZ. For example, 2017-08-15T12:00:00Z (or 20:00:00, August 15, 2017, China Standard Time).
EndTimestamp	String	The end time of the timestamp range of the data stored in the subscription channel. The date format follows the ISO8601 standard. It is in the UTC format of YYYY-MM-DDThh:mm:ssZ. For example, 2017-08-15T12:00:00Z (or 20:00:00, August 15, 2017, China Standard Time).
ConsumptionClient	String	The downstream client information, in the following format: IP address of the downstream client:Random ID generated by DTS.

2.12.1.3.5.4. Endpoint parameter definitions

Name	Type	Description
InstanceType	String	The instance type.
Region	String	The region of the source instance.
InstanceId	String	The instance ID.
EngineName	String	The database type.
IP	String	The connection address of the database.
Port	String	The listening port of the database.
UserName	String	The username to access the database.
OracleSID	String	The Oracle SID.

Name	Type	Description
DatabaseName	String	The database name.

2.12.1.3.5.5. SubscriptionObject parameter definitions

Name	Type	Description
databaseName	String	The name of the database from which the list of objects are to be subscribed.
tableList	List	The names of the tables to be subscribed.
wholeDatabase	Boolean	Indicates whether to subscribe to the whole database.

2.12.1.3.5.6. Examples

The following code provides an example of how to use the Java SDK to query the status of a subscription channel.

```
 private void describe(String jobId) throws ClientException {
      DescribeSubscriptionInstanceStatusRequest request = new DescribeSubscriptionInstanceStatusReq
uest();
      request.setSubscriptionInstanceId(jobId);
      DescribeSubscriptionInstanceStatusResponse response = client.getAcsResponse(
         request);
      System.out.println(response.getStatus());
      System.out.println(response.getBeginTimestamp());
      System.out.println(response.getEndTimestamp());
      System.out.println(response.getConsumptionCheckpoint());
   }
```

2.12.1.3.6. ModifyComsumptionTimestamp

2.12.1.3.6.1. Overview

You can call this operation to modify the consumption checkpoint only when the subscription channel is in the Normal status and the consumption client is stopped.

2.12.1.3.6.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifyComsumptionTimestamp.
SubscriptionInstanceId	String	Yes	The ID of the subscription channel for which the consumption checkpoint needs to be modified.
ConsumptionTimestamp	String	Yes	The timestamp of the modified consumption checkpoint. The timestamp format follows the ISO8601 standard. The UTC time is used. Format: yyyy-MM-ddTHH:mm:ssZ. For example, 2013-08-15T12:00:00Z indicates 20:00:00 on Tuesday, August 15, 2013 Beijing Time).

2.12.1.3.6.3. Response parameters

Name	Type	Description
RequestId	String	The GUID of the request.
Success	String	Indicates whether the request is successful. Valid values: true and false.
ErrCode	String	The error code.
ErrMessage	String	The detailed error message.

2.12.1.3.6.4. Examples

The following code provides an example of how to use the Java SDK to modify the consumption checkpoint.

```
private void modifyTimestamp(String jobId,String ts) throws ClientException {
    ModifyConsumptionTimestampRequest request = new ModifyConsumptionTimestampRequest();
    request.setSubscriptionInstanceId(jobId);
    //ts
    request.setConsumptionTimestamp(ts);
    ModifyConsumptionTimestampResponse response = client.getAcsResponse(request);
    System.out.println("modify timestamp ,result:" + response.getSuccess());
    }
```

2.12.1.3.7. ModifySubscriptionObject

2.12.1.3.7.1. Overview

When the subscription channel is in the NotStarted, Failed, Normal or Abnormal status, you can call this operation to modify the list of objects to be subscribed.

- If the subscription channel is in the Normal status, you call this operation to modify the list of objects to be subscribed. After that, DTS calls the StartSubscriptionInstance operation directly to start the subscription channel.
- If the subscription channel is in the NotStarted, Failed, or Abnormal status, you call this operation to modify the list of objects to be subscribed. After that, you need to call the StartSubscriptionInstance operation to start the subscription channel if you want to.

2.12.1.3.7.2. Request parameters

Description	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifySubscriptionObject.
SubscriptionInstanceId	String	Yes	The ID of the subscription channel for the list of objects to be modified.
SubscriptionObjects	List	Yes	The new list of objects to be subscribed after the modification. For more information, see SubscriptionObject parameter definitions.

2.12.1.3.7.3. SubscriptionObject parameter definitions

The SubscriptionObject parameters are defined as JSON strings. Certain regular expressions can be used in the object configuration.

The SubscriptionObject parameter definitions are as follows:

```
SubscriptionObject:{
    DBName:"The name of the database to be subscribed",
    TableIncludes:[{
        TableName: "The name of the table to be migrated"
    }]
}
```

SubscriptionObject indicates the whitelist of objects to be subscribed.

You can use the following regular expressions to define different object names:

- A period (.) matches any single character except '\r\n'.
- An asterisk (*) matches zero or more occurrences of a subexpression which occurs before. h.*llo matches strings such as hllo and heeeello.
- A question mark (?) matches zero or one occurrence of a subexpression which occurs before. h.?llo matches hllo and hello, but not haello.
- The [characters] character set matches any character included in the braces. For example, h[aello] matches hallo and hello.
- The [^characters] negative character set does not match any character included in the braces. For example, h[^ae]llo matches hcllo and hdllo, but not hallo or hello.
- The [character1-character2] character range matches any character included in the range from character1 to character2, such as [0-9] and [a-z].

2.12.1.3.7.4. Response parameters

Name	Type	Description
RequestId	String	The GUID of the request.
Success	String	Indicates whether the request is successful. Valid values: true and false.
ErrCode	String	The error code.
ErrMessage	String	The detailed error message.

2.12.1.3.7.5. Examples

The following code provides an example of how to use the Java SDK to modify the list of objects to be subscribed.

```
private void modifyObject(String jobId) throws ClientException {
    ModifySubscriptionObjectRequest request = new ModifySubscriptionObjectRequest();
    request.setSubscriptionInstanceId(jobId);
    String sbeObject = "[{\n"
                + "\"DBName\":\"miyuntest\","
                + "\"TableIncludes\":["
                + "{\"TableName\":\"t1\"},"
                + "{\"TableName\":\"t2\"},"
                + "{\"TableName\":\"t3\"}"
                + "]"
                + "}]";
    request.setSubscriptionObject(sbeObject);
    ModifySubscriptionObjectResponse response = client.getAcsResponse(request);
    System.out.println(response.getSuccess());
  }
```

2.12.1.3.8. StartSubscriptionInstance

2.12.1.3.8.1. Overview

You can call this operation to start a subscription channel only when the channel is in the NotStarted, Failed, or Suspending status.

2.12.1.3.8.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to StartSubscriptionInstance.
SubscriptionInstanceId	String	Yes	The ID of the subscription channel to be started.

2.12.1.3.8.3. Response parameters

Name	Type	Description
RequestId	String	The GUID of the request.
Success	String	Indicates whether the request is successful. Valid values: true and false.
ErrCode	String	The error code.
ErrMessage	String	The detailed error message.

2.12.1.3.8.4. Examples

The following code provides an example of how to use the Java SDK to start a subscription task.

```
private static void startSbeJob(String MigrationJobId){
    StartSubscriptionInstanceRequest request = new StartSubscriptionInstanceRequest();
    request.setSubscriptionInstanceId(jobId);
    try {
       StartSubscriptionInstanceResponse response = client.getAcsResponse(request);
       System.out.println("Start "+MigrationJobId+" Succeed");
    } catch (Exception e) {
       // TODO: handle exception
       System.out.println("Start "+MigrationJobId + " Failed");
       System.out.println(e.toString());
    }
  }
```

2.12.1.4. Data synchronization APIs

2.12.1.4.1. ConfigureSynchronizationJob

2.12.1.4.1.1. Overview

After you call the CreateSynchronizationJob operation to purchase a synchronization instance, you can call this operation to configure a synchronization task, provided that the synchronization task is not configured.

2.12.1.4.1.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ConfigureSynchronizationJob.
SynchronizationJobId	String	Yes	The ID of the synchronization job.
SynchronizationJobName	String	No	The name of the synchronization task.
SourceEndpoint.InstanceId	String	Yes	The ID of the source synchronization instance.
SynchronizationDirection	String	No	The synchronization direction. This parameter is used only when two-way synchronization is configured for the instance. Valid values: Forward and Reverse. Default value: Forward.

Name	Type	Required	Description
SourceEndpoint.OwnerID	String	No	The GUID generated by Alibaba Cloud for the request. This parameter is used when source and destination instances do not belong to the same Alibaba Cloud account.
SourceEndpoint.Role	String	No	The role that the source instance grants to the destination instance. This parameter is used when the source and destination instances do not belong to the same Alibaba Cloud account. For more information about role permissions and how to grant a role, see Migrate or synchronize an instance across accounts.
DestinationEndpoint.InstanceId	String	Yes	The ID of the destination instance. If the destination instance is a MaxCompute or DataHub instance, the parameter indicates the corresponding project.
SynchronizationObjects	List	Yes	The objects to be synchronized.
StructureInitialization	Boolean	No	Whether initial schema synchronization is performed before the synchronization task starts. Valid values: • true: Initial schema synchronization is performed. • false: Initial schema synchronization is not performed. • Default value: true.
DataInitialization	Boolean	No	Whether initial full data synchronization is performed before the synchronization task starts. Valid values: • true: Initial full data synchronization is performed. • false: Initial full data synchronization is not performed. • Default value: true.
PartitionKey.ModifyTime_Year	Boolean	No	The definition of the partitioned key in the incremental log table when the destination instance is a MaxCompute instance. Valid values: • true: The primary partition of the incremental log table is a yearly partition. • false: The incremental log table does not support yearly partitions. • Default value: true.
PartitionKey.ModifyTime_Month	Boolean	No	The definition of the partitioned key in the incremental data table when the destination instance is a MaxCompute instance. Valid values: • true: The incremental data table supports monthly partitions. • false: The incremental data table does not support monthly partitions. • Default value: true.

Name	Type	Required	Description
PartitionKey.ModifyTime_Day	Boolean	No	The definition of the partitioned key in the incremental data table when the destination instance is a MaxCompute instance. Valid values: • true: The incremental data table supports daily partitions. • false: The incremental data table does not support daily partitions. • Default value: true.
PartitionKey.ModifyTime_Hour	Boolean	No	The definition of the partitioned key in the incremental data table when the destination instance is a MaxCompute instance. Valid values: • true: The incremental data table supports hourly partitions. • false: The incremental data table does not support hourly partitions. • Default value: true.
PartitionKey.ModifyTime_Minute	Boolean	No	The definition of the partitioned key in the incremental data table when the destination instance is a MaxCompute instance. Valid values: • true: The incremental data table supports minute partitions. • false: The incremental data table does not support minute partitions. A minute partition is generated every 15 minutes.

2.12.1.4.1.3. Response parameters

Name	Type	Description
<Common response parameters>	-	The request ID.

2.12.1.4.1.4. Example

This topic describes how to use the Java SDK to configure a synchronization task.

```
public void configureSyncJobRDS2RDS(String SyncJobId,DefaultAcsClient client) {
        ConfigureSynchronizationJobRequest request = new ConfigureSynchronizationJobRequest();
        request.setSynchronizationJobId(SyncJobId);
        request.setSynchronizationJobName("jiangliu_test_rds2rds_sync");
        request.setSourceEndpointInstanceId("rm-axxxxxxxxxxxxxxxxx");
        request.setDestinationEndpointInstanceId("rm-bxxxxxxxxxxxxxxxxx");
        request.setStructureInitialization(true);
        request.setDataInitialization(true);
        String SyncObject="[{\"DBName\":\"jiangliutest\",\"NewDBName\":\"jiangliutest\","
              + "\"TableIncludes\":[{\"TableName\":\"t1\",\"NewTableName\":\"t1\"}]}]";
        request.setSynchronizationObjects(SyncObject);
        ConfigureSynchronizationJobResponse response = new ConfigureSynchronizationJobResponse();
        try {
           response = client.getAcsResponse(request);
           System.out.println("Configure Sync Job Succeed!") ;
        } catch (Exception e) {
           // TODO: handle exception
           System.out.println("Configure Sync Job Failed");
           System.out.println(e.toString());
        }
    }
```

2.12.1.4.2. CreateSynchronizationJob

2.12.1.4.2.1. Overview

You can call this operation to purchase a data synchronization instance. After the purchase, you need to call the ConfigureSynchronizationJob operation to configure the instance. If your synchronization instance adopts the Pay-As-You-Go billing method, you will be charged only when you have called the ConfigureSynchronizationJob operation and started the synchronization task.

2.12.1.4.2.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to CreateSynchronizationJob.

Name	Type	Required	Description
SourceRegion	String	Yes	The region of the source instance specified in the synchronization task. Valid values: • cn-hangzhou: Alibaba Cloud in Hangzhou • cn-shanghai: Alibaba Cloud in Shanghai • cn-qingdao: Alibaba Cloud in Qingdao • cn-beijing: Alibaba Cloud in Beijing • cn-zhangbei: Alibaba Cloud in Zhangbei • cn-shenzhen: Alibaba Cloud in Shenzhen • cn-hongkong: Alibaba Cloud in Hong Kong • us-west-1: Alibaba Cloud in Western US • us-east-1: Alibaba Cloud in Eastern US • ap-southeast-1: Alibaba Cloud in Singapore • cn-hangzhou-finance-1: Finance Cloud in Hangzhou • cn-qingdao-finance-1: Finance Cloud in Qingdao • cn-shanghai-finance-1: Finance Cloud in Shanghai • cn-shenzhen-finance-1: Finance Cloud in Shenzhen • me-east-1: Alibaba Cloud in Dubai • en-central-1: Alibaba Cloud in Frankfurt
SourceEndpoint.InstanceType	String	No	The type of the source instance specified in the synchronization task. Valid value: RDS. Default value: RDS.
DestinationEndpoint.InstanceType	String	No	The type of the destination instance specified in the synchronization task. Valid values: RDS, MaxCompute, and DataHub. Default value: RDS.

Name	Type	Required	Description
SourceRegion	String	Yes	The region of the destination instance specified in the synchronization task. Valid values: • cn-hangzhou: Alibaba Cloud in Hangzhou • cn-shanghai: Alibaba Cloud in Shanghai • cn-qingdao: Alibaba Cloud in Qingdao • cn-beijing: Alibaba Cloud in Beijing • cn-zhangbei: Alibaba Cloud in Zhangbei • cn-shenzhen: Alibaba Cloud in Shenzhen • cn-hongkong: Alibaba Cloud in Hong Kong • us-west-1: Alibaba Cloud in Western US • us-east-1: Alibaba Cloud in Eastern US • ap-southeast-1: Alibaba Cloud in Singapore • cn-hangzhou-finance-1: Finance Cloud in Hangzhou • cn-qingdao-finance-1: Finance Cloud in Qingdao • cn-shanghai-finance-1: Finance Cloud in Shanghai • cn-shenzhen-finance-1: Finance Cloud in Shenzhen • me-east-1: Alibaba Cloud in Dubai • en-central-1: Alibaba Cloud in Frankfurt
NetworkType	String	No	The type of the data transmission network used for cross-region synchronization. Valid values: Internet and Intranet. Default value: Internet.
SynchronizationJobClass	String	No	The synchronization task type. Valid values: micro, small, medium, and large. Default value: small.
PayType	String	Yes	The billing method. Valid values: Postpaid and Prepaid.
Period	String	No	Indicates whether to subscribe to the instance on a yearly or monthly basis. This parameter is required when PayType is set to Prepaid. Valid values: Year and Month.
UsedTime	String	No	The duration of the subscription, in months. This parameter is required when Period is set to Month. Set the value to an integer greater than 0.
ClientToken	String	No	The token used to ensure the idempotence of the request. It can be any string.

2.12.1.4.2.3. Response parameters

Name	Type	Description
SynchronizationJobId	String	The GUID of the synchronization task.

2.12.1.4.2.4. Examples

The following code provides an example of how to use the Java SDK to purchase a synchronization instance.

```
public class DataSyncTest {
    public String createSyncJob(DefaultAcsClient client) {
        CreateSynchronizationJobRequest request = new CreateSynchronizationJobRequest();
        request.setSourceRegion("cn-hangzhou");
        request.setDestRegion("cn-hangzhou");
        request.setSynchronizationJobClass("micro");
        request.setPayType("Postpaid");
        request.setClientToken("createsyncjob_1");
        CreateSynchronizationJobResponse response = new CreateSynchronizationJobResponse();
        try {
            response = client.getAcsResponse(request);
            String DataSyncId  = response.getSynchronizationJobId();
            System.out.println("Create Synchronization Job Succeed! Synchronization Job Id is "+DataSyncId);
            return DataSyncId;
        } catch (Exception e) {
            // TODO: handle exception
            System.out.println("Create Synchronization Job Failed!") ;
            return null;
        }
    }
```

2.12.1.4.3. DeleteSynchronizationJob

2.12.1.4.3.1. Overview

You can call this operation to delete a synchronization task regardless of the synchronization task status. After a synchronization task is released, you cannot query or manage it through OpenAPI or the console.

2.12.1.4.3.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DeleteSynchronizationJob.
SynchronizationJobId	String	Yes	The synchronization task ID.

2.12.1.4.3.3. Response parameters

Name	Type	Description
<Common response parameters>	-	The request ID.

2.12.1.4.3.4. Examples

The following code provides an example of how to use the Java SDK to delete a synchronization task.

```
public void deleteSyncJob(String SyncJobId,DefaultAcsClient client) {
    DeleteSynchronizationJobRequest request = new DeleteSynchronizationJobRequest();
    request.setSynchronizationJobId(SyncJobId);
    DeleteSynchronizationJobResponse response = new DeleteSynchronizationJobResponse();
    try {
       response = client.getAcsResponse(request);
       System.out.println("Delete Sync Job "+SyncJobId+ " Succeed!") ;
    } catch (Exception e) {
       // TODO: handle exception
       System.out.println("Delete Sync Job "+SyncJobId+ " Failed!") ;
    }
  }
```

2.12.1.4.4. DescribeDataLoadStatus

2.12.1.4.4.1. Overview

You can call this operation to query initial synchronization details regardless of the synchronization task status.

2.12.1.4.4.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeDataLoadStatus.
SynchronizationJobId	String	Yes	The synchronization task ID.
StructureInitialization	Boolean	No	The schema initialization details.
DataInitialization	Boolean	No	The full data initialization details.
DataSynchronization	Boolean	No	The incremental data initialization details.
PageSize	Integer	No	The number of records on each page. Valid values: 30, 50, and 100. Default value: 30. This parameter is required when only one of these three parameters is set to true: StructureInitialization, DataInitialization, and DataSynchronization.
PageNum	Integer	No	The page number. It must be greater than 0 and smaller than or equal to the maximum value of Integer. Default value: 1. This parameter is required when only one of these three parameters is set to true: StructureInitialization, DataInitialization, and DataSynchronization.

2.12.1.4.4.3. Response parameters

Name	Type	Description
<Common response parameters>	-	The request ID.

2.12.1.4.4.4. Examples

The following code provides an example of how to use the Java SDK to query the initial synchronization details.

```
public void descInitStatus(String SyncJobId, DefaultAcsClient client) {
    DescribeInitializationStatusRequest request = new DescribeInitializationStatusRequest();
    request.setSynchronizationJobId(SyncJobId);
    DescribeInitializationStatusResponse response = new DescribeInitializationStatusResponse();
    try {
      response = client.getAcsResponse(request);
      System.out.println("Describe Initialization Detail of Synchronization Job "+SyncJobId+" Succeed!")
;
      List<StructureInitializationDetail> strucInitDetails  = response.getStructureInitializationDetails();
      List<DataInitializationDetail> dataInitDetails  = response.getDataInitializationDetails();
      List<com.aliyuncs.dts.model.v20160801. DescribeInitializationStatusResponse.DataSynchronizatio
nDetail> dataSynchronizationDetails = response.getDataSynchronizationDetails();
      System.out.println("Structure Initialization Detail:");
      for (int i = 0; i < strucInitDetails.size(); i++) {
        System.out.println("ObjectName:"+strucInitDetails.get(i).getObjectName()
            +"; ObjectType:"+strucInitDetails.get(i).getObjectType()
            +"; SRCDBName:"+strucInitDetails.get(i).getSourceOwnerDBName()
            +"; DESTDBName:"+strucInitDetails.get(i).getDestinationOwnerDBName()
            +"; Status:"+strucInitDetails.get(i).getStatus()
            +"; ErrMSG:"+strucInitDetails.get(i).getErrorMessage());
      }
      System.out.println("Data Initialization Detail:");
      for (int i = 0; i < dataInitDetails.size(); i++) {
        System.out.println("TableName:"+dataInitDetails.get(i).getTableName()
            +"; SRCDBName:"+dataInitDetails.get(i).getSourceOwnerDBName()
            +"; DESTDBName:"+dataInitDetails.get(i).getDestinationOwnerDBName()
            +"; Status:"+dataInitDetails.get(i).getStatus()
            +"; TotalRows:"+dataInitDetails.get(i).getTotalRowNum()
            +"; FinishedRows:"+dataInitDetails.get(i).getFinishRowNum()
            +"; UsedTime:"+dataInitDetails.get(i).getUsedTime()
            +"; ErroMSG:"+dataInitDetails.get(i).getErrorMessage());
      }
      System.out.println("Data Synchronization Detail:");
      for (int i = 0; i < dataSynchronizationDetails.size(); i++) {
        System.out.println("TableName:"+dataSynchronizationDetails.get(i).getTableName()
            +"; SRCDBName:"+dataSynchronizationDetails.get(i).getSourceOwnerDBName()
            +"; DESTDBName:"+dataSynchronizationDetails.get(i).getDestinationOwnerDBName()
```

```
                +"; Status:"+dataSynchronizationDetails.get(i).getStatus()
                +"; ErrMSG:"+dataSynchronizationDetails.get(i).getErrorMessage());
        }
    } catch (Exception e) {
        // TODO: handle exception
        System.out.println("Describe Initialization Status of Synchronization Job "+SyncJobId+" Failed!") ;
        System.out.println(e.toString());
    }
}
```

2.12.1.4.5. DescribeSynchronizationJobStatus

2.12.1.4.5.1. Overview

You can call this operation to query the status and running details of a synchronization task regardless of its status.

2.12.1.4.5.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSynchronizationJobStatus.
SynchronizationJobId	String	Yes	The ID of the synchronization instance.
SynchronizationDirection	String	No	The synchronization direction. Valid values: Forward and Reverse. Default value: Forward.

2.12.1.4.5.3. Response parameters

Name	Type	Description
SynchronizationJobId	String	The synchronization task ID.
SynchronizationJobName	String	The synchronization task name.
SynchronizationJobClass	String	The synchronization task type.
PayType	String	The billing method.

Name	Type	Description
ExpireTime	String	The expiration time, in the format of YYYY-MM-DDT hh:mm:ssZ, such as 2011-06-09T 12:11:11Z.
SourceEndpoint	SourceEndpoint	The endpoint to access the source instance specified in the synchronization task.
DestinationEndpoint	DestinationEndpoint	The endpoint to access the destination instance specified in the synchronization task.
SynchronizationObjects	List	The objects to be synchronized.
StructureInitialization	String	Indicates whether to perform schema initialization.
DataInitialization	String	Indicates whether to perform full data initialization.
Status	String	The synchronization task status. Valid values: NotStarted, Prechecking, PrecheckFailed, Initializating, InitializeFailed, Synchronizing, Failed, Suspending, Modifying, and Finished.
ErrorMessage	String	The cause of the synchronization error.
PrecheckStatus	PrecheckStatus	The precheck status. For more information, see PrecheckStatus parameter definitions.
StructureInitializationStatus	StructureInitializationStatus	The schema initialization status. For more information, see StructureInitializationStatus parameter definitions.
DataInitializationStatus	DataInitializationStatus	The full data initialization status. For more information, see DataInitializationStatus parameter definitions.
DataSynchronizationStatus	DataSynchronizationStatus	The incremental data initialization status. For more information, see DataSynchronizationStatus parameter definitions.
Delay	String	The synchronization latency. Unit: second.
Performance	String	The synchronization performance. For more information, see Performance parameter definitions.

2.12.1.4.5.4. PrecheckStatus parameter definitions

Name	Type	Description
Status	String	The precheck status.
Percent	String	The precheck progress. Unit: %.
Detail	List	The check details of each precheck item. For more information, see CheckItem parameter definitions.

2.12.1.4.5.5. CheckItem parameter definitions

Name	Type	Description
ItemName	String	The check item name.
CheckStatus	String	The check status. Valid values: • NotStarted • Checking • Failed • Finished
ErrorMessage	String	The cause of the error.
RepairMethod	String	The repair method.

2.12.1.4.5.6. StructureInitializationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.

Name	Type	Description
Progress	String	The number of tables that have been migrated.

2.12.1.4.5.7. DataInitializationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Progress	String	The number of tables that have been migrated.

2.12.1.4.5.8. DataSynchronizationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Delay	String	The migration latency. Unit: second.

2.12.1.4.5.9. Performance parameter definitions

Name	Type	Description
TPS	String	The number of records that are synchronized per second.
Flow	String	The data traffic that is synchronized per second. Unit: Mbit/s.

2.12.1.4.5.10. Examples

The following code provides an example of how to use the Java SDK to query the status of a synchronization task.

```
public void descSyncJobStatus(String SyncJobId,DefaultAcsClient client) {
    DescribeSynchronizationJobStatusRequest request = new DescribeSynchronizationJobStatusReques
t();
    request.setSynchronizationJobId(SyncJobId);
    DescribeSynchronizationJobStatusResponse response = new DescribeSynchronizationJobStatusRes
ponse();
    try {
      response = client.getAcsResponse(request);
      /*Get Sync Configure of the Sync Job*/
      System.out.println("SyncJobId:"+response.getSynchronizationJobId()
          +"SyncJobName:"+response.getSynchronizationJobName()
          +"; PayType:"+response.getPayType()+"; ExpireTime:"+response.getExpireTime()
          +"; SyncClass:"+response.getSynchronizationJobClass()
          +"; StrucInit:"+response.getStructureInitialization()
          +"; DataInit:"+response.getDataInitialization()+"; Status:"+response.getStatus()
          +"; Delay:"+response.getDelay()
          +"; ErrMSG:"+response.getErrorMessage());
      /*Get Sync Objects of the Sync Job*/
      System.out.println("Sync Objects:");
      List<SynchronizationObject> syncObjects = response.getSynchronizationObjects();
      /*Get the Source Endpoint of the synchronization job*/
      SourceEndpoint sourceEndpoint = response.getSourceEndpoint();
      System.out.println("InstanceType:"+sourceEndpoint.getInstanceType()
          +"InstanceId:"+sourceEndpoint.getInstanceId());
      /*Get the Destination Endpoint of the synchronization job*/
      DestinationEndpoint destinationEndpoint = new DestinationEndpoint();
      System.out.println("Instance Type:"+destinationEndpoint.getInstanceType()
          +destinationEndpoint.getInstanceId());
      // Get Sync Object of the synchronization job
      System.out.println("SyncObject:"+org.json.JSONObject.valueToString(syncObjects));
```

```
        // Get Precheck Status of the synchronization job
        try {
            com.aliyuncs.dts.model.v20160801. DescribeSynchronizationJobStatusResponse.PrecheckStatus
precheckStatus = response.getPrecheckStatus();
            System.out.println("Get Precheck Status for Sync Job Succeed");
            System.out.println("Precheck Status:"+response.getPrecheckStatus().getStatus()
                  +";  Precheck Percent:"+response.getPrecheckStatus().getPercent());
            List<com.aliyuncs.dts.model.v20160801. DescribeSynchronizationJobStatusResponse.PrecheckSt
atus.CheckItem> precheckDetails= precheckStatus.getDetail();
            for (int i = 0; i < response.getPrecheckStatus().getDetail().size(); i++) {
               System.out.println("CheckItem:"+response.getPrecheckStatus().getDetail().get(i).getCheckSt
atus()
                     +"; ErrorMSG:"+response.getPrecheckStatus().getDetail().get(i).getErrorMessage()
                     +"; RepairMethod:"+response.getPrecheckStatus().getDetail().get(i).getRepairMethod()
);
            }
        } catch (Exception e) {
            // TODO: handle exception
            System.out.println("Get Precheck Status for Sync Job Failed");
        }
        // Get Structure Initialization Status of the synchronization job
        try {
            System.out.println("Get Structure Initialization Status Succeed!") ;
            System.out.println("Structure Init Status:"+response.getStructureInitializationStatus().getStat
us()
                  +"; Percent:"+response.getStructureInitializationStatus().getPercent()
                  +"; Progress:"+response.getStructureInitializationStatus().getProgress()
                  +"; ErrMSG:"+response.getStructureInitializationStatus().getErrorMessage());
        } catch (Exception e) {
            // TODO: handle exception
            System.out.println("Get Structure Init Status Failed!") ;
        }
        // Get Data Initialization Status of the synchronization job
        try {
            System.out.println("Get Data Initialization Status Succeed!") ;
            System.out.println("Data Init Status:"+response.getDataInitializationStatus().getStatus()
                  +"; Percent:"+response.getDataInitializationStatus().getPercent()
                  +"; Progress:"+response.getDataInitializationStatus().getProgress()
                  +"; ErrMSG:"+response.getDataInitializationStatus().getErrorMessage());
        } catch (Exception e) {
            // TODO: handle exception
```

```
            System.out.println("Get Data Init Status Failed!") ;
            System.out.println(e.toString());
        }
        //Get Data Sync Status
        try {
            com.aliyuncs.dts.model.v20160801. DescribeSynchronizationJobStatusResponse.DataSynchroniz
ationStatus dataSyncStatus = response.getDataSynchronizationStatus();
            System.out.println("Get Data Synchronization Status Succeed!") ;
            System.out.println("Data Sync Status:"+response.getDataSynchronizationStatus().getStatus()
                    +"; Percent:"+response.getDataSynchronizationStatus().getPercent()
                    +"; Delay:"+response.getDataSynchronizationStatus().getDelay()
                    +"; ErrMSG:"+response.getDataSynchronizationStatus().getErrorMessage());
        } catch (Exception e) {
            // TODO: handle exception
            System.out.println("Get Data Sync Status Failed!") ;
            System.out.println(e.toString());
        }
        //Get Performance
        System.out.println("TPS:"+response.getPerformance().getRPS()
                +"Flow:"+response.getPerformance().getRPS());
    } catch (Exception e) {
        // TODO: handle exception
        System.out.println("Describe Status of Data Sync Job "+ SyncJobId + "Failed");
        System.out.println(e.toString());
    }
  }
```

2.12.1.4.6. DescribeSynchronizationJobs

2.12.1.4.6.1. Overview

You can call this operation to query the status and details of all synchronization tasks under the current account.

2.12.1.4.6.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeSynchronizationJobs.

Name	Type	Required	Description
PageSize	Integer	No	The number of records on each page. Valid values: 30, 50, and 100. Default value: 30.
PageNum	Integer	No	The page number. It must be greater than 0 and smaller than or equal to the maximum value of Integer. Default value: 1.

2.12.1.4.6.3. Response parameters

Name	Type	Description
PageNumber	Integer	The page number.
TotalRecordCount	Integer	The total number of records.
PageRecordCount	Integer	The number of records on the page.
SynchronizationInstances	List	The synchronization task status. For more information, see SynchronizationInstance parameter definitions.

2.12.1.4.6.4. SynchronizationInstance parameter definitions

Name	Type	Description
SynchronizationJobId	String	The synchronization task ID.
SynchronizationJobName	String	The synchronization task name.
SynchronizationJobClass	String	The synchronization task type.
PayType	String	The billing method.
ExpireTime	String	The expiration time, in the format of YYYY-MM-DDT hh:mm:ssZ, such as 2011-06-09T 12:11:11Z.
SourceEndpoint	SourceEndpoint	The endpoint to access the source instance specified in the synchronization task.

Name	Type	Description
DestinationEndpoint	DestinationEndpoint	The endpoint to access the destination instance specified in the synchronization task.
SynchronizationObjects	List	The objects to be synchronized.
StructureInitialization	String	Indicates whether to perform schema initialization.
DataInitialization	String	Indicates whether to perform full data initialization.
Status	String	The synchronization task status. Valid values: • NotStarted • Prechecking • PrecheckFailed • Initializating • InitializeFailed • Synchronizing • Failed • Suspending • Modifying • Finished
ErrorMessage	String	The cause of the synchronization error.
PrecheckStatus	PrecheckStatus	The precheck status. For more information, see PrecheckStatus parameter definitions.
StructureInitializationStatus	StructureInitializationStatus	The schema initialization status. For more information, see StructureInitializationStatus parameter definitions.
DataInitializationStatus	DataInitializationStatus	The full data initialization status. For more information, see DataInitializationStatus parameter definitions.
DataSynchronizationStatus	DataSynchronizationStatus	The incremental data initialization status. For more information, see DataSynchronizationStatus parameter definitions.

Name	Type	Description
Delay	String	The synchronization latency. Unit: second.
Performance	String	The synchronization performance. For more information, see Performance parameter definitions.

2.12.1.4.6.5. PrecheckStatus parameter definitions

Name	Type	Description
Status	String	The precheck status.
Percent	String	The precheck progress. Unit: %.
Detail	List	The check details of each precheck item. For more information, see CheckItem parameter definitions.

2.12.1.4.6.6. CheckItem parameter definitions

Name	Type	Description
ItemName	String	The check item name.
CheckStatus	String	The check status. Valid values: • NotStarted • Checking • Failed • Finished
ErrorMessage	String	The cause of the error.
RepairMethod	String	The repair method.

2.12.1.4.6.7. StructureInitializationStatus parameter definitions

Name	Type	Description

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Progress	String	The number of tables that have been migrated.

2.12.1.4.6.8. DataInitializationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Progress	String	The number of tables that have been migrated.

2.12.1.4.6.9. DataSynchronizationStatus parameter definitions

Name	Type	Description

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Delay	String	The migration latency. Unit: second.

2.12.1.4.6.10. Performance parameter definitions

Name	Type	Description
TPS	String	The number of records that are synchronized per second.
Flow	String	The data traffic that is synchronized per second. Unit: Mbit/s.

2.12.1.4.6.11. Examples

The following code provides an example of how to use the Java SDK to query the list of synchronization tasks.

```
public void descSyncJobs(DefaultAcsClient client) {
    DescribeSynchronizationJobsRequest request = new DescribeSynchronizationJobsRequest();
    DescribeSynchronizationJobsResponse response = new DescribeSynchronizationJobsResponse();
    try {
      response = client.getAcsResponse(request);
      System.out.println("Describe all Synchronization Jobs Succeed!") ;
      List<SynchronizationInstance> syncInstances=response.getSynchronizationInstances();
      System.out.println("Total num of Synchronization Jobs:"+syncInstances.size());
      for (SynchronizationInstance syncInstance : syncInstances) {
        System.out.println("SyncJobId:"+syncInstance.getSynchronizationJobId()
            +"; SyncJobName:"+syncInstance.getSynchronizationJobName()
            +"; PayType:"+syncInstance.getPayType()
            +"; InstanceClass:"+syncInstance.getSynchronizationJobClass()
```

```
                +"; StrucInit:"+syncInstance.getStructureInitialization()
                +"; DataInit:"+syncInstance.getDataInitialization()
                +"; Status:"+syncInstance.getStatus()
                +"; ErrMSG:"+syncInstance.getErrorMessage()
                +"; Delay:"+syncInstance.getDelay());
            System.out.println("SourceEndpointInstanceType:"+syncInstance.getSourceEndpoint().getInsta
nceType()
                +"SourceEnpointInstanceId:"+syncInstance.getSourceEndpoint().getInstanceId());
            System.out.println("DestEndpointInstanceType:"+syncInstance.getDestinationEndpoint().getIn
stanceType()
                +"DestEndpointInstanceId:"+syncInstance.getDestinationEndpoint().getInstanceId());
            // Get Precheck Status
            try {
              com.aliyuncs.dts.model.v20160801. DescribeSynchronizationJobsResponse.SynchronizationIns
tance.PrecheckStatus precheckStatus = syncInstance.getPrecheckStatus();
              System.out.println("Get Precheck Status for Sync Job Succeed");
              System.out.println("Precheck Status:"+syncInstance.getPrecheckStatus().getStatus()
                  +"Precheck Percent:"+syncInstance.getPrecheckStatus().getPercent());
              for (int j = 0; j < syncInstance.getPrecheckStatus().getDetail().size(); j++) {
                System.out.println("CheckItem:"+syncInstance.getPrecheckStatus().getDetail().get(j).getC
heckStatus()
                    +"; ErrorMSG:"+syncInstance.getPrecheckStatus().getDetail().get(j).getErrorMessage(
)
                    +"; RepairMethod:"+syncInstance.getPrecheckStatus().getDetail().get(j).getRepairMet
hod());
              }
            } catch (Exception e) {
              // TODO: handle exception
              System.out.println("Get Precheck Status for Sync Job Failed");
            }
            // Get Structure Initialization Status
            try {
              System.out.println("Get Structure Initialization Status Succeed!") ;
              System.out.println("Structure Init Status:"+syncInstance.getStructureInitializationStatus().ge
tStatus()
                  +"; Percent:"+syncInstance.getStructureInitializationStatus().getPercent()
                  +"; Progress:"+syncInstance.getStructureInitializationStatus().getProgress()
                  +"; ErrMSG:"+syncInstance.getStructureInitializationStatus().getErrorMessage());
            } catch (Exception e) {
              // TODO: handle exception
              System.out.println("Get Structure Initialization Status Failed!") ;
            }
```

```
            }
            // Get Data Initialization Status
            try {
               System.out.println("Get Data Init Status Succeed!") ;
               System.out.println("Data Init Status:"+syncInstance.getDataInitializationStatus().getStatus()
                     +"; Percent:"+syncInstance.getDataInitializationStatus().getPercent()
                     +"; Progress:"+syncInstance.getDataInitializationStatus().getProgress()
                     +"; ErrMSG:"+syncInstance.getDataInitializationStatus().getErrorMessage());
            } catch (Exception e) {
               // TODO: handle exception
               System.out.println("Get Data Init Status Failed!") ;
               System.out.println(e.toString());
            }
            //Get Data Synchronization Status
            try {
               System.out.println("Get Data Synchronization Status Succeed!") ;
               System.out.println("Data Sync Status:"+syncInstance.getDataSynchronizationStatus().getSta
tus()
                     +"; Percent:"+syncInstance.getDataSynchronizationStatus().getPercent()
                     +"; Delay:"+syncInstance.getDataSynchronizationStatus().getDelay()
                     +"; ErrMSG:"+syncInstance.getDataSynchronizationStatus().getErrorMessage());
            } catch (Exception e) {
               // TODO: handle exception
               System.out.println("Get Data Sync Status Failed!") ;
               System.out.println(e.toString());
            }
         }
      } catch (Exception e) {
         // TODO: handle exception
         System.out.println("Desc all Sync Jobs Failed!") ;
         System.out.println(e.toString());
      }
   }
```

2.12.1.4.7. DescribeObjectModifyStatus

2.12.1.4.7.1. Overview

After you call the ModifySynchronizationObject operation to modify the list of objects to be synchronized, you can call this operation to query the modification status and progress.

2.12.1.4.7.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to DescribeObjectModifyStatus.
TaskId	String	Yes	The ID of the task for modifying the list of objects to be synchronized. It is the response parameter of the ModifySynchronizationObject operation.

2.12.1.4.7.3. Response parameters

Name	Type	Description
Status	String	The modification status of the list of objects to be synchronized. Valid values: • NotStarted • Prechecking • PrecheckFailed • Migrating • Failed • Finished
ErrorMessage	String	The reason why the list of objects to be synchronized failed to be modified.
PrecheckStatus	PrecheckStatus	The precheck status. For more information, see PrecheckStatus parameter definitions.
StructureInitializationStatus	StructureInitializationStatus	The schema initialization status. For more information, see StructureInitializationStatus parameter definitions.
DataInitializationStatus	DataInitializationStatus	The full data initialization status. For more information, see DataInitializationStatus parameter definitions.
DataSynchronizationStatus	DataSynchronizationStatus	The incremental data initialization status. For more information, see DataSynchronizationStatus parameter definitions.

2.12.1.4.7.4. PrecheckStatus parameter definitions

Name	Type	Description
Status	String	The precheck status.
Percent	String	The precheck progress. Unit: %.
Detail	List	The check details of each precheck item. For more information, see CheckItem parameter definitions.

2.12.1.4.7.5. CheckItem parameter definitions

Name	Type	Description
ItemName	String	The check item name.
CheckStatus	String	The check status. Valid values: • NotStarted • Checking • Failed • Finished
ErrorMessage	String	The cause of the error.
RepairMethod	String	The repair method.

2.12.1.4.7.6. StructureInitializationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Progress	String	The number of tables that have been migrated.

2.12.1.4.7.7. DataInitializationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Progress	String	The number of tables that have been migrated.

2.12.1.4.7.8. DataSynchronizationStatus parameter definitions

Name	Type	Description
Status	String	The migration status. Valid values: • NotStarted • Migrating • Failed • Finished
ErrorMessage	String	The cause of the migration error.
Percent	String	The migration progress. Unit: %.
Delay	String	The migration latency.

2.12.1.4.7.9. Examples

The following code provides an example of how to use the Java SDK to query the status of a task for modifying the list of objects to be synchronized.

```
public void descObjectModifyStatus(String SyncJobId,String TaskId,DefaultAcsClient client) {
        DescribeSynchronizationObjectModifyStatusRequest request = new DescribeSynchronizationObject
ModifyStatusRequest();
        request.setTaskId(TaskId);
```

```
    request.setRegionId(regionId);
    DescribeSynchronizationObjectModifyStatusResponse response = new DescribeSynchronizationObj
ectModifyStatusResponse();
    try {
      response = client.getAcsResponse(request);
      System.out.println("Describe Sync Object Modify Status Succeed!") ;
      String status=response.getStatus();
      PrecheckStatus precheckStatus = response.getPrecheckStatus();
      StructureInitializationStatus strucInitStatus=response.getStructureInitializationStatus();
      DataInitializationStatus dataInitStatus=response.getDataInitializationStatus();
      DataSynchronizationStatus dataSyncStatus = response.getDataSynchronizationStatus();
      String errorMSG=response.getErrorMessage();
      //Get Precheck Status
      System.out.println("The precheck status of SYNC Job "+SyncJobId);
      String precheck_status=precheckStatus.getStatus();
      String precheck_percent=precheckStatus.getPercent();
      System.out.println("Precheck Status:"+precheckStatus.getStatus()
          +"; Precheck Percent:"+precheckStatus.getPercent());
      System.out.println("Precheck Detail:");
      for (int i = 0; i < precheckStatus.getDetail().size(); i++) {
        String ItemName=precheckStatus.getDetail().get(i).getItemName();
        String CheckStatus=precheckStatus.getDetail().get(i).getCheckStatus();
        String CheckErrorMsg=precheckStatus.getDetail().get(i).getErrorMessage();
        String RepairMethod = precheckStatus.getDetail().get(i).getRepairMethod();
        System.out.println("CheckItme:"+ItemName+"; Status:"+CheckStatus+"; ErrorMSG:"+CheckError
Msg
            +"; RepairMethod:"+RepairMethod);
      }
      // Get the status of the structure Initialization
      String strucInit_Status=strucInitStatus.getStatus();
      String strucInit_percent=strucInitStatus.getPercent();
      String strucInit_progress=strucInitStatus.getProgress();
      String strucInit_ErrMsg=strucInitStatus.getErrorMessage();
      System.out.println("The Structure Init Status of SYNC Job "+SyncJobId);
      System.out.println("Status:"+strucInit_Status+"; Percent:"+strucInit_percent
          +"; Progress:"+strucInit_progress+"; ErrMSG:"+strucInit_ErrMsg);
      // Get the status of the data Initialization
      String dataInit_Status=dataInitStatus.getStatus();
      String dataInit_Percent = dataInitStatus.getPercent();
      String dataInit_Progress = dataInitStatus.getProgress();
      String dataInit_ErrMSG = dataInitStatus.getErrorMessage();
      System.out.println("The data Init Status of SYNC Job "+SyncJobId);
```

```
        System.out.println("Status:"+dataInit_Status+"; Percent:"+dataInit_Percent
            +"; Progress:"+dataInit_Progress+"; ErrMSG:"+dataInit_ErrMSG);
        // Get the status of the data synchronization
        String dataSync_Status=dataSyncStatus.getStatus();
        String dataSync_Percent=dataSyncStatus.getPercent();
        String dataSync_Delay=dataSyncStatus.getDelay();
        String dataSync_ErrMSG=dataSyncStatus.getErrorMessage();
        System.out.println("The data Init Status of SYNC Job "+SyncJobId);
        System.out.println("Status:"+dataSync_Status+"; Percent:"+dataSync_Percent
            +"; Delay:"+dataSync_Delay+"; ErrMSG:"+dataSync_ErrMSG);
    } catch (Exception e) {
        // TODO: handle exception
        System.out.println("Describe Synchronization Objects Modify Status Failed");
        System.out.println(e.toString());
    }
}
```

2.12.1.4.8. ModifySynchronizationObject

2.12.1.4.8.1. Overview

When a synchronization task is in the NotStarted, Synchronizing, Failed, or Suspending status, you can call this operation to modify the list of objects to be synchronized. After that, you can call the DescribeObjectModifyStatus operation to query the detailed modification status of the list of objects to be synchronized.

2.12.1.4.8.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to ModifySynchronization Object.
SynchronizationJobId	String	Yes	The ID of the synchronization task.
SynchronizationObjects	List	Yes	The list of modified objects to be synchronized.

2.12.1.4.8.3. Response parameters

Name	Type	Description
TaskId	String	The ID of the task for modifying the list of objects to be synchronized. You can call the DescribeObjectModifyStatus operation based on this ID to query the modification status.

2.12.1.4.8.4. Examples

The following code provides an example of how to use the Java SDK to modify the list of objects to be synchronized.

```
public String modifySyncObjects(String SyncJobId,DefaultAcsClient client) {
        String SyncObject="[{\"DBName\":\"jiangliutest\",\"NewDBName\":\"jiangliutest\","
                + "\"TableIncludes\":[{\"TableName\":\"t2\",\"NewTableName\":\"t2\"}]}]";
        ModifySynchronizationObjectRequest request = new ModifySynchronizationObjectRequest();
        request.setSynchronizationJobId(SyncJobId);
        request.setSynchronizationObjects(SyncObject);
        ModifySynchronizationObjectResponse response = new ModifySynchronizationObjectResponse();
        try {
            response = client.getAcsResponse(request);
            String TaskId=response.getTaskId();
            System.out.println("Modify Sync Job "+SyncJobId+" Succeed! Modify task Id:"+TaskId);
            return TaskId;
        } catch (Exception e) {
            // TODO: handle exception
            System.out.println("Modify Sync Job "+ SyncJobId +" Failed!") ;
            System.out.println(e.toString());
            return null;
        }
    }
```

2.12.1.4.9. StartSynchronizationJob

2.12.1.4.9.1. Overview

When a synchronization task is in the NotStarted, Failed, or Suspending status, you can call this operation to start the synchronization task.

2.12.1.4.9.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to StartSynchronizationJob.
SynchronizationJobId	String	Yes	The synchronization task ID.

2.12.1.4.9.3. Response parameters

Name	Type	Description
<Common response parameters>	-	The request ID.

2.12.1.4.9.4. Examples

The following code provides an example of how to use the Java SDK to start a synchronization task.

```
public void startSyncJob(String SyncJobId,DefaultAcsClient client) {
      StartSynchronizationJobRequest request  = new StartSynchronizationJobRequest();
      request.setSynchronizationJobId(SyncJobId);
      StartSynchronizationJobResponse response = new StartSynchronizationJobResponse();
      try {
         response = client.getAcsResponse(request);
         System.out.println("Start Sync Job "+SyncJobId+" Succeed!") ;
      } catch (Exception e) {
         // TODO: handle exception
         System.out.println("Start Sync Job "+SyncJobId+ " Failed");
         System.out.println(e.toString());
      }
   }
```

2.12.1.4.10. SuspendSynchronizationJob

2.12.1.4.10.1. Overview

When a synchronization task is in the Synchronizing status, you can call this operation to suspend the synchronization task. If a synchronization task has been suspended for over 6 hours, it may fail to be started.

2.12.1.4.10.2. Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to SuspendSynchronizationJob.
SynchronizationJobId	String	Yes	The synchronization task ID.

2.12.1.4.10.3. Response parameters

Name	Type	Description
<Common response parameters>	-	The request ID.

2.12.1.4.10.4. Examples

The following code provides an example of how to use the Java SDK to suspend a synchronization task.

```
public void suspendSyncJob(String SyncJobId,DefaultAcsClient client) {
    SuspendSynchronizationJobRequest request = new SuspendSynchronizationJobRequest();
    request.setSynchronizationJobId(SyncJobId);
    SuspendSynchronizationJobResponse response = new SuspendSynchronizationJobResponse();
    try {
       response = client.getAcsResponse(request);
       System.out.println("Suspend Sync Job "+SyncJobId+ " Succeed!") ;
    } catch (Exception e) {
       // TODO: handle exception
       System.out.println("Suspend Sync Job "+SyncJobId+" Failed");
       System.out.println(e.toString());
    }
  }
```

2.12.2. Call the Java SDK

2.12.2.1. Quick start

This topic describes how to obtain and call the *DTS* Java SDK.

Install the Apsara Stack Java SDK

If you use Apache Maven to manage Java projects, you only need to import the JAR file to *pom.xml* of the project.

To use the development kit of Alibaba Cloud products, you must install the SDK core library and the product SDK.

The SDK core library version is 3.2.8, and the *DTS* SDK version is *2.0.3*.

```
<dependency>
   <groupId>com.aliyun</groupId>
   <artifactId>aliyun-java-sdk-core</artifactId>
   <version>3.2.8</version>
</dependency>
<dependency>
   <groupId>com.aliyun</groupId>
   <artifactId>aliyun-java-sdk-dts</artifactId>
   <version>2.0.3-SNAPSHOT</version>
</dependency>
```

Use the Java SDK

The DTS SDK includes two core kits: aliyun-java-sdk-core-inner and aliyun-java-sdk-dts. The aliyun-java-sdk-core-inner kit automatically routes requests to the DTS endpoint. The aliyun-java-sdk-dts kit includes the related classes of all DTS functions.

The following uses CreateMigrationJob, the method that uses the DTS Java SDK to create a data migration task, to describe the complete process of using the SDK. The aliyun-java-sdk-dts kit includes all classes used.

1. Create an object of IClientProfile named profile. This object stores the Access Key ID, Access Key Secret, and default region information.

   ```
   IClientProfile profile = DefaultProfile.getProfile("cn-hangzhou", accsessKeyId, accessSecret);
   ```

2. Create the DefaultAcsClient object. All subsequent responses are obtained from DefaultAcsClient.

   ```
   client = new DefaultAcsClient(profile);
   ```

3. Create a request for the corresponding method. The request class is named in the format of API method name + Request. For example, the name of the API method used to create a migration task is CreateMigrationJob, so the corresponding request class name is CreateMigrationJobRequest. You can use a constructor to create a default class.

   ```
   CreateMigrationJobRequest request=new CreateMigrationJobRequest();
   ```

4. Use the setXxx method of the request class to configure information that must be provided in API parameters. For example, configure the region and specification of a migration task.

```
request.setRegion("cn-hangzhou");
request.setMigrationJobClass("small");
```

5. Use the DefaultAcsClient object to obtain a response to the corresponding request.

```
ConfigureMigrationJobResponse response = client.getAcsResponse(request);
```

6. Call the getXxx method in the response to obtain a returned parameter value, such as the migration task ID.

```
String MigrationJobId = response.getMigrationJobId();
```

7. The call process is now completed.

2.12.2.2. User manual

2.12.2.2.1. Install the Java SDK

This topic describes how to install and use the *DTS* Java SDK.

The Apsara Stack Java SDK supports JDK V1.6 and later. You can install the latest JDK version by importing the JAR file.

You can click here to download the *DTS* JAR file.

If you are using Eclipse or IntelliJ, you can install the *DTS* Java SDK directly by importing the JAR file.

The installation method is as follows:

- In Eclipse

  To install the DTS Java SDK in Eclipse, follow these steps:

  i. Copy the downloaded `aliyun-java-sdk-dts-2.0.3.jar` file to your project folder.
  ii. In Eclipse, right click the project, and then select **Properties**.
  iii. In the dialog box that appears, choose **Java Build Path** > **Libraries** > **Add JARs** to add the downloaded JAR files.
  iv. Click **Apply and Close**.

- In IntelliJ

  To install the DTS Java SDK in IntelliJ, follow these steps:

  i. Copy the downloaded `aliyun-java-sdk-dts-2.0.3.jar` file to your project folder.
  ii. Open your project in IntelliJ, and choose **File** > **Project Structure** .
  iii. Click **Apply** and then **OK**.

2.12.2.2.2. Configure identity verification credentials

When using the Apsara Stack SDK to access Apsara Stack services, you must provide an authorized account for identity verification.

Currently, the Java SDK supports identity verification based on the AccessKey.

When an Access Key is used as the access credential, you need to configure the credential during client initialization.

> **Notice** Do not disclose any code that may contain your AccessKey. For example, do not commit the code to public GitHub projects. Otherwise, your Apsara Stack tenant account may be compromised.

```
DefaultProfile profile = DefaultProfile.getProfile(
   "<your-region-id>",        // The region ID.
   "<your-access-key-id>",    // The AccessKey ID of the authorized account.
   "<your-access-key-secret>"); // The AccessKey Secret of the authorized account.
```

2.12.2.2.3. Initiate a call

This topic describes how to use the *DTS* Java SDK to initiate a request.

Procedure

1. Create an AcsClient instance.

   ```
   IAcsClient client = new DefaultAcsClient(profile);
   ```

2. Create a request.

   A request class name is in the format of `${apiName}Request`, where ${apiName} indicates the API name, such as *CreateMigrationJobRequest*.

   When the SDKs of multiple services are used, different requests may have the same name. Distinguish the requests by service package.

   ```
   CreateMigrationJobRequest request=new CreateMigrationJobRequest();
   ```

3. Initiate a call and handle the response.

   ```
   try {
                   ConfigureMigrationJobResponse response = client.getAcsResponse(request);
                   System.out.println("Configure "+ MigrationJobId+ " Succeed");
                   } catch (Exception e) {
                   // TODO: handle exception
                   System.out.println("Configure "+MigrationJobId + " Failed!") ;
                   System.out.println(e.toString());
                   }
   ```

   In normal cases, all response fields are deserialized into the response. You can directly call `response.getXXX()` to obtain the response fields.

   However, if an exception occurs or you want to obtain the original HTTP response, you can use the `doAction()` method to obtain the original response.

```
HttpResponse response = client.doAction(request);
```

2.12.2.2.4. Troubleshooting

The Java SDK returns corresponding errors when errors occur on the server side or the SDK side. These errors contain detailed error information, including the error code and the error message.

In normal cases, you do not need to solve the errors returned by the Java SDK. You only need to handle the errors returned by the server.

- `ServerException` is the error returned by the server.
- `ClientException` is the error returned by the SDK side.

For example, when the following error occurs, you have to modify the AccessKey ID based on the error message.

```
com.aliyuncs.exceptions.ClientException: InvalidAccessKeyId.NotFound : Specified access key is not foun
d.
```

If you want to handle the errors returned by the Java SDK, refer to the following example to write your code:

```
try {
    FooResponse response = client.getAcsResponse(request);
    // The following code is used to solve returned errors:
    // ...
}catch (ServerException e){
    // You can add your own error handling logic here
    // For example, display the error message
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
    // If you cannot solve the error, submit a ticket and provide the request ID to Alibaba technical suppor
t personnel.
    System.out.println("ResponseId=" + e.getRequestId());
}catch (ClientException e){
    // You can add your own error handling logic here.
    // For example, display the error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
}
```

2.12.2.2.5. Errors and troubleshooting

The following are some common errors you may experience when using the Apsara Stack SDK.

Error code	Error message	Cause	Solution
SDK.CanNotResolveEndpoint	Can not resolve endpoint, please check the user guide	The SDK cannot automatically obtain the endpoint of the called product in the specified region.	Check whether the provided region ID and endpoint are correct. After obtaining the correct endpoint, run the following code to set the endpoint: `DefaultProfile.addEndpoint("your-region-id", "your-region-id", "product", "endpoint"");`
SDK.JsonUnmarshalError	Failed to unmarshal response	SDK response deserialization fails. In most cases, it is because the response structure received by the SDK does not conform to the API metadata. For example, the fields do not match or the format is incorrect.	You can use the `client.doAction(request)` method to obtain the original HTTP response.
SDK.TimeoutError	*The request timed out 4 times(3 for retry), perhaps we should have the threshold raised a little?*	The request has timed out and all retry attempts have failed.	In scenarios such as low network quality, we recommend that you increase the timeout value or the allowed number of retries.
SDK.ServerError: InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The operation only accepts HTTPS requests but not HTTP requests.	Add the following code before sending a request: `request.setProtocol(ProtocolType.HTTPS)`

2.13. Server Load Balancer (SLB)

2.13.1. API reference

2.13.1.1. List of operations by function

Instance operations

Operation	Description
CreateLoadBalancer	Creates an SLB instance.
DeleteLoadBalancer	Deletes an SLB instance.
SetLoadBalancerStatus	Sets the status of an SLB instance.
SetLoadBalancerName	Modifies the name of an SLB instance.
DescribeLoadBalancers	Queries created SLB instances.
DescribeLoadBalancerAttribute	Queries detailed information of a specified SLB instance.
DescribeRegions	Queries available regions.
DescribeZones	Queries the zone information of a specified region.

Listener operations

Operation	Description
TCP listeners	
CreateLoadBalancerTCPListener	Creates a TCP listener.
SetLoadBalancerTCPListenerAttribute	Modifies the configurations of a TCP listener.
DescribeLoadBalancerTCPListenerAttribute	Queries the configurations of a TCP listener.
UDP listeners	
CreateLoadBalancerUDPListener	Creates a UDP listener.
SetLoadBalancerUDPListenerAttribute	Modifies the configurations of a UDP listener.
DescribeLoadBalancerUDPListenerAttribute	Queries the configurations of a UDP listener.

Operation	Description
HTTP listeners	
CreateLoadBalancerHTTPListener	Creates an HTTP listener.
SetLoadBalancerHTTPListenerAttribute	Modifies the configurations of an HTTP listener.
DescribeLoadBalancerHTTPListenerAttribute	Queries the configurations of an HTTP listener.
HTTPS listeners	
CreateLoadBalancerHTTPSListener	Creates an HTTPS listener.
SetLoadBalancerHTTPSListenerAttribute	Modifies the configurations of an HTTPS listener.
DescribeLoadBalancerHTTPSListenerAttribute	Queries the configurations of an HTTPS listener.
General listener operations	
StartLoadBalancerListener	Enables a listener.
DeleteLoadBalancerListener	Deletes a listener.
StopLoadBalancerListener	Disables a listener.
Access control	
SetListenerAccessControlStatus	Enables or disables access control for a specified listener.
DescribeListenerAccessControlAttribute	Queries the access control configurations of a specified listener.
AddListenerWhiteListItem	Adds an IP address to the whitelist of a specified listener.
RemoveListenerWhiteListItem	Removes an IP address from the whitelist of a specified listener.
Forwarding rules	
CreateRules	Adds forwarding rules to a specified HTTP or HTTPS listener.
DeleteRules	Deletes forwarding rules.
DescribeRules	Queries the configured forwarding rules of a specified listener.

Operation	Description
SetRule	Modifies the target VServer group of a specified forwarding rule.
DescribeRuleAttribute	Queries detailed information of a specified forwarding rule.

Back-end server operations

Operation	Description
AddBackendServers	Adds back-end servers.
RemoveBackendServers	Removes back-end servers.
SetBackendServers	Sets the weights of back-end servers.
VServer groups	
CreateVServerGroup	Creates a VServer group and adds back-end servers to the VServer group.
SetVServerGroupAttribute	Modifies the configurations of a VServer group.
AddVServerGroupBackendServers	Adds back-end servers to a specified VServer group.
RemoveVServerGroupBackendServers	Removes back-end servers from a specified VServer group.
ModifyVServerGroupBackendServers	Replaces back-end servers in a specified VServer group.
DeleteVServerGroup	Deletes a specified VServer group.
DescribeVServerGroups	Queries created VServer groups.
DescribeVServerGroupAttribute	Queries detailed information of a specified VServer group.
Primary/secondary server groups	
CreateMasterSlaveServerGroup	Creates a primary/secondary server group.
DeleteMasterSlaveServerGroup	Deletes a primary/secondary server group.
DescribeMasterSlaveServerGroupAttribute	Queries detailed information of a specified primary/secondary server group.

Operation	Description
DescribeMasterSlaveServerGroups	Queries created primary/secondary server groups.

Tag operations

Operation	Description
AddTags	Adds tags to a specified SLB instance.
DescribeTags	Queries created tags.
RemoveTags	Removes tags from a specified SLB instance.

2.13.1.2. Make API requests

When you call an SLB API, an HTTP GET request is sent to the endpoint of the SLB API. You must add corresponding request parameters to the request based on the API description. After the API is called, the system returns the processing result. Requests and responses are encoded using UTF-8.

Request structure

RPC applies to SLB APIs. You can call SLB APIs by sending HTTP GET requests.

The request structure is as follows:

```
http://Endpoint/?Action=xx&Parameters
```

In the request,

- Endpoint: The endpoint for SLB APIs is `slb.example.com`.

  > **Note** `example.com` is a custom domain name. Contact the system administrator to obtain the domain name. For more information, see Obtain an endpoint.

- Action: The operation that you want to perform. For example, call DescribeLoadBalancers to query all created SLB instances.
- Version: The version of the APIs that you want to use. The current SLB API version is *2014-05-15*.
- Parameters: Request parameters that are separated with ampersands (&).

  Request parameters consist of common parameters and custom API parameters. Common parameters include the API version number and identity verification information. For more information, see Common parameters.

The following code provides an example of how to call DescribeLoadBalancers to query SLB instances that have been created.

> **Note** The API request is displayed in the following format:

```
https://slb.example.com/?Action=DescribeLoadBalancers
&Format=xml
&Version=2014-05-15
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&TimeStamp=2016-02-23T12:46:24Z
...
```

API authorization

To keep your account secure, we recommend that you call SLB APIs as a RAM user. Before calling SLB APIs as a RAM user, you must create a RAM user and assign corresponding permissions to it.

For more information about SLB resources and APIs that you can assign permissions to, see RAM authentication.

Add a signature to an API request

To secure your API, you must add signature information to the API request. SLB uses the signature in the request to verify the identity of the caller.

SLB implements symmetric encryption through an AccessKey ID and an AccessKey Secret to authenticate the request sender. The AccessKey is an identity credential issued to Apsara Stack tenant accounts and RAM users (similar to the login password). The AccessKey ID is used to identify the user. The AccessKey Secret is used to encrypt the signature string on the client side and to verify the signature string on the server side. The AccessKey Secret must be kept strictly confidential. For more information, see Obtain an AccessKey pair.

For an RPC API, you must add the signature to the API request in the following format:

`https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf`

Take DescribeLoadBalancers as an example. If the AccessKey ID is `testid`, and the AccessKey Secret is `testsecret`, the pre-signed request URL is as follows:

```
http://slb.example.com/?Action=DescribeLoadBalancers
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2014-05-26
&SignatureVersion=1.0
```

To calculate the signature, perform the following operations:

1. Use the request parameters to create a query string for the signature.

```
GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeLoadBalancers&Format%3DXML&SignatureMethod%3DHMAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&TimeStamp%3D2016-02-23T12%253A46%253A24Z&Version%3D2014-05-15
```

.

2. Calculate the HMAC value of the string you want to sign.

   Add an ampersand (&) to the AccessKey Secret and use the new string as the key to calculate the HMAC value. In this example, the key is `testsecret&` .

```
CT9X0VtwR86fNWSnsc6v8YGOjuE=
```

3. Add the signature to the request parameters:

```
http://slb.example.com/?Action=DescribeLoadBalancers
&TimeStamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2014-05-26
&SignatureVersion=1.0
&Signature=CT9X0VtwR86fNWSnsc6v8YGOjuE%3D
```

2.13.1.3. RAM authentication

Before calling an SLB API as a RAM user, you must use an Alibaba Cloud account to create an authorization policy to assign permissions to the RAM user. In the authorization policy, you must use an Alibaba Cloud Resource Name (ARN) as the unique identifier of the resource.

Available SLB resources

The following table describes the ARN format for different types of SLB resources.

Resource type	ARN format
LoadBalancer	`acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid`
	`acs:slb:$regionid:$accountid:loadbalancer/*`
	`acs:slb:*:$accountid:loadbalancer/*`
	`acs:slb:*:*:loadbalancer/*`
	`acs:slb:$regionid:$accountid:certificate/$servercertificateId`

Resource type	ARN format
Certificate	
	acs:slb:$regionid:$accountid:certificate/*

`$regionid/accoutid/servercertificateId` is the resource ID. `*` indicates the corresponding resources.

SLB APIs

The following table lists the APIs that can be authorized and their corresponding ARN formats.

API	ARN format
CreateLoadBalancer	acs:slb:$regionid:$accountid:loadbalancer/*
ModifyLoadBalancerInternetSpec	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DeleteLoadBalancer	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
SetLoadBalancerStatus	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
SetLoadBalancerName	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DescribeLoadBalancers	acs:slb:$regionid:$accountid:loadbalancer/*
DescribeLoadBalancerAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DescribeRegions	acs:slb:*:$accountid:*
UploadServerCertificate	acs:slb:%s:%s:certificate/*
DeleteServerCertificate	acs:slb:%s:%s:certificate/%
DescribeServerCertificate	acs:slb:%s:%s:certificate/%
SetServerCertificateName	acs:slb:%s:%s:certificate/%
DescribeServerCertificates	acs:slb:%s:%s:certificate/*
CreateLoadBalancerHTTPListener	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
CreateLoadBalancerHTTPSListener	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
	acs:slb:%s:%s:certificate/%
CreateLoadBalancerTCPListener	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid

API	ARN format
CreateLoadBalancerUDPListener	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DeleteLoadBalancerListener	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
StartLoadBalancerListener	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
StopLoadBalancerListener	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
SetLoadBalancerHTTPListenerAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
SetLoadBalancerHTTPSListenerAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid acs:slb:%s:%s:certificate/%
SetLoadBalancerTCPListenerAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
SetLoadBalancerUDPListenerAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DescribeLoadBalancerHTTPListenerAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DescribeLoadBalancerHTTPSListenerAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DescribeLoadBalancerTCPListenerAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DescribeLoadBalancerUDPListenerAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
AddBackendServers	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid acs:ecs:$regionid:$accountid:instance/$instanceid
RemoveBackendServers	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid acs:ecs:$regionid:$accountid:instance/$instanceid
SetBackendServers	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid acs:ecs:$regionid:$accountid:instance/$instanceid
DescribeHealthStatus	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid

API	ARN format
CreateVServerGroup	acs:ecs:$regionid:$accountid:instance/$instanceid
SetVServerGroupAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DeleteVServerGroup	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DescribeVServerGroups	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
DescribeVServerGroupAttribute	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid
AddVServerGroupBackendServers	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid acs:ecs:$regionid:$accountid:instance/$instanceid
RemoveVServerGroupBackendServers	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid acs:ecs:$regionid:$accountid:instance/$instanceid
ModifyVServerGroupBackendServers	acs:slb:$regionid:$accountid:loadbalancer/$loadbalancerid acs:ecs:$regionid:$accountid:instance/$instanceid

2.13.1.4. Common parameters

Common request parameters

Common request parameters are request parameters that you must use when you call any API.

Common request parameters

Name	Type	Required	Description
Format	String	No	The format of the response. Valid values: *JSON (default) | XML*
Version	String	Yes	The API version in the format of `YYYY-MM-DD`. Valid values: *2014-05-15*
AccessKeyId	String	Yes	The AccessKey ID that is used to access a service.
Signature	String	Yes	The signature result string.

Name	Type	Required	Description
SignatureMethod	String	Yes	The algorithm used to create the request signature. Valid values: *HMAC-SHA1*
Timestamp	String	Yes	The request timestamp. The timestamp uses UTC and it complies with the ISO 8601 standard. The timestamp format is `YYYY-MM-DDThh:mm:ssZ`. For example, 20:00:00 on January 1st, 2013 in China Standard Time (UTC +8) would be written as 2013-01-10T12:00:00Z.
SignatureVersion	String	Yes	The signature algorithm version. Valid value: 1.0
SignatureNonce	String	Yes	A unique random number that is used to prevent network replay attacks. You must use different random numbers for different requests.

Example

```
http://slb.example.com/?Action=DescribeLoadBalancers
&TimeStamp=2014-05-19T10%3A33%3A56Z
&Format=xml
&AccessKeyId=testid
&Action=DescribeLoadBalancerAttribute
&SignatureMethod=Hmac-SHA1
&LoadBalancerId=loadBalancerID
&SignatureNonce=NwDAxvLU6tFE0DVb
&Version=2014-05-15
&SignatureVersion=1.0
&Signature=Signature
```

Common response parameters

API responses use a unified format. The 2xx HTTP status code indicates a successful invocation. The 4xx or 5xx HTTP status code indicates a failed invocation. The responses can be returned in JSON or XML format. The XML format is used by default. You can specify the format when calling an API.

Each time a request is sent to call an API, the system returns a unique identifier RequestId, regardless of whether the invocation is successful.

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
  <!—Result root node-->
  <API name+Response>
    <!—Returned request tag-->
    <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
    <!—Returned result-->
  </API name+Response>
```

- JSON format

```
{
  "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
  /*Returned result*/
  }
```

2.13.1.5. Obtain an AccessKey pair

You can obtain the AccessKey pair on the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

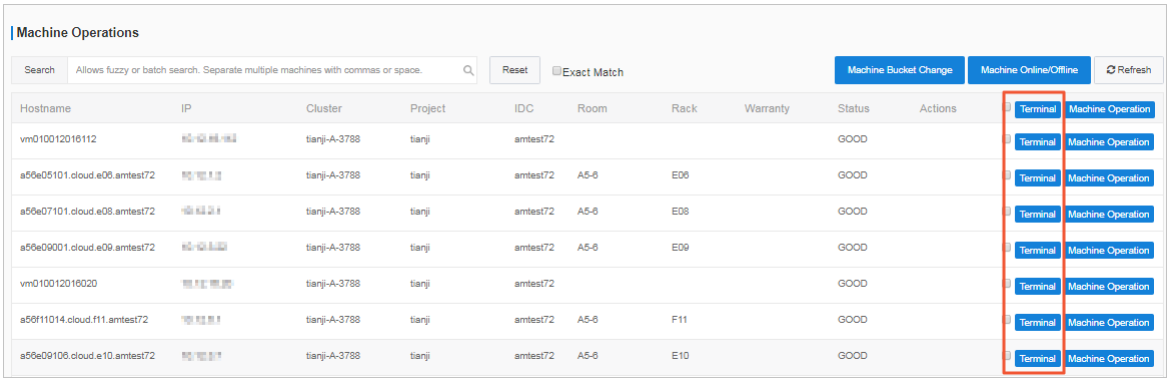
1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**. The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.13.1.6. Obtain an endpoint

You can obtain the product endpoint in Apsara Stack Operations.

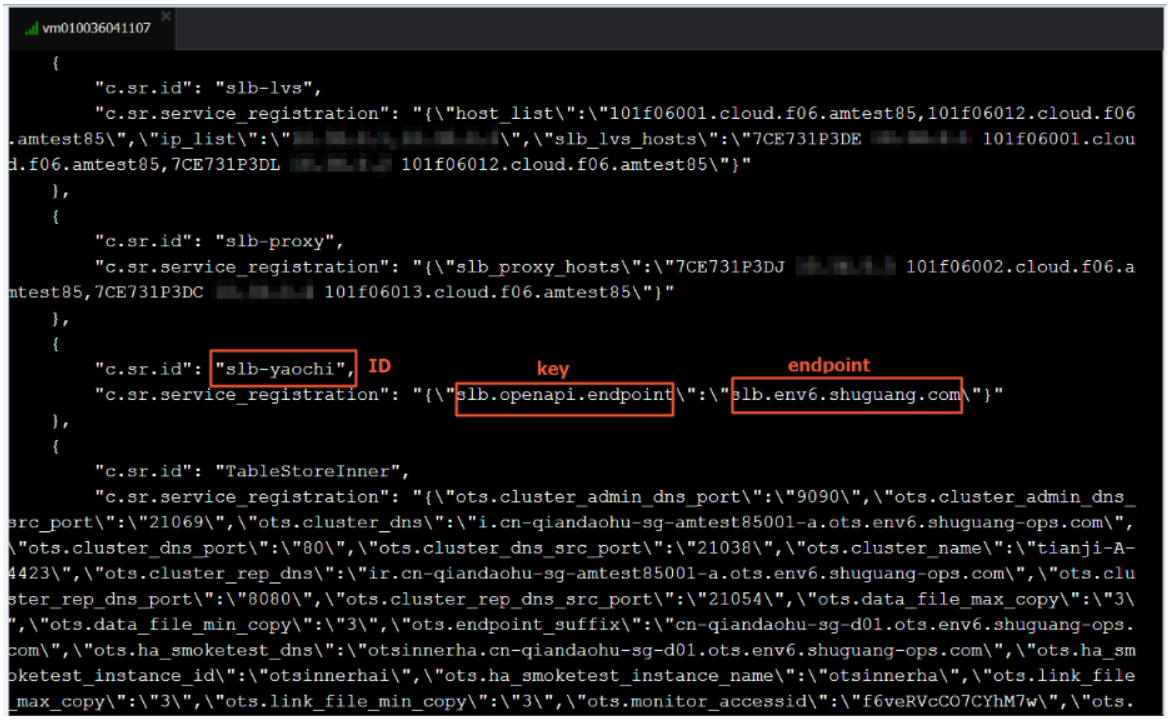
Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms > Apsara Stack Operations > Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. Choose **Operations > Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the command **curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration"** to obtain JSON data.

7. You can locate the endpoint of the SLB instance based on the SLB product ID (slb-yaochi) and the key value (slb.openapi.endpoint).




```
{
    "c.sr.id": "slb-lvs",
    "c.sr.service_registration": "{\"host_list\":\"101f06001.cloud.f06.amtest85,101f06012.cloud.f06
.amtest85\",\"ip_list\":\"[redacted]\",\"slb_lvs_hosts\":\"7CE731P3DE [redacted] 101f06001.clou
d.f06.amtest85,7CE731P3DL [redacted] 101f06012.cloud.f06.amtest85\"}"
},
{
    "c.sr.id": "slb-proxy",
    "c.sr.service_registration": "{\"slb_proxy_hosts\":\"7CE731P3DJ [redacted] 101f06002.cloud.f06.a
mtest85,7CE731P3DC [redacted] 101f06013.cloud.f06.amtest85\"}"
},
{
    "c.sr.id": "slb-yaochi",
    "c.sr.service_registration": "{\"slb.openapi.endpoint\":\"slb.env6.shuguang.com\"}"
},
{
    "c.sr.id": "TableStoreInner",
    "c.sr.service_registration": "{\"ots.cluster_admin_dns_port\":\"9090\",\"ots.cluster_admin_dns_
src_port\":\"21069\",\"ots.cluster_dns\":\"i.cn-qiandaohu-sg-amtest85001-a.ots.env6.shuguang-ops.com\",
\"ots.cluster_dns_port\":\"80\",\"ots.cluster_dns_src_port\":\"21030\",\"ots.cluster_name\":\"tianji-A-
4423\",\"ots.cluster_rep_dns\":\"ir.cn-qiandaohu-sg-amtest85001-a.ots.env6.shuguang-ops.com\",\"ots.clu
ster_rep_dns_port\":\"8080\",\"ots.cluster_rep_dns_src_port\":\"21054\",\"ots.data_file_max_copy\":\"3\
",\"ots.data_file_min_copy\":\"3\",\"ots.endpoint_suffix\":\"cn-qiandaohu-sg-d01.ots.env6.shuguang-ops.
com\",\"ots.ha_smoketest_dns\":\"otsinnerha.cn-qiandaohu-sg-d01.ots.env6.shuguang-ops.com\",\"ots.ha_sm
oketest_instance_id\":\"otsinnerhai\",\"ots.ha_smoketest_instance_name\":\"otsinnerha\",\"ots.link_file
_max_copy\":\"3\",\"ots.link_file_min_copy\":\"3\",\"ots.monitor_accessid\":\"f6veRVcCO7CYhM7w\",\"ots.
```


2.13.1.7. SLB instance

2.13.1.7.1. CreateLoadBalancer

You can call this operation to create an SLB instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *CreateLoadBalancer*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerName	String	No	The name of the SLB instance. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-).

Parameter	Type	Required	Description
AddressType	String	No	The network type of the SLB instance. Valid values: • *internet*: After an Internet SLB instance is created, the system allocates a public IP address to it so that the instance can forward requests from the Internet. • *intranet*: After an intranet SLB instance is created, the system allocates a private IP address to it so that the instance can only forward intranet requests.
VSwitchId	String	No	The ID of the VSwitch to which the intranet SLB instance belongs. Note When this parameter is specified, the AddressType parameter is automatically set to *intranet*.
ClientToken	String	No	The client token that is used to guarantee the idempotency of the request. The value of this parameter is generated by the client and must be unique among different requests. The maximum length is 64 ASCII characters.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
LoadBalancerId	String	The ID of the SLB instance.
Address	String	The IP address of the SLB instance.
VpcId	String	The ID of the VPC to which the SLB instance belongs.
VSwitchId	String	The ID of the VSwitch to which the SLB instance belongs.
LoadBalancerName	String	The name of the SLB instance.

Examples

Sample requests

```
https://slb.example.com/
&Action=CreateLoadBalancer
&RegionId=cn-east-hangzhou-01
&LoadBalancerName=abc**
&AddressType=internet
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CreateLoadBalancerResponse>
   <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
   <LoadBalancerId>139a0*****</LoadBalancerId>
   <Address>42. **. **. **</Address>
   <NetworkType>classic<NetworkType>
   <LoadBalancerName>abc</LoadBalancerName>
</CreateLoadBalancerResponse>
```

- JSON format

```
{
  "RequestId":"365F4154-92F6-4AE4-92F8-7FF34B540710",
  "LoadBalancerId":"139a00******,
  "Address":"42. **. **. **",
  "NetworkType":"classic",
  "LoadBalancerName":"abc*****"
}
```

2.13.1.7.2. DeleteLoadBalancer

You can call this operation to delete an SLB instance.

> **Note** The listeners and tags configured for the SLB instance will also be deleted.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DeleteLoadBalancer*.

Parameter	Type	Required	Description
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/
&Action=DeleteLoadBalancer
&LoadBalancerId=lb-t4nj5vuz8******
&RegionId=ap-southeast-1
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteLoadBalancerResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</DeleteLoadBalancerResponse>
```

- JSON format

```
{
 "RequestId": " CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.13.1.7.3. SetLoadBalancerStatus

You can call this operation to set the status of an SLB instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *SetLoadBalancerStatus*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.
LoadBalancerStatus	String	Yes	The status of the SLB instance. Valid values: • *active* When an SLB instance is in the *active* state, listeners in the instance forward the received traffic based on rules. By default, an SLB instance is in the *active* state after it is created. • *inactive* When an SLB instance is in the *inactive* state, listeners in the SLB instance do not forward the received traffic. Note If all listeners in an SLB instance are deleted, the SLB instance automatically enters the *inactive* state.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/
&Action=SetLoadBalancerStatus
&LoadBalancerId=lb-t4nj5vu******
&LoadBalancerStatus=active
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<SetLoadBalancerStatusResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</SetLoadBalancerStatusResponse>
```

- JSON format

```
{
 "RequestId": " CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.13.1.7.4. SetLoadBalancerName

You can call this operation to modify the name of an SLB instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *SetLoadBalancerName*.
RegionId	String	No	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.
LoadBalancerName	String	Yes	The name of the SLB instance. The name must be 2 to 128 characters in length. It must start with a letter and can contain letters, digits, periods (.), underscores (_), and hyphens (-).

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/
&Action=SetLoadBalancerName
&LoadBalancerId=lb-t4nj5vuz8*****
&LoadBalancerName=abc
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<SetLoadBalancerNameResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</SetLoadBalancerNameResponse>
```

- JSON format

```
{
 "RequestId": " CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.13.1.7.5. DescribeLoadBalancers

You can call this operation to query created SLB instances.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeLoadBalancers*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	No	The ID of the SLB instance. A maximum of 10 IDs can be queried each time. The entered values must be separated with commas (,).
LoadBalancerName	String	No	The name of the SLB instance. A maximum of 10 names can be queried each time. The entered values must be separated with commas (,).

Parameter	Type	Required	Description
AddressType	String	No	The network type of the SLB instance. Valid values: *intranet* | *internet*
NetworkType	String	No	The network type of the intranet SLB instance. Valid values: • *vpc* • *classic*
VpcId	String	No	The ID of the VPC to which the SLB instance belongs.
VswitchId	String	No	The ID of the VSwitch to which the SLB instance belongs.
Address	String	No	The IP address of the SLB instance.
ServerIntranet Address	String	No	The internal IP address of the attached back-end server. Multiple IP addresses can be queried each time. The entered values must be separated with commas (,).
ServerId	String	No	The ID of the attached back-end server.
MasterZoneId	String	No	The ID of the primary zone where the SLB instance resides.
SlaveZoneId	String	No	The ID of the secondary zone where the SLB instance resides.
Tags	JSON string	No	The tags bound to the SLB instance to query. A maximum of 10 tags can be specified.
tags elements			
TagKey	String	No	The key of the tag bound to the SLB instance to query. Note If you set the Tags parameter, you must also set this parameter.
TagValue	String	No	The key value of the tag bound to the SLB instance to query. The value cannot start with `aliyun`. Note If you set the Tags parameter, you must also set this parameter.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
LoadBalancers	JSON string	The list of SLB instances that were queried.
LoadBalancer elements		
LoadBalancerId	String	The ID of the SLB instance.
LoadBalancerName	String	The name of the SLB instance.
LoadBalancerStatus	String	The status of the SLB instance. • *inactive*: The listeners of the SLB instance in the inactive state do not forward traffic. • *active*: After the SLB instance is created, it is in the *active* state by default. • *locked*: The SLB instance is locked.
Address	String	The IP address of the SLB instance.
RegionId	String	The ID of the region where the SLB instance resides.
RegionIdAlias	String	The alias of the region to which the SLB instance belongs.
AddressType	String	The network type of the SLB instance.
VSwitchId	String	The ID of the VSwitch to which the intranet SLB instance belongs.
VpcId	String	The ID of the VPC to which the intranet SLB instance belongs.
NetworkType	String	The network type of the intranet SLB instance. Valid values: • *vpc* • *classic*
CreateTime	String	The time when the SLB instance was created.
CreateTimeStamp	Integer	The timestamp generated when the SLB instance was created.
MasterZoneId	String	The ID of the primary zone where the SLB instance resides.
SlaveZoneId	String	The ID of the secondary zone where the SLB instance resides.

Examples

Sample requests

```
https://slb.example.com/
&Action=DescribeLoadBalancers
&RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeLoadBalancersResponse>
  <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
  <LoadBalancers>
    <LoadBalancer>
      <LoadBalancerId>139a0*****</LoadBalancerId>
      <LoadBalancerName>abc</LoadBalancerName>
      <Address>100. **. **. **</Address>
      <AddressType>intranet</AddressType>
      <RegionId>cn-east-hangzhou-01</RegionId>
      <VSwitchId>vsw-25*******</VSwitchId>
      <VpcId>vpc-25*****</VpcId>
      <NetworkType>vpc</NetworkType>
      <LoadBalancerStatus>active</LoadBalancerStatus>
      <MasterZoneId>cn-hangzhou-**</MasterZoneId>
      <SlaveZoneId>cn-hangzhou-**</SlaveZoneId>
    </LoadBalancer>
    <LoadBalancer>
      <LoadBalancerId>282******</LoadBalancerId>
      <LoadBalancerName>def</LoadBalancerName>
      <Address>100. **. **. **</Address>
      <AddressType>intranet</AddressType>
      <RegionId>cn-east-hangzhou-01</RegionId>
      <VSwitchId>vsw-255ec****</VSwitchId>
      <VpcId>vpc-25dv****</VpcId>
      <NetworkType>vpc</NetworkType>
      <LoadBalancerStatus>active</LoadBalancerStatus>
      <MasterZoneId>cn-hangzhou-**</MasterZoneId>
      <SlaveZoneId>cn-hangzhou-**</SlaveZoneId>
    </LoadBalancer>
  </LoadBalancers>
</DescribeLoadBalancersResponse>
```

- JSON format

```
{
 "RequestId": "365F4154-92F6-4AE4-92F8-7FF34B540710",
 "LoadBalancers": {
  "LoadBalancer": [
   {
    "LoadBalancerId": "139a0*****",
    "LoadBalancerName": "abc",
    "Address": "100. **. **. **",
    "AddressType": "intranet",
    "RegionId": "cn-east-hangzhou-01",
    "VSwitchId": "vsw-255e****",
    "VpcId": "vpc-25d*****",
    "NetworkType": "vpc",
    "LoadBalancerStatus ": "active",
    "MasterZoneId": "cn-hangzhou-**",
    "SlaveZoneId": "cn-hangzhou-**"
   },
   {
    "LoadBalancerId": "282b00102ac-cn-east-hangzhou-01",
    "LoadBalancerName": "def",
    "Address": "100. **. **. **",
    "AddressType": "intranet",
    "RegionId": "cn-east-hangzhou-01",
    "VSwitchId": "vsw-255******",
    "VpcId": "vpc-25dv*****",
    "NetworkType": "vpc",
    "LoadBalancerStatus ": "active",
    "MasterZoneId": "cn-hangzhou-**",
    "SlaveZoneId": "cn-hangzhou-**"
   }
  ]
 }
}
```


2.13.1.7.6. DescribeLoadBalancerAttribute

You can call this operation to query the details of a specified SLB instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeLoadBalancerAttribute*.
LoadBalancerId	String	Yes	The ID of the SLB instance.
RegionId	String	No	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
LoadBalancerId	String	The ID of the SLB instance.
RegionId	String	The ID of the region where the SLB instance resides.
RegionIdAlias	String	The alias of the region where the SLB instance resides.
LoadBalancerName	String	The name of the SLB instance.
LoadBalancerStatus	String	The status of the SLB instance. Valid values: • *inactive*: The listeners of the SLB instance in the inactive state do not forward traffic. • *active*: After the SLB instance is created, it is in the *active* state by default. • *locked*: The SLB instance is locked.
Address	String	The IP address of the SLB instance.
AddressType	String	The network type of the SLB instance.
NetworkType	String	The network type of the intranet SLB instance.
VpcId	String	The ID of the VPC to which the intranet SLB instance belongs.
VswitchId	String	The ID of the VSwitch to which the intranet SLB instance belongs.
CreateTimeStamp	Integer	The timestamp generated when the SLB instance was created.
CreateTime	String	The time when the SLB instance was created.

Parameter	Type	Description
ListenerPorts	JSON string	The list of front-end port numbers used by the SLB instance.
ListenerPortsAndProtocol	JSON string	The list of front-end port numbers and protocols used by the SLB instance.
BackendServers	JSON string	The list of back-end servers for the SLB instance.
MasterZoneId	String	The ID of the primary zone to which the SLB instance belongs.
SlaveZoneId	String	The ID of the secondary zone to which the SLB instance belongs.
ListenerPortsAndProtocol elements		
ListenerPort	String	The front-end port number used by the SLB instance.
ListenerProtocol	Integer	The front-end listener protocol used by the SLB instance.
BackendServers elements		
ServerId	String	The ID of the ECS instance.
Weight	Integer	The weight of the back-end server.

Examples

Sample requests

```
https://slb.example.com/
&Action=DescribeLoadBalancerAttribute
&LoadBalancerId=lb-t4nj5vuz8ish9emfk1f20
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeLoadBalancerAttributeResponse>
  <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
  <LoadBalancerId>139a0*****</LoadBalancerId>
  <RegionId>cn-east-hangzhou-01</RegionId>
  <LoadBalancerName>abc**</LoadBalancerName>
  <LoadBalancerStatus>active</LoadBalancerStatus>
  <Address>42. **. **. **</Address>
  <AddressType>internet</AddressType>
  <InternetChargeType>paybybandwidth</InternetChargeType>
  <Bandwidth>5</Bandwidth>
  <CreateTime>2014-01-01 00:00:00</CreateTime>
  <ListenerPorts>
    <ListenerPort>80</ListenerPort>
    <ListenerPort>443</ListenerPort>
  </ListenerPorts>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-**</ServerId>
      <Weight>100</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-**</ServerId>
      <Weight>90</Weight>
    </BackendServer>
  </BackendServers>
  <MasterZoneId>cn-hangzhou-**</MasterZoneId>
  <SlaveZoneId>cn-hangzhou-**</SlaveZoneId>
</DescribeLoadBalancerAttributeResponse>
```

- JSON format

```
{
 "RequestId": "365F4154-92F6-4AE4-92F8-7FF34B540710",
 "LoadBalancerId": "139a0060****",
 "RegionId": "cn-east-hangzhou-01",
 "LoadBalancerName": "abc**",
 "LoadBalancerStatus ": "active",
 "Address": "42. **. **. **",
 "AddressType": "internet",
 "InternetChargeType": "paybybandwidth",
 "Bandwidth": "5",
 "CreateTime": "2014-01-01 00:00:00",
 "ListenerPorts": {
  "ListenerPort": [
   80,
   443
  ]
 },
 "BackendServers": {
  "BackendServer": [
   {
    "ServerId": "vm-**",
    "Weight": 100
   },
   {
    "ServerId": "vm-**",
    "Weight": 90
   }
  ]
 },
 "MasterZoneId": "cn-hangzhou-**",
 "SlaveZoneId": "cn-hangzhou-**"
}
```


2.13.1.7.7. DescribeRegions

This topic describes how to query available regions.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeRegions*.

Response parameters

Name	Type	Description
RequestId	string	The request ID.
Regions	JSON string	The list of regions.
Region elements		
RegionId	String	The region ID.
LocalName	String	The region name.

Examples

Sample requests

```
https://slb.example.com/
&Action=DescribeRegions
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeRegionsResponse>
  <RequestId>1651FBB6-4FBF-49FF-A9F5-DF5D696C7EC6</RequestId>
  <Regions>
    <Region>
      <RegionId>cn-east-hangzhou-01</RegionId>
      <LocalName>Hangzhou</LocalName>
    </Region>
    <Region>
      <RegionId>cn-beijing</RegionId>
      <LocalName>Beijing</LocalName>
    </Region>
  </Regions>
</DescribeRegionsResponse>
```

- JSON format

```
{
 "RequestId": "1651FBB6-4FBF-49FF-A9F5-DF5D696C7EC6",
 "Regions": {
  "Region": [
   {
    "RegionId": "cn-hangzhou",
    "LocalName": "Qingdao"
   },
   {
    "RegionId": "cn-beijing"
    "LocalName": "Beijing"
   }
  ]
 }
}
```

2.13.1.7.8. DescribeZones

This topic describes how to query the zone information in a specified region.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeZones*.
RegionId	String	Yes	The ID of the region.

Response parameters

Name	Type	Description
RequestId	String	The request ID.
Zones	JSON string	The list of zones.
Zone elements		
ZoneId	String	The zone ID.
LocalName	String	The name of the zone.
SlaveZones	JSON string	The list of secondary zones.

Name	Type	Description
SlaveZone elements		
ZoneId	String	The ID of the secondary zone.
LocalName	String	The name of the secondary zone.

Examples

Sample requests

```
https://slb.example.com/
&Action=DescribeZones
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<RequestId>A48D35FF-440A-4BC0-A4A2-A9BF69B7E43A</RequestId>
<Zones>
  <Zone>
    <SlaveZones></SlaveZones>
    <ZoneId>cn-beijing-b</ZoneId>
    <LocalName>Beijing Zone B</LocalName>
  </Zone>
</Zones>
```

- JSON format

```
{
 "RequestId": "1FF3C0EC-588C-4872-8F86-8D88A652D1E4",
 "Zones": {
  "Zone": [
   {
    "ZoneId": "cn-beijing-b",
    "LocalName": "Beijing Zone B",
    "SlaveZones": {
     "SlaveZone": []
    }
   }
  ]
 }
}
```


2.13.1.8. Listener

2.13.1.8.1. TCP listener

2.13.1.8.2. UDP listener

2.13.1.8.3. HTTP listener

2.13.1.8.4. HTTPS listener

2.13.1.8.5. Access control

2.13.1.8.6. Forwarding rules

2.13.1.8.7. DeleteLoadBalancerListener

You can call this operation to delete a listener.

> **Note** A listener can be deleted only when it is in the stopped or running state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DeleteLoadBalancerListener*.

Parameter	Type	Required	Description
LoadBalancerId	String	Yes	The ID of the SLB instance. You can call the DescribeRegions operation to obtain the region ID.
ListenerPort	Integer	Yes	The front-end port number used by the SLB instance. Valid values: 1 to 65535

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=DeleteLoadBalancerListener
&LoadBalancerId=lb-t4nj5vuz8ish9e*****
&ListenerPort=80
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteLoadBalancerListenerResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</DeleteLoadBalancerListenerResponse>
```

- JSON format

```
{
 "RequestId": " CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.13.1.8.8. StartLoadBalancerListener

You can call this operation to enable a listener.

> **Note**
>
> When you call this operation, note the following items:
>
> - You can call the operation only when the listener is in the stopped state.
> - After the operation is called, the listener enters the starting state.
> - You cannot call the operation when the SLB instance to which the listener belongs is in the locked state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *StartLoadBalancerListener*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.
ListenerPort	Integer	Yes	The front-end port number used by the SLB instance. Valid values: 1 to 65535

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action= StartLoadBalancerListener
&LoadBalancerId=lb-t4nj5vuz8ish9*****8
&ListenerPort=80
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<StartLoadBalancerListenerResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</StartLoadBalancerListenerResponse>
```

- JSON format

```
{
 "RequestId": " CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.13.1.8.9. StopLoadBalancerListener

You can call this operation to stop a listener.

> **Note**
>
> When you call this operation, note the following items:
>
> - After the operation is called, the listener enters the stopped state.
> - You cannot call the operation when the SLB instance to which the listener belongs is in the locked state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *StopLoadBalancerListener*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.
ListenerPort	Integer	Yes	The front-end port number used by the SLB instance. Valid values: 1 to 65535

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action= StopLoadBalancerListener
&LoadBalancerId=lb-t4nj5vuz8ish9*****8
&ListenerPort=80
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<StopLoadBalancerListenerResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</StopLoadBalancerListenerResponse>
```

- JSON format

```
{
 "RequestId": " CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.13.1.9. Server certificate

2.13.1.9.1. UploadServerCertificate

You can call this operation to upload a server certificate.

Only one server certificate and a corresponding private key can be uploaded at a time. This API operation is transactional. Either both the certificate and the private key are uploaded, or neither are uploaded. After the certificate and the private key are uploaded, the fingerprints of all server certificates for your account are returned.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *UploadServerCertificate*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
ServerCertificate	String	No	The server certificate that you want to upload.
ServerCertificate Name	String	No	The name of the server certificate that you want to upload.

Parameter	Type	Required	Description
PrivateKey	String	Yes	The private key that you want to upload.
ResourceGroupId	String	No	The ID of the enterprise resource group.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
ServerCertificateId	String	The ID of the server certificate.
ServerCertificateName	String	The name of the server certificate.
Fingerprint	String	The fingerprint of the server certificate.

Examples

Sample requests

```
https://slb.example.com/?Action=UploadServerCertificate
&RegionId=cn-hangzhou-01
&ServerCertificate=test
&ServerCertificateName=mycert01
&PrivateKey=wmsa*****
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<UploadServerCertificateResponse>
   <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
   <ServerCertificateId>idkp-123-cn-******-01</ServerCertificateId>
   <ServerCertificateName>mycert01</ServerCertificateName>
   <Fingerprint>01:DF:AB:CD</Fingerprint>
</UploadServerCertificateResponse>
```

- JSON format

```
{
  "RequestId":"365F4154-92F6-4AE4-92F8-7FF34B540710",
  "ServerCertificateId":"idkp-123-cn-****-01",
  "ServerCertificateName":"mycert01",
  "Fingerprint":"01:DF:AB:CD"
}
```

2.13.1.9.2. DeleteServerCertificate

You can call this operation to delete a server certificate.

> **Note** You cannot delete a certificate that is in use.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DeleteServerCertificate*.
RegionId	String	No	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
ServerCertificateId	String	Yes	The ID of the server certificate.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=DeleteServerCertificate
&RegionId=cn-hangzhou
&ServerCertificateId=idkp-123-cn-****-01
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteServerCertificateResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</DeleteServerCertificateResponse>
```

- JSON format

```
{
    "RequestId":" CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
 }
```

2.13.1.9.3. DescribeServerCertificates

You can call this operation to query uploaded server certificates.

Note To guarantee certificate security, only the fingerprint and name of the certificate are returned.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeServerCertificates*.
RegionId	String	No	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
ServerCertificateId	String	No	The ID of the server certificate.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
ServerCertificates	JSON string	The list of the server certificates.
ServerCertificate elements		
ServerCertificateId	String	The ID of the server certificate.
ServerCertificateName	String	The name of the server certificate.
RegionId	String	The region of the server certificate.

Parameter	Type	Description
Fingerprint	String	The fingerprint of the server certificate.
CreateTime	String	The time when the server certificate was uploaded.
CreateTimeStamp	Long	The timestamp generated when the server certificate was uploaded.

Examples

Sample requests

```
https://slb.example.com/?Action=DescribeServerCertificates
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeServerCertificatesResponse>
  <RequestId>9F8232CD-29B5-4A21-86C5-4154D5F6A578</RequestId>
  <ServerCertificates>
    <ServerCertificate>
        <AliCloudCertificateId />
        <AliCloudCertificateName />
        <CreateTime>2018-03-14T09:15:21Z</CreateTime>
        <CreateTimeStamp>1521018921000</CreateTimeStamp>
        <Fingerprint>cd:90:1b:7b:49:4d:1d:90:f6:01:de:9a:81:7d:31:a7:38:1d:84:8d</Fingerprint>
        <IsAliCloudCertificate>0</IsAliCloudCertificate>
        <RegionId>cn-hangzhou</RegionId>
        <RegionIdAlias>cn-hangzhou</RegionIdAlias>
        <ResourceGroupId>rg-acfmxaz******</ResourceGroupId>
        <ServerCertificateId>1231579085529123_16223cae1ec_2024*****_797495279</ServerCertificateId
>
        <ServerCertificateName>www.aliyuntest.club</ServerCertificateName>
    </ServerCertificate>
    <ServerCertificate>
        <AliCloudCertificateId>0</AliCloudCertificateId>
        <AliCloudCertificateName />
        <CreateTime>2016-12-13T09:57:49Z</CreateTime>
        <CreateTimeStamp>1481623069000</CreateTimeStamp>
        <Fingerprint>cd:90:1b:7b:49:4d:1d:90:f6:01:de:9a:81:7d:31:a7:38:1d:84:8d</Fingerprint>
        <IsAliCloudCertificate>0</IsAliCloudCertificate>
        <RegionId>cn-hangzhou</RegionId>
        <RegionIdAlias>cn-hangzhou</RegionIdAlias>
        <ResourceGroupId>rg-acfmxazb4p*****</ResourceGroupId>
        <ServerCertificateId>1231579085529123_158f7*****</ServerCertificateId>
        <ServerCertificateName>test_certificate</ServerCertificateName>
    </ServerCertificate>
  </ServerCertificates>
</DescribeServerCertificatesResponse>
```

- JSON format

```
{
  "RequestId":"9F8232CD-29B5-4A21-86C5-4154D5F6A578",
  "ServerCertificates":{
    "ServerCertificate":[
      {
        "CreateTimeStamp":1521018921000,
        "ServerCertificateId":"1231579085529123_16223cae1ec_2024493633_797495279",
        "RegionIdAlias":"cn-hangzhou",
        "AliCloudCertificateId":"",
        "CreateTime":"2018-03-14T09:15:21Z",
        "ResourceGroupId":"rg-acfmxazb4ph6aiy",
        "RegionId":"cn-hangzhou",
        "ServerCertificateName":"www.aliyuntest.club",
        "IsAliCloudCertificate":0,
        "AliCloudCertificateName":"",
        "Fingerprint":"cd:90:1b:7b:49:4d:1d:90:f6:01:de:9a:81:7d:31:a7:38:1d:84:8d"
      },

      {
        "CreateTimeStamp":1481623069000,
        "ServerCertificateId":"1231579085529123_158f79de306",
        "RegionIdAlias":"cn-hangzhou",
        "AliCloudCertificateId":"0",
        "CreateTime":"2016-12-13T09:57:49Z",
        "ResourceGroupId":"rg-acfmxazb4ph6aiy",
        "RegionId":"cn-hangzhou",
        "ServerCertificateName":"test_certificate",
        "IsAliCloudCertificate":0,
        "AliCloudCertificateName":"",
        "Fingerprint":"cd:90:1b:7b:49:4d:1d:90:f6:01:de:9a:81:7d:31:a7:38:1d:84:8d"
      }
    ]
  }
}
```


2.13.1.9.4. SetServerCertificateName

You can call this operation to configure a name for a server certificate.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *SetServerCertificateName*.
ServerCertificateId	String	Yes	The ID of the server certificate.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
ServerCertificateName	String	Yes	The name of the server certificate. The name must be 1 to 80 characters in length. It must start with letters. It can contain digits, periods (.), underscores (_), and hyphens (-).

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=SetServerCertificateName
&RegionId=cn-hangzhou
&ServerCertificateId=139a00604ad-cn-east-****-01
&ServerCertificateName=abc
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<SetServerCertificateNameResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FE7BA984</RequestId>
</SetServerCertificateNameResponse>
```

- JSON format

```
{
 "RequestId": " CEF72CEB-54B6-4AE8-B225-F876FE7BA984"
}
```

2.13.1.9.5. UploadCACertificate

You can call this operation to upload a CA certificate.

You can upload only one CA certificate at a time. After a certificate is uploaded, the ID, name, and fingerprint of the certificate are returned.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *UploadCACertificate*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
CACertificate	String	Yes	The CA certificate to upload.
CACertificateName	String	No	The name of the CA certificate.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CACertificateId	String	The ID of the CA certificate.
CACertificateName	String	The name of the CA certificate.
Fingerprint	String	The fingerprint of the CA certificate.
CreateTime	String	The time when the CA certificate was uploaded.
Fingerprint	Long	The timestamp generated when the CA certificate was uploaded.

Examples

Sample requests

```
https://slb.example.com/?Action=UploadCACertificate
&RegionId=cn-east-hangzhou-01
&CACertificate=test
&CACertificateName=mycacert01
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<UploadCACertificateResponse>
   <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
   <CACertificateId>idkp-234-cn-****-02</CACertificateId>
   <CACertificateName>mycacert01</CACertificateName>
   <Fingerprint>02:DF:AB:ED</Fingerprint>
</UploadCACertificateResponse>
```

- JSON format

```
{
 "RequestId":"365F4154-92F6-4AE4-92F8-7FF34B540710",
 "CACertificateId":"idkp-234-cn-****-02",
 "CACertificateName":"mycacert01",
 "Fingerprint":"02:DF:AB:ED"
}
```

2.13.1.9.6. DeleteCACertificate

You can call this operation to delete a CA certificate.

> **Note** You cannot delete a CA certificate that is in use.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DeleteCACertificate*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
CACertificateId	String	Yes	The ID of the CA certificate to delete.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=DeleteCACertificate
&RegionId=cn-hangzhou
&CACertificateId=idkp-234-cn-*****-02
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteCACertificateResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FF7BA984</RequestId>
</DeleteCACertificateResponse>
```

- JSON format

```
{
 "RequestId": " CEF72CEB-54B6-4AE8-B225-F876FF7BA984"
}
```

2.13.1.9.7. DescribeCACertificates

You can call this operation to query uploaded CA certificates.

> **Note** To guarantee certificate security, only the fingerprint and name of the certificate are returned.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeCACertificates*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
CACertificateId	String	No	The ID of the CA certificate.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Parameter	Type	Description
CACertificates	JSON string	The list of CA certificates.
CACertificate elements		
CACertificateId	String	The ID of the CA certificate.
CACertificateName	String	The name of the CA certificate.
RegionId	String	The region of the CA certificate.
Fingerprint	String	The fingerprint of the CA certificate.
ResourceGroupId	String	The ID of the resource group.
CreateTimeStamp	Long	The timestamp generated when the CA certificate was uploaded.

Examples

Sample requests

```
https://slb.example.com/?Action=DescribeCACertificates
&RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeCACertificatesResponse>
  <RequestId>6DFA147D-EE7E-4FE2-831A-9FAC41C52AFA</RequestId>
  <CACertificates>
    <CACertificate>
        <CACertificateId>1231579085529123_15c73*******_-986300114_-2110544408</CACertificateId>
        <CACertificateName>CA1</CACertificateName>
        <CreateTime>2017-06-04T16:01:58Z</CreateTime>
        <CreateTimeStamp>1496592118000</CreateTimeStamp>
        <Fingerprint>0d:f6:9e:ed:c2:6d:df:06:ac:af:82:fb:17:1b:5b:08:39:b3:d9:d0</Fingerprint>
        <RegionId>cn-hangzhou</RegionId>
        <ResourceGroupId>rg-acfmxazb4*****</ResourceGroupId>
      </CACertificate>
  </CACertificates>
</DescribeCACertificatesResponse>
```

- JSON format

```
{
  "RequestId":"6DFA147D-EE7E-4FE2-831A-9FAC41C52AFA",
  "CACertificates":{
    "CACertificate":[
      {
        "CreateTimeStamp":1496592118000,
        "CACertificateName":"CA1",
        "CreateTime":"2017-06-04T16:01:58Z",
        "ResourceGroupId":"rg-acfmxazb4*****",
        "RegionId":"cn-hangzhou",
        "CACertificateId":"1231579085529123_15c73d******_-986300114_-2110544408",
        "Fingerprint":"0d:f6:9e:ed:c2:6d:df:06:ac:af:82:fb:17:1b:5b:08:39:b3:d9:d0"
      }
    ]
  }
}
```


2.13.1.9.8. SetCACertificateName

You can call this operation to configure the name of a CA certificate.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *SetCACertificateName*.
CACertificateId	String	Yes	The ID of the CA certificate.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
CACertificateName	String	Yes	The name of the CA certificate. The name must be 1 to 80 characters in length. It must start with letters. It can contain letters, digits, periods (.), underscores (_), and hyphens (-).

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=SetCACertificateName
&CACertificateId=139a00604ad-cn-east-*****-01
&CACertificateName=mycacert02
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<SetCACertificateNameResponse>
   <RequestId>CEF72CEB-54B6-4AE8-B225-F876FE7BA984</RequestId>
</SetCACertificateNameResponse>
```

- JSON format

```
{
 "RequestId": " CEF72CEB-54B6-4AE8-B225-F876FE7BA984"
}
```

2.13.1.10. Backend server

2.13.1.10.1. AddBackendServers

You can call this operation to add back-end servers.

> **Note** If the information of multiple identical ECS instances is contained in a request, only the first ECS instance is added and the other ECS instances are ignored.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *AddBackendServers*.
LoadBalancerId	String	Yes	The ID of the SLB instance.
BackendServers	JSON string	Yes	The list of back-end servers to add. **Note** Only back-end servers in the running state can be added to the SLB instance. A maximum of 20 back-end servers can be added each time.

Parameter	Type	Required	Description
BackendServer elements			
ServerId	String	Yes	The ID of the ECS instance.
Weight	Integer	No	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
LoadBalancerId	String	The ID of the SLB instance.
BackendServers	JSON string	The list of back-end servers.
BackendServer elements		
ServerId	String	The ID of the ECS instance.
Weight	Integer	The weight of the back-end server.

Examples

Sample requests

```
https://slb.example.com/?Action=AddBackendServers
&LoadBalancerId=lb-t4nj5vuz8ish9e*****
&BackendServers=[
  {"ServerId":" vm-***","Weight":"100"},
  {"ServerId":" vm-****","Weight":"100"}]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<AddBackendServersResponse>
  <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
  <LoadBalancerId>139a00604ad-cn-east-hangzhou-01</LoadBalancerId>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Weight>100</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Weight>100</Weight>
    </BackendServer>
  </BackendServers>
</AddBackendServersResponse>
```

- JSON format

```
{
 "RequestId": "365F4154-92F6-4AE4-92F8-7FF34B540710",
 "LoadBalancerId": "139a00604ad-cn-east-****-01",
 "BackendServers": {
  "BackendServer": [
   {
    "ServerId": "vm-***",
    "Weight": 100
   },
   {
    "ServerId": "vm-***",
    "Weight": 100
   }
  ]
 }
}
```

2.13.1.10.2. RemoveBackendServers

You can call this operation to remove back-end servers.

> **Note** If the back-end servers are not included in the server list of the specified SLB instance, they cannot be deleted and no error is returned.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *RemoveBackendServers*.
RegionId	String	Yes	The ID of the region where the SLB instance resides.
LoadBalancerId	String	Yes	The ID of the SLB instance.
BackendServers	JSON string	Yes	The list of back-end servers to remove. Note Up to 20 back-end servers can be removed at a time.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
LoadBalancerId	String	The ID of the SLB instance.
BackendServers	JSON string	The list of back-end servers.

Examples

Sample requests

```
https://slb.example.com/?Action=RemoveBackendServers
&LoadBalancerId=lb-t4nj5vuz8is*****
&BackendServers=["i-bp143t8c5uralrxxxx","i-bp12zdi79965uxxxx"]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<RemoveBackendServersResponse>
  <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
  <LoadBalancerId>139a00604ad-cn-east-*****-01</LoadBalancerId>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-2**1</ServerId>
      <Weight>100</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-****</ServerId>
      <Weight>100</Weight>
    </BackendServer>
  </BackendServers>
</RemoveBackendServersResponse>
```

- JSON format

```
{
 "RequestId": "365F4154-92F6-4AE4-92F8-7FF34B540710",
 "LoadBalancerId": "139a00604ad-cn-east-*****-01",
 "BackendServers": {
  "BackendServer": [
   {
    "ServerId": "vm-***",
    "Weight": 100
   },
   {
    "ServerId": "vm-***",
    "Weight": 100
   }
  ]
 }
}
```

2.13.1.10.3. SetBackendServers

You can call this operation to set weights for back-end servers.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *SetBackendServers*.
LoadBalancerId	String	Yes	The ID of the SLB instance.
BackendServers	JSON string	Yes	The list of back-end servers to add. Note Only back-end servers in the running state can be added to the SLB instance. A maximum of 20 back-end servers can be added each time.
BackendServer elements			
ServerId	String	Yes	The ID of the ECS instance.
Weight	Integer	No	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
LoadBalancerId	String	The ID of the SLB instance.
BackendServers	JSON string	The list of back-end servers.
BackendServer elements		
ServerId	String	The ID of the ECS instance.
Weight	Integer	The weight of the back-end server.

Examples

Sample requests

```
https://slb.example.com/?Action=SetBackendServers
&LoadBalancerId=lb-t4nj5vuz8ish9emfk1f20
&BackendServers=[{"ServerId":"vm-233","Weight":"0"},{"ServerId":"vm-234","Weight":"0"}]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<SetBackendServersResponse>
  <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
  <LoadBalancerId>139a00604ad-cn-east-hangz*****hou-01</LoadBalancerId>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Weight>0</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Weight>0</Weight>
    </BackendServer>
  </BackendServers>
</SetBackendServersResponse>
```

- JSON format

```
{
 "RequestId": "365F4154-92F6-4AE4-92F8-7FF34B540710",
 "LoadBalancerId": "139a00604ad-cn-east-****-01",
 "BackendServers": {
  "BackendServer": [
   {
    "ServerId": "vm-***",
    "Weight": 0
   },
   {
    "ServerId": "vm-***",
    "Weight": 0
   }
  ]
 }
}
```

2.13.1.10.4. DescribeHealthStatus

You can call this operation to query the health status of back-end servers.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeHealthStatus*.
LoadBalancerId	String	Yes	The ID of the SLB instance.
ListenerPort	Integer	No	The front-end port number used by the SLB instance. Valid values: 1 to 65535 **Note** If you do not specify this parameter, the health status of all ports is checked.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
BackendServers	List	The list of back-end servers.
BackendServer elements		
ServerId	String	The ID of the ECS instance.
ServerHealthStatus	String	The health status of the back-end server: • *normal*: The back-end server is healthy. • *abnormal*: The back-end server is unhealthy. • *unavailable*: The health check has not been completed.

Examples

Sample requests

```
https://slb.example.com/?Action=DescribeHealthStatus
&LoadBalancerId=lb-t4nj5vuz8i******
&ListenerPort=80
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeHealthStatusResponse>
  <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <ServerHealthStatus>normal</ServerHealthStatus>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <ServerHealthStatus>abnormal</ServerHealthStatus>
    </BackendServer>
  </BackendServers>
</DescribeHealthStatusResponse>
```

- JSON format

```
{
 "RequestId": "365F4154-92F6-4AE4-92F8-7FF34B540710",
 "LoadBalancerId": "139a00604ad-cn-east-****-01",
 "BackendServers": {
  "BackendServer": [
   {
    "ServerId": "vm-***",
    "ServerHealthStatus": "normal"
   },
   {
    "ServerId": "vm-***",
    "ServerHealthStatus": "abnormal"
   }
  ]
 }
}
```

2.13.1.10.5. AddNcServers

You can call this operation to add physical back-end servers.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *AddNcServers*.

Parameter	Type	Required	Description
RegionId	String	Yes	The ID of the region where the SLB instance resides.
HostEcsInstanceId	String	Yes	The ID of an ECS instance in the VPC.
LoadBalancerId	String	Yes	The ID of the SLB instance.
BackendServers	List	Yes	The list of physical back-end servers to add. You can add a maximum of 20 physical back-end servers.
BackendServer elements			
ServerId	String	Yes	The IP address of the physical back-end server.
Weight	Integer	No	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.
Type	String	Yes	The type of the back-end server. Set the value to *nc*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=AddNcServers
&RegionId=cn-hangzhou
&LoadBalancerId=lb-bp1mbyphktev5qnfts3p4
&BackendServers=[
    {"ServerId":"192. **. **. **", "Weight":"50","Type":"nc"},
    {"ServerId":"192. **. **. **", "Weight":"50","Type":"nc"}]
&HostEcsInstanceId=i-bp1fiznm0sikg4q6****
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<AddNcServersResponse>
   <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
</AddNcServersResponse>
```

- JSON format

```
{
 "RequestId": "365F4154-92F6-4AE4-92F8-7FF34B540710"
}
```

2.13.1.10.6. RemoveNcServers

You can call this operation to delete physical back-end servers.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *RemoveNcServers*.
RegionId	String	Yes	The ID of the region where the SLB instance resides.
LoadBalancerId	String	Yes	The ID of the SLB instance.
BackendServers	List	Yes	The list of physical back-end servers to remove.
HostEcsInstanceId	String	Yes	The ID of an ECS instance in the VPC.
BackendServer elements			
ServerId	String	Yes	The IP address of the physical back-end server.
Weight	Integer	No	The weight of the physical back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.
Type	String	Yes	The type of the back-end server. Set the value to *nc*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=RemoveNcServers
&RegionId=cn-hangzhou
&LoadBalancerId=lb-bp1mbyphktev5qnfts3p4
&BackendServers=[
    {"ServerId":"192. **. **. **", "Weight":"50","Type":"nc"},
    {"ServerId":"192. **. **. **", "Weight":"50","Type":"nc"}]
&HostEcsInstanceId=i-bp1fiznm0sikg4q6xyrt
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<RemoveNcServersResponse>
  <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
</RemoveNcServersResponse>
```

- JSON format

```
{
 "RequestId": "365F4154-92F6-4AE4-92F8-7FF34B540710"
}
```

2.13.1.10.7. SetNcServers

You can call this operation to set the weight of physical back-end servers.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *SetNcServers*.
RegionId	String	Yes	The ID of the region where the SLB instance resides.
HostEcsInstanceId	String	Yes	The ID of an ECS instance in the VPC.
LoadBalancerId	String	Yes	The ID of the SLB instance.
BackendServers	List	Yes	The list of physical back-end servers.
BackendServer elements			

Parameter	Type	Required	Description
ServerId	String	Yes	The IP address of the physical back-end server.
Weight	Integer	No	The weight of the physical back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.
Type	String	Yes	The type of the back-end server. Set this parameter to *nc*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=SetNcServers
&RegionId=cn-hangzhou
&LoadBalancerId=lb-bp1mbyphktev5qnfts3p4
&BackendServers=[
    {"ServerId":"192. **. **. **", "Weight":"50","Type":"nc"},
    {"ServerId":"192. **. **. **", "Weight":"50","Type":"nc"}]
&HostEcsInstanceId=i-bp1fiznm0sikg4*****
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<SetNcServersResponse>
   <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
</SetNcServersResponse>
```

- JSON format

```
{
  "RequestId": "365F4154-92F6-4AE4-92F8-7FF34B540710"
}
```

2.13.1.11. VServer group

2.13.1.11.1. CreateVServerGroup

You can call this operation to create a VServer group and add back-end servers to the VServer group.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *CreateVServerGroup*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.
VServerGroupName	String	No	The name of the VServer group.
BackendServers	JSON string	No	The list of back-end servers. A VServer group can contain a maximum of 20 back-end servers. If you do not specify this parameter, an empty VServer group is created.
BackendServer elements			
ServerId	String	Yes	The ID of the ECS instance.
Port	Integer	Yes	The port number used by the back-end server. Valid values: 1 to 65535
Weight	Integer	Yes	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Parameter	Type	Description
VServerGroupId	String	The ID of the VServer group.
BackendServers	JSON string	The list of back-end servers.

Examples

Sample requests

```
https://slb.example.com/?Action=CreateVServerGroup
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8ish9***
&VServerGroupName=Group1
&BackendServers=[
   {"ServerId":"vm-***","Port":"80","Weight":"100"},
   {"ServerId":"vm-**","Port":"90","Weight":"100"},
   {"ServerId":"vm-***","Port":"70","Weight":"100"}
]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<CreateVServerGroupResponse>
   <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
   <VServerGroupId>rsp-cige6j***</VServerGroupId>
   <BackendServers>
      <BackendServer>
         <ServerId>vm-***</ServerId>
         <Port>80</Port>
         <Weight>100</Weight>
      </BackendServer>
      <BackendServer>
         <ServerId>vm-***</ServerId>
         <Port>90</Port>
         <Weight>100</Weight>
      </BackendServer>
      <BackendServer>
         <ServerId>vm-***</ServerId>
         <Port>70</Port>
         <Weight>100</Weight>
      </BackendServer>
   </BackendServers>
</CreateVServerGroupResponse>
```

- JSON format

```
{
 "RequestId":"9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C",
 "VServerGroupId":"rsp-cige6****",
 "BackendServers":{
 "BackendServer":[
  {"ServerId":"vm-***","Port":"80","Weight":"100"},
  {"ServerId":"vm-***","Port":"90","Weight":"100"},
  {"ServerId":"vm-***","Port":"70","Weight":"100"}
  ]
 }
}
```

2.13.1.11.2. SetVServerGroupAttribute

You can call this operation to modify a VServer group.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *SetVServerGroupAttribute*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.
VServerGroupName	String	No	The name of the VServer group.
BackendServers	JSON string	No	The list of back-end servers. A VServer group can contain a maximum of 20 back-end servers. If you do not specify this parameter, an empty VServer group is created.
BackendServer elements			
ServerId	String	Yes	The ID of the ECS instance.
Port	Integer	Yes	The port number used by the back-end server. Valid values: 1 to 65535
Weight	Integer	Yes	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
VServerGroupId	String	The ID of the VServer group.
BackendServers	JSON string	The list of back-end servers.

Examples

Sample requests

```
https://slb.example.com/?Action=SetVServerGroupAttribute
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8ish9em****
&VServerGroupName=Group1
&BackendServers=[
  {"ServerId":"vm-***","Port":"80","Weight":"100"},
  {"ServerId":"vm-***","Port":"90","Weight":"100"},
  {"ServerId":"vm-***","Port":"70","Weight":"100"}
]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<SetVServerGroupAttributeResponse>
  <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
  <VServerGroupId>rsp-cige6****</VServerGroupId>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>80</Port>
      <Weight>100</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>90</Port>
      <Weight>100</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>70</Port>
      <Weight>100</Weight>
    </BackendServer>
  </BackendServers>
</SetVServerGroupAttributeResponse>
```

- JSON format

```
{
 "RequestId":"9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C",
 "VServerGroupId":"rsp-cige6*****",
 "BackendServers":{
 "BackendServer":[
  {"ServerId":"vm-***","Port":"80","Weight":"100"},
  {"ServerId":"vm-***","Port":"90","Weight":"100"},
  {"ServerId":"vm-***","Port":"70","Weight":"100"}
  ]
 }
}
```

2.13.1.11.3. AddVServerGroupBackendServers

You can call this operation to add back-end servers to a specified VServer group.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *AddVServerGroupBackendServers*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
VServerGroupId	String	Yes	The ID of the VServer group.
BackendServers	JSON string	Yes	The list of back-end servers. A VServer group can contain a maximum of 20 back-end servers.
BackendServer elements			
ServerId	String	Yes	The ID of the ECS instance.
Port	Integer	Yes	The port number used by the back-end server. Valid values: 1 to 65535
Weight	Integer	Yes	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
VServerGroupId	String	The ID of the VServer group.
BackendServers	JSON string	The list of back-end servers.

Examples

Sample requests

```
https://slb.example.com/?Action=AddVServerGroupBackendServers
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8is*****
&VServerGroupName=Group1
&BackendServers=[
   {"ServerId":"vm-***","Port":"80","Weight":"100"},
   {"ServerId":"vm-***","Port":"90","Weight":"100"},
   {"ServerId":"vm-***","Port":"70","Weight":"100"}
]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<AddVServerGroupBackendServersResponse>
  <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
  <VServerGroupId>rsp-cige6j*****</VServerGroupId>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>80</Port>
      <Weight>100</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>90</Port>
      <Weight>100</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>70</Port>
      <Weight>100</Weight>
    </BackendServer>
  </BackendServers>
</AddVServerGroupBackendServersResponse>
```

- JSON format

```
{
 "RequestId":"9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C",
 "VServerGroupId":"rsp-cige6j5e7p",
 "BackendServers":{
 "BackendServer":[
  {"ServerId":"vm-233","Port":"80","Weight":"100"},
  {"ServerId":"vm-232","Port":"90","Weight":"100"},
  {"ServerId":"vm-231","Port":"70","Weight":"100"}
  ]
 }
}
```

2.13.1.11.4. RemoveVServerGroupBackendServers

You can call this operation to remove back-end servers from a specified VServer group.

Note If the back-end servers specified in BackendServers do not exist in the VServer group, they cannot be deleted and no error is returned.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *RemoveVServerGroupBackendServers*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
VServerGroupId	String	Yes	The ID of the VServer group.
BackendServers	JSON string	Yes	The list of back-end servers. A VServer group can contain a maximum of 20 back-end servers.
BackendServer elements			
ServerId	String	Yes	The ID of the ECS instance.
Port	Integer	Yes	The port number used by the back-end server. Valid values: 1 to 65535

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
VServerGroupId	String	The ID of the VServer group.
BackendServers	JSON string	The list of back-end servers.

Examples

Sample requests

```
https://slb.example.com/?Action=RemoveVServerGroupBackendServers
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8ish9******
&VServerGroupName=Group1
&BackendServers=[
  {"ServerId":"vm-***","Port":"80","Weight":"100"},
  {"ServerId":"vm-***","Port":"90","Weight":"100"},
]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<RemoveVServerGroupBackendServersResponse>
  <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
  <VServerGroupId>rsp-cige6j***</VServerGroupId>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>70</Port>
      <Weight>100</Weight>
    </BackendServer>
  </BackendServers>
</RemoveVServerGroupBackendServersResponse>
```

- JSON format

```
{
 "RequestId":"9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C",
 "VServerGroupId":"rsp-cige6****",
 "BackendServers":{
 "BackendServer":[
  {"ServerId":"vm-***","Port":"80","Weight":"100"},
  {"ServerId":"vm-***","Port":"90","Weight":"100"},
  {"ServerId":"vm-***","Port":"70","Weight":"100"}
  ]
 }
}
```

2.13.1.11.5. ModifyVServerGroupBackendServers

You can call this operation to replace back-end servers in a specified VServer group.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *ModifyVServerGroupBackendServers*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
VServerGroupId	String	Yes	The ID of the VServer group.
OldBackendServers	JSON string	Yes	Back-end servers to be removed.
NewBackendServers	JSON string	Yes	Back-end servers to be added. A VServer group can contain a maximum of 20 back-end servers. **Note** Make sure that the same number of back-end servers are listed in OldBackendServers and NewBackendServers.
BackendServer elements			
ServerId	String	Yes	The ID of the ECS instance.
Port	Integer	Yes	The port number used by the back-end server. Valid values: 1 to 65535
Weight	Integer	Yes	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
VServerGroupId	String	The ID of the VServer group.
BackendServers	JSON string	The list of back-end servers.

Examples

Sample requests

```
https://slb.example.com/?Action=ModifyVServerGroupBackendServers
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8ish9em*****
&VServerGroupName=Group1
&OldBackendServers=[{"ServerId":"vm-***","Port":"80","Weight":"100"},{"ServerId":"vm-***","Port":"90","W
eight":"100"},]
&NewBackendServers=[{"ServerId":"vm-***","Port":"80","Weight":"100"},{"ServerId":"vm-***","Port":"90","W
eight":"100"},]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<ModifyVServerGroupBackendServersResponse>
  <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
  <VServerGroupId>rsp-cige6j*****</VServerGroupId>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>80</Port>
      <Weight>100</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>90</Port>
      <Weight>100</Weight>
    </BackendServer>
  </BackendServers>
</ModifyVServerGroupBackendServersResponse>
```

- JSON format

```
{
 "RequestId":"9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C",
 "VServerGroupId":"rsp-cige6j****",
 "BackendServers":{
 "BackendServer":[
  {"ServerId":"vm-***","Port":"80","Weight":"100"},
  {"ServerId":"vm-***","Port":"90","Weight":"100"},
  ]
 }
}
```

2.13.1.11.6. DeleteVServerGroup

You can call this operation to delete a specified VServer group.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DeleteVServerGroup*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
VServerGroupId	String	Yes	The ID of the VServer group to be deleted. **Note** You cannot delete a VServer group that is in use.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=DeleteVServerGroup
&RegionId=cn-hangzhou
&VServerGroupId=rsp-cige6****
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<DeleteVServerGroupResponse>
   <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
</DeleteVServerGroupResponse>
```

- JSON format

```
{ "RequestId":"9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C"}
```

2.13.1.11.7. DescribeVServerGroups

You can call this operation to query all VServer groups created in a specified SLB instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeVServerGroups*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
VServerGroupId	String	The ID of the VServer group.
VServerGroupName	String	The name of the VServer group.
BackendServers	JSON string	The list of back-end servers.
BackendServer elements		
ServerId	String	The ID of the ECS instance.
Port	Integer	The port number used by the back-end server.

Parameter	Type	Description
Weight	Integer	The weight of the back-end server.

Examples

Sample requests

```
https://slb.example.com/?Action=DescribeVServerGroups
&RegionId=cn--hangzhou
&LoadBalancerId=139a0***
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<DescribeVServerGroupsResponse>
  <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
  <VServerGroupId>rsp-cige6****</VServerGroupId>
  <VServerGroupName>Group1</VServerGroupName>
  <BackendServers>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>80</Port>
      <Weight>100</Weight>
    </BackendServer>
    <BackendServer>
      <ServerId>vm-***</ServerId>
      <Port>90</Port>
      <Weight>100</Weight>
    </BackendServer>
  </BackendServers>
</DescribeVServerGroupsResponse>
```

- JSON format

```
{
 "RequestId": "9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C",
 "VServerGroupId": "rsp-cige6j****",
 "VServerGroupName": "Group1",
 "BackendServers": {
  "BackendServer": [
   {
    "ServerId": "vm-***",
    "Port": "80",
    "Weight": "100"
   },
   {
    "ServerId": "vm-***",
    "Port": "90",
    "Weight": "100"
   }
  ]
 }
}
```


2.13.1.11.8. DescribeVServerGroupAttribute

You can call this operation to query the details of a VServer group.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeVServerGroupAttribute*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	No	The ID of the SLB instance.
ListenerPort	String	No	The front-end port number used by the SLB instance. Valid values: 1 to 65535

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
VServerGroupId	String	The ID of the VServer group.
VServerGroupName	String	The name of the VServer group.
BackendServers	JSON string	The list of back-end servers.
BackendServers elements		
ServerId	String	The ID of the ECS instance.
Port	Integer	The port number used by the back-end server.
Weight	Integer	The weight of the back-end server.

Examples

Sample requests

```
https://slb.example.com/?Action=DescribeVServerGroupAttribute
&RegionId=cn-hangzhou
&VServerGroupId=rsp-cige6j5e7p
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<DescribeVServerGroupAttributeResponse>
   <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
   <VServerGroupId>rsp-cige6*****</VServerGroupId>
   <VServerGroupName>Group1</VServerGroupName>
   <BackendServers>
      <BackendServer>
         <ServerId>vm-***</ServerId>
         <Port>80</Port>
         <Weight>100</Weight>
      </BackendServer>
      <BackendServer>
         <ServerId>vm-***</ServerId>
         <Port>90</Port>
         <Weight>100</Weight>
      </BackendServer>
   </BackendServers>
</DescribeVServerGroupAttributeResponse>
```

- JSON format

```
{
 "RequestId": "9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C",
 "VServerGroupId": "rsp-cige6****",
 "VServerGroupName": "Group1",
 "BackendServers": {
  "BackendServer": [
   {
    "ServerId": "vm-***",
    "Port": "80",
    "Weight": "100"
   },
   {
    "ServerId": "vm-***",
    "Port": "90",
    "Weight": "100"
   }
  ]
 }
}
```

2.13.1.12. Primary/secondary VServer group

2.13.1.12.1. CreateMasterSlaveServerGroup

You can call this operation to create a primary/secondary server group. A primary/secondary server group contains only two back-end servers: a primary back-end server and a secondary back-end server.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *CreateMasterSlaveServerGroup*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.
MasterSlaveServerGroupName	String	No	The name of the primary/secondary server group.
MasterSlaveBackendServers	JSON string	No	The list of back-end servers in the primary/secondary server group. A primary/secondary server group can contain a maximum of two back-end servers. If you do not specify this parameter, an empty primary/secondary server group is created.
ServerId	String	Yes	The ID of the ECS instance.
Port	String	Yes	The port number used by the back-end server. Valid values: *1 to 65535*
Weight	String	Yes	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.
ServerType	String	Yes	The role of the back-end server. Default value: Master. Valid values: *Master and Slave*

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
MasterSlaveServerGroupId	String	The ID of the primary/secondary server group.
MasterSlaveBackendServers	JSON string	The list of back-end servers in the primary/secondary server group.
MasterSlaveBackendServer elements		
ServerId	String	The ID of the ECS instance.
Port	String	The port number used by the back-end server. Valid values: 1 to 65535
Weight	String	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to the back-end server.
ServerType	String	The role of the back-end server. Default value: Master. Valid values: *Master and Slave*

Examples

Sample requests

```
https://slb.example.com/?Action=CreateMasterSlaveServerGroup
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8ish9emf*****
&MasterSlaveServerGroupName=Group1
&MasterSlaveBackendServers=[
   {"ServerId":"vm-***","Port":"80","Weight":"100","ServerType":"Master"},
   {"ServerId":"vm-***","Port":"90","Weight":"100","ServerType":"Slave"},
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<CreateMasterSlaveServerGroupResponse>
 <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
 <MasterSlaveServerGroupId>rsp-cige6*****</MasterSlaveServerGroupId>
 <MasterSlaveBackendServers>
   <MasterSlaveBackendServers>
     <ServerId>vm-***</ServerId>
     <Port>80</Port>
     <Weight>100</Weight>
     <ServerType>Master</ServerType>
   </MasterSlaveBackendServers>
   <MasterSlaveBackendServers>
     <ServerId>vm-***</ServerId>
     <Port>90</Port>
     <Weight>100</Weight>
     <ServerType>Slave</ServerType>
   </MasterSlaveBackendServers>
 </MasterSlaveBackendServers>
</CreateMasterSlaveServerGroupResponse>
```

- JSON format

```
{
 "RequestId":"9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C",
 "MasterSlaveServerGroupId":"rsp-cige6j****",
 "MasterSlaveBackendServers":{
   "MasterSlaveBackendServers":[
    {"ServerId":"vm-***","Port":"80","Weight":"100","ServerType":"Master"},
    {"ServerId":"vm-***","Port":"90","Weight":"100","ServerType":"Slave"},
   ]
  }
}
```

2.13.1.12.2. DeleteMasterSlaveServerGroup

You can call this operation to delete a specified primary/secondary server group.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DeleteMasterSlaveServerGroup*.

Parameter	Type	Required	Description
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
MasterSlaveServerGroupId	String	Yes	The ID of the primary/secondary server group to delete. Note You cannot delete a primary/secondary server group that is in use.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=DeleteMasterSlaveServerGroup
&RegionId=cn-hangzhou
&MasterSlaveServerGroupId=rsp-cige6j*****
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<DeleteMasterSlaveServerGroupResponse>
   <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
</DeleteMasterSlaveServerGroupResponse>
```

- JSON format

```
{ "RequestId":"9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C"}
```

2.13.1.12.3. DescribeMasterSlaveServerGroupAttribute

You can call this operation to query the details of a primary/secondary server group.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeMasterSlaveServerGroupAttribute*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
MasterSlaveServerGroupId	String	Yes	The ID of the primary/secondary server group to query.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
MasterSlaveServerGroupId	String	The ID of the primary/secondary server group.
MasterSlaveBackendServers	JSON string	The list of back-end servers in the primary/secondary server group.
MasterSlaveBackendServer elements		
ServerId	String	The ID of the ECS instance.
Port	String	The port number used by the back-end server. Valid values: 1 to 65535
Weight	String	The weight of the back-end server. Valid values: [0,100]. The default value is *100*. If the value is *0*, no requests are forwarded to this back-end server.
ServerType	String	The role of the back-end server. Default value: Master. Valid values: *Master and Slave*

Examples

Sample requests

```
https://slb.example.com/?Action=DescribeMasterSlaveServerGroupAttribute
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8ish9e*****
&MasterSlaveServerGroupName=Group1
&MasterSlaveBackendServers=[
   {"ServerId":"vm-***","Port":"80","Weight":"100","ServerType":"Master"},
   {"ServerId":"vm-***","Port":"90","Weight":"100","ServerType":"Slave"},
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<DescribeMasterSlaveServerGroupAttributeResponse>
 <RequestId>9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C</RequestId>
 <MasterSlaveServerGroupId>rsp-cige6j****</MasterSlaveServerGroupId>
 <MasterSlaveBackendServers>
    <MasterSlaveBackendServers>
       <ServerId>vm-***</ServerId>
       <Port>80</Port>
       <Weight>100</Weight>
       <ServerType>Master</ServerType>
    </MasterSlaveBackendServers>
    <MasterSlaveBackendServers>
       <ServerId>vm-***</ServerId>
       <Port>90</Port>
       <Weight>100</Weight>
       <ServerType>Slave</ServerType>
    </MasterSlaveBackendServers>
 </MasterSlaveBackendServers>
</DescribeMasterSlaveServerGroupAttributeResponse>
```

- JSON format

```
{
 "RequestId":"9DEC9C28-AB05-4DDF-9A78-6B08EC9CE18C",
 "MasterSlaveServerGroupId":"rsp-cige6j5e7p",
 "MasterSlaveBackendServers":{
    "MasterSlaveBackendServers":[
     {"ServerId":"vm-233","Port":"80","Weight":"100","ServerType":"Master"},
     {"ServerId":"vm-232","Port":"90","Weight":"100","ServerType":"Slave"},
    ]
  }
}
```


2.13.1.12.4. DescribeMasterSlaveServerGroups

You can call this operation to query primary/secondary server groups you have created.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeMasterSlaveServerGroups*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerId	String	Yes	The ID of the SLB instance.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
MasterSlaveServerGroupId	String	The ID of the primary/secondary server group.
MasterSlaveServerGroupName	String	The name of the primary/secondary server group.

Examples

Sample requests

```
https://slb.example.com/?Action=DescribeMasterSlaveServerGroups
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8ish9em****
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
<DescribeMasterSlaveServerGroupsResponse>
  <RequestId>2631BB5E-B576-4925-BDED-07A66D23E5DE</RequestId>
  <MasterSlaveServerGroups>
  <MasterSlaveServerGroup>
    <MasterSlaveServerGroupId>rsp-bp1ro3****</MasterSlaveServerGroupId>
    <MasterSlaveServerGroupName>test</MasterSlaveServerGroupName>
  </MasterSlaveServerGroup>
  </MasterSlaveServerGroups>
</DescribeMasterSlaveServerGroupsResponse>
```

- JSON format

```
{
 "RequestId": "2631BB5E-B576-4925-BDED-07A66D23E5DE",
 "MasterSlaveServerGroups": {
  "MasterSlaveServerGroup": [
   {
    "MasterSlaveServerGroupId": "rsp-bp1ro3m****",
    "MasterSlaveServerGroupName": "test"
   }
  ]
 }
}
```

2.13.1.13. Tags

2.13.1.13.1. AddTags

You can call this operation to add tags to a specified SLB instance.

When you call this operation, note the following items:

- You can add up to 10 tags to an SLB instance.
- You can add a maximum of five tags at a time.
- All tags and keys added to an SLB instance must be unique.

- If you add a tag that has the same key as an existing tag but with a different value, the new tag overwrites the existing one.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *AddTags*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerID	String	Yes	The ID of the SLB instance.
Tags	JSON string	Yes	The list of tags to be added. A maximum of five tags can be specified.
Tag elements			
TagKey	String	Yes	The key value of the tag. The key value must be 1 to 64 characters in length. It cannot start with `aliyun`.
TagValue	String	No	The value of the tag. The value must be 1 to 128 characters in length. It cannot start with `aliyun`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=AddTags
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8ish9emf*****
&Tags=[
  {"TagKey":"Key1","TagValue":"Value1"}
  {"TagKey":"Key2","TagValue":"Value2"}]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<AddTagsResponse>
  <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
</AddTagsResponse>
```

- JSON format

```
{
 "RequestId":"365F4154-92F6-4AE4-92F8-7FF34B540710",
}
```

2.13.1.13.2. DescribeTags

You can call this operation to query tags you have created.

When you call this operation, note the following items:

- You can query the tags by instance ID, tag key, or tag value.
- The specified conditions are of "and" relation. Only tags meeting all specified conditions are returned.
- If you specify a tag key without specifying a tag value, all tags associated with the key are returned.
- You must also specify TagKey if you have specified TagValue.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeTags*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.

Parameter	Type	Required	Description
LoadBalancerID	String	No	The ID of the SLB instance.
Tags	JSON string	No	The list of tags to query.
PageSize	Integer	No	The number of entries to return on each page. Valid values: [1, 50]. Default value: *10*
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
Tag elements			
TagKey	String	Yes	The key value of the tag. The key value must be 1 to 64 characters in length. It cannot start with `aliyun`.
TagValue	String	No	The value of the tag. The value must be 1 to 128 characters in length. It cannot start with `aliyun`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TagSets	JSON string	The list of tags.
PageSize	Integer	The number of entries returned on each page.
PageNumber	Integer	The number of the returned page.
TotalCount	Integer	The total number of queried tags.
Tag elements		
TagKey	String	The key value of the tag.
TagValue	String	The value of the tag.
InstanceCount	Integer	The total number of instances bound to the tag.

Examples

Sample requests

```
https://slb.example.com/?Action=DescribeTags
&RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeTagsResponse>
 <RequestId>87696689-7951-4206-B30F-79D35A95C904</RequestId>
 <TotalCount>3</TotalCount>
 <PageNumber>1</PageNumber>
 <PageSize>50</PageSize>
  <TagSets>
    <TagSet>
      <InstanceCount>1</InstanceCount>
      <TagKey>Protocol</TagKey>
      <TagValue>HTTPS</TagValue>
    </TagSet>
    <TagSet>
      <InstanceCount>1</InstanceCount>
      <TagKey>network</TagKey>
      <TagValue>classic</TagValue>
    </TagSet>
    <TagSet>
      <InstanceCount>1</InstanceCount>
      <TagKey>acs_cluster</TagKey>
      <TagValue>cb2f4d713ba634931bf5851f08c073256</TagValue>
    </TagSet>
  </TagSets>
</DescribeTagsResponse>
```

- JSON format

```
{
  "PageNumber":1,
  "TotalCount":3,
  "PageSize":50,
  "RequestId":"87696689-7951-4206-B30F-79D35A95C904",
  "TagSets":{
    "TagSet":[
      {
        "InstanceCount":1,
        "TagValue":"HTTPS",
        "TagKey":"Protocol"
      },
      {
        "InstanceCount":1,
        "TagValue":"classic",
        "TagKey":"network"
      },
      {
        "InstanceCount":1,
        "TagValue":"cb2f4d713ba634931bf5851f08c0*****",
        "TagKey":"acs_cluster"
      }
    ]
  }
}
```


2.13.1.13.3. RemoveTags

You can call this operation to remove tags from a specified SLB instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *RemoveTags*.
RegionId	String	Yes	The ID of the region where the SLB instance resides. You can call the DescribeRegions operation to obtain the region ID.
LoadBalancerID	String	Yes	The ID of the SLB instance.

Parameter	Type	Required	Description
Tags	JSON string	No	The list of tags to remove.
Tag elements			
TagKey	String	Yes	The key value of the tag. It must be 1 to 64 characters in length. It cannot start with `aliyun`.
TagValue	String	No	The value of the tag. The value must be 1 to 128 characters in length. It cannot start with `aliyun`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://slb.example.com/?Action=RemoveTags
&RegionId=cn-hangzhou
&LoadBalancerId=lb-t4nj5vuz8ish9*****
&Tags=[
  {"TagKey":"Key1","TagValue":"Value1"}
  {"TagKey":"Key2","TagValue":"Value2"}]
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<RemoveTagsResponse>
  <RequestId>365F4154-92F6-4AE4-92F8-7FF34B540710</RequestId>
</RemoveTagsResponse>
```

- JSON format

```
{
 "RequestId":"365F4154-92F6-4AE4-92F8-7FF34B540710",
}
```

2.13.1.14. Error codes

Error code	Error message	HTTP status code	Description
CertificateAndPrivateKeyIsRefered	Certificate and PrivateKey Is Refered.	400	The error message returned when the certificate is already in use by other listeners.
CertificateNotMatchPrivateKey	Certificate and key does not match.	400	The error message returned when the certificate and private key do not match.
CheckedListenerNotFound	No health-checked Listener to the specified port of the Load Balancer.	404	The error message returned when the health check function has not been configured.
Forbbiden.SubUser	User not authorized to operate on the specified resource as your account is created by another user.	403	The error message returned when you do not have permission to operate the resource.
Forbidden	User not authorized to operate on the specified resource.	403	The error message returned when you do not have permission to operate the resource.
IncorrectListenerAccessControlStatusStatus	Current listener access control status does not support this operation.	500	The error message returned when the current access control status of the listener does not support this operation.

Error code	Error message	HTTP status code	Description
InternalError	The request processing has failed due to backend service exception.	400	The error message returned when an unknown internal error occurs.
InternalInvokeError	The request processing has failed due to some unknown error, exception or failure.	500	The error message returned when an unknown internal error occurs.
InvalidBackendServers.Inconsistent	Specified LoadBalancer instance's addresstype is private, so it is forbidden to add ecs vpc backendservers for now.	400	The error message returned when the network types of the backend server and the SLB instance do not match.
InvalidBackendServers.Inconsistent	All BackendServers on one Specified LoadBalancer have to be in the same vpc or all classic	400	The error message returned when the ECS instances acting as backend servers for the SLB are deployed in both a classic network and a VPC.
InvalidIdentity	The request identity was not allowed operated.	400	The error message returned when you do not have permission to operate.
InvalidLoadBalancerId.NotFound	LoadBalancerId does not exist.	404	The error message returned when the specified SLB instance does not exist.

Error code	Error message	HTTP status code	Description
InvalidParameter	The specified parameter ServerCertificate format is error.	404	The error message returned when the format of the specified certificate is incorrect.
InvalidParameter	The specified parameter ServerCertificateId is empty.	404	The error message returned when the certificate value is not specified.
InvalidParameter	The specified parameter ServerCertificateId is not supported.	404	The error message returned when the specified server certificate ID is invalid.
InvalidParameter	The specified parameter ServerCertificate or Key is empty.	404	The error message returned when the values of the certificate and the private key are not specified.
InvalidParameter	The specified parameter key format is error.	404	The error message returned when the format of the specified private key is incorrect.
InvalidParameter	Specified region is not supported.	404	The error message returned when the specified region is not supported.
InvalidParameter	Port is not Integer.	400	The error message returned when the specified port number is not an integer or is not in the range of 1 to 65535.
InvalidParameter	The specified port is not valid.	400	The error message returned when the specified port number is not an integer or is not in the range of 1 to 65535.
InvalidParameter	The specified bandwidth is not valid.	400	The error message returned when the specified instance bandwidth is invalid.

Error code	Error message	HTTP status code	Description
InvalidParameter	Specified parameter Check is not valid.	400	The error message returned when the specified parameter is invalid.
InvalidParameter	The specified parameter HealthCheckHttpCode is not valid.	400	The error message returned when the specified value of HealthCheckHttpCode is invalid.
InvalidParameter	The specified parameter bandwidth is not valid, out of the instance total bandwidth.	400	The error message returned when the specified value of Bandwidth exceeds the total bandwidth and is therefore invalid.
InvalidParameter	The specified parameter bandwidth is not valid.	400	The error message returned when the specified value of Bandwidth is invalid.
InvalidParameter	The specified parameter HealthCheck is not valid.	400	The error message returned when the specified health check parameter is invalid.
InvalidParameter	The specified parameter SourceItem is not valid.	400	The error message returned when the specified value of SourceItem is invalid.
InvalidParameter	The specified protocol is not valid.	400	The error message returned when the specified protocol type is invalid.
InvalidParameter	RS Pool is empty.	400	The error message returned when there are no available backend servers.
InvalidParameter	RS Pool doesn't exist.	400	The error message returned when there are no available backend servers.

Error code	Error message	HTTP status code	Description
InvalidParameter	Illegal user ID.	400	The error message returned when the user ID is invalid.
InvalidParameter	User ID is null	400	The error message returned when the user ID field is empty.
InvalidParameter	The specified parameter lb_type is not valid.	400	The error message returned when the SLB instance type is invalid.
InvalidParameter	The specified parameter mode is not valid..	400	The error message returned when the specified value of Mode is invalid.
InvalidParameter	The specified parameter AccessControlStatus is not valid.	400	The error message returned when the specified value of AccessControlStatus is invalid.
InvalidParameter	The specified parameter SourceItems is not valid.	400	The error message returned when the specified value of SourceItem is invalid.
InvalidParameter	The specified parameter BackendServers is not valid.	404	The error message returned when the specified value of BackendServers is invalid.
InvalidParameter	Specified parameter is not valid.	400	The error message returned when the specified parameter is invalid.
InvalidParameter	The specified parameter Domain is not valid.	400	The error message returned when the specified value of Domain is invalid.
InvalidParameter	The specified parameter URI is not valid.	400	The error message returned when the specified value of URI is invalid.

Error code	Error message	HTTP status code	Description
InvalidParameter	The specified parameter Scheduler is not valid.	400	The error message returned when the specified value of Scheduler is invalid.
InvalidParameter	The specified parameter ListenerStatus is not valid.	400	The error message returned when the specified value of ListenerStatus is invalid.
InvalidParameter	The specified parameter PersistenceTimeout is not valid.	400	The error message returned when the specified value of PersistenceTimeout is invalid.
InvalidParameter	The specified parameter ConnectPort is not valid.	400	The error message returned when the specified value of ConnectPort is invalid.
InvalidParameter	The specified parameter ConnectTimeou is not valid.	400	The error message returned when the specified value of ConnectTimeout is invalid.
InvalidParameter	The specified parameter StickySessionType is not valid.	400	The error message returned when the specified value of StickySessionType is invalid.
InvalidParameter	The specified parameter HealthyThreshold is not valid.	400	The error message returned when the specified value of HealthyThreshold is invalid.
InvalidParameter	The specified parameter UnhealthyThreshold is not valid.	400	The error message returned when the specified value of UnhealthyThreshold is invalid.

Error code	Error message	HTTP status code	Description
InvalidParameter	The specified parameter Interval is not valid.	400	The error message returned when the specified value of Interval is invalid.
InvalidParameter	The specified parameter XForwardedFor is not valid.	400	The error message returned when the specified value of XForwardedFor is invalid.
InvalidParameter	The specified parameter IsPublicAddress is not valid.	400	The error message returned when the specified value of IsPublicAddress is invalid.
InvalidRegionId.NotFound	Specified region does not exist.	404	The error message returned when the specified region does not exist.
InvalidServerId.Malformed	A specified server ID is not valid, flush control ip chain fail.	400	The error message returned when the specified backend server ID is invalid.
InvalidServerId.NotFound	The specified server is not found.	400	The error message returned when the specified backend server does not exist.
InvalidWeight.Malformed	A specified weight is not valid.	400	The error message returned when the specified value of weight is invalid.
IpNotAvailable	The specified parameter Address is not valid.	400	The error message returned when the specified value of Address is invalid.
ListenerAlreadyExists	There is already a listener bound to the port on the specified load balancer.	400	The error message returned when there is already a listener bound to the port on the specified SLB instance.

Error code	Error message	HTTP status code	Description
ListenerNotFound	No Listener to the specified port of the Load Balancer.	404	The error message returned when the specified listener does not exist.
MissingParameter	The input parameter Cookie that is mandatory for processing this request is not supplied.	400	The error message returned when the Cookie parameter is not specified.
MissingParameter	The input parameter BackendServerPort that is mandatory for processing this request is not supplied.	400	The error message returned when the BackendServerPort parameter is not specified.
MissingParameter	The input parameter LoadBalancerId that is mandatory for processing this request is not supplied.	400	The error message returned when the LoadBalancerId parameter is not specified.
MissingParameter	The input parameter RegionId that is mandatory for processing this request is not supplied.	400	The error message returned when the RegionId parameter is not specified.
MissingParameter	The combination of some parameters violates the spec.	400	The error message returned when a required parameter is not specified.

Error code	Error message	HTTP status code	Description
MissingParameter	The input parameter OwnerId,OwnerAccount that is mandatory for processing this request is not supplied.	403	The error message returned when OwnerAccount and OwnerId are not specified.
PrivateKeyEncryption	Key has Encrypted.	400	The error message returned when the private key is encrypted.
ProcessingSameRequest	The same request is being processed. Please try later.	400	The error message returned when the same request is being processed. You can try again later.
ServerCertificateId.NotFound	Specified ServerCertificateId does not exist.	404	The error message returned when the specified certificate does not exist.
ServiceUnavailable	The request has failed due to a temporary failure of the server.	503	The error message returned when the service is unavailable.
ServiceUnavailable	The specified loadbalancer name has been used.	503	The error message returned when the specified instance name is already being used.
TcpNotSupportForHybridLb	Hybrid type loadbalancer doesn't support TCP type listener.	400	The error message returned when a TCP listener cannot be created.
TooManyBackendServers	The total number of input real servers exceeds max supported number: 20.	400	The error message returned when you are trying to add more than 20 backend servers at a time.

Error code	Error message	HTTP status code	Description
TooManyBackendServers	The backend server parameter has too many entries.	400	The error message returned when the specified number of backend servers exceeds the limit.
UnsupportedOperation	The Loadbalancer doesn't support this function.	400	The error message returned when the SLB instance does not support the operation.
UnsupportedOperation	The specified action is not supported.	400	The error message returned when the specified operation is not supported.
UnsupportedOperationfixedprotocolport	The specified port has been assigned one type of protocol, and this protocol doesn't support this operation.	400	The error message returned when the specified port does not support the operation.
UnsupportedParameter	The parameter is not supported.	400	The error message returned when the input parameter is not supported.
VipNotMatchRspool	The vip protocol is not match with Rspool.	400	The error message returned when the protocol type of the listener and the application protocol of the backend server do not match.
VipTooManyListeners	The total number of input listeners exceeds max supported number: 50.	400	The error message returned when you are trying to add more than 50 listeners at a time.
InvalidParameter	The specified resource does not exist.	400	The error message returned when the specified resource does not exist.

Error code	Error message	HTTP status code	Description
ServiceUnavailable	The specified loadbalancer is configuring, please retry later.	503	The error message returned when the specified instance is currently under configuration. You can try again later.
ServiceUnavailable	Obtain Ip Fail, please make sure the ECS exists and the status is running.	503	The error message returned when the IP address cannot be obtained. Verify that the ECS instance exists and that it is in the running state.
ServiceUnavailable	The specified region not support VPC.	503	The error message returned when the specified region does not support VPCs.
InvalidParameter	The specified vpc cloud instance has been deleted.	400	The error message returned when the specified VPC instance has been deleted.

2.13.2. SDK reference

2.13.2.1. Java SDK

2.13.2.1.1. Quick start

This topic describes how to install and use Alibaba Cloud Apsara Stack SLB Java SDK.

Preparation

- To use the SLB Java SDK, you must have an Apsara Stack tenant account as well as an AccessKey. See Obtain an AccessKey pair for more information about how to obtain and view your AccessKey in the Apsara Stack console.
- Obtain the SLB endpoint. For more information, see Obtain an endpoint.
- The SLB Java SDK supports JDK V1.6 and later.

Installation

If you use Apache Maven to manage Java projects, you only need to import the JAR file to the *pom.xml* file of the project.

To use the SLB Java SDK, you must install both the SDK and the SDK core library.

The SDK core library version is 3.7.1, and the SLB Java SDK version is 1.0.

```
<dependencies>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-sdk-core</artifactId>
      <version>3.7.1</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-core-3.7.1.jar</systemPath>
    </dependency>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-ecs</artifactId>
      <version>3.5.0</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-slb-1.0.jar</systemPath>
    </dependency>
  </dependencies>
```

Usage

The following code example shows the three main steps to use the SLB Java SDK:

1. Create and initialize a DefaultAcsClient instance.
2. Create an API request and set parameters.
3. Initiate the request and handle the response or exception.

```
package com.testprogram;
 import com.aliyuncs.profile.DefaultProfile;
 import com.aliyuncs.DefaultAcsClient;
 import com.aliyuncs.IAcsClient;
 import com.aliyuncs.exceptions.ClientException;
 import com.aliyuncs.exceptions.ServerException;
 import com.aliyuncs.ecs.model.v20140526.*;
 public class Main {
    public static void main(String[] args) {
       //Create a DefaultAcsClient instance and initialize it.
       DefaultProfile profile = DefaultProfile.getProfile(
          "<your-region-id>",         // Your region ID
          "<your-access-key-id>",     // AccessKey ID of your Apsara Stack tenant account
          "<your-access-key-secret>"); // AccessKey Secret of your Apsara Stack tenant account
       // Set the service endpoint.
      profile.addEndpoint("your-region-id", "your-region-id", "product", "endpoint");
       IAcsClient client = new DefaultAcsClient(profile);
       // Create an API request and set parameters.
       DescribeInstancesRequest request = new DescribeInstancesRequest();
       request.setPageSize(10);
       // Initiate the request and handle the response or exception.
       DescribeInstancesResponse response;
       try {
          response = client.getAcsResponse(request);
          for (DescribeInstancesResponse.Instance instance:response.getInstances()) {
             System.out.println(instance.getPublicIpAddress());
          }
       } catch (ServerException e) {
          e.printStackTrace();
       } catch (ClientException e) {
          e.printStackTrace();
       }
    }
 }
```

2.13.2.1.2. Use the SDK

2.13.2.1.2.1. Install Java SDK

This topic describes how to install and use Alibaba Cloud Apsara Stack SLB Java SDK.

The SLB Java SDK supports JDK V1.6 and later. You can install the latest JDK version by importing the JAR file.

You can click here to download SLB JAR files.

If you are using Eclipse or IntelliJ as the IDE, you can install the SLB Java SDK directly by importing JAR files.

The installation methods are as follows:

- In Eclipse

  Complete the following steps to install the SLB Java SDK in Eclipse:

  i. Copy the downloaded `aliyun-java-sdk-slb.jar` file to your project folder.

  ii. Open your project in Eclipse, right-click the project, and choose **Properties** from the shortcut menu.

  iii. In the dialog box that appears, click **Java Build Path** in the left-side navigation pane and then the **Libraries** tab. Click **Add JARs** to add the downloaded JAR files.

  iv. Click **Apply and Close**.

- In IntelliJ

  Complete the following steps to install the SLB Java SDK in IntelliJ:

  i. Copy the downloaded `aliyun-java-sdk-slb.jar` file to your project folder.

  ii. Open your project in IntelliJ, and choose **File > Project Structure** .

  iii. Click **Apply** and then **OK**.

2.13.2.1.2.2. Configure identity verification credentials

When using Alibaba Cloud Apsara Stack SDK to access Apsara Stack services, you must provide your Apsara Stack tenant account for identity verification.

Currently, the SLB Java SDK supports identity verification using AccessKeys. For details on how to obtain an AccessKey, see Obtain an AccessKey pair.

If you use an AccessKey as the access credential, you must configure your credential when initializing the client.

> **Notice** Do not disclose any code containing your AccessKey (for example, do not commit the code to public GitHub projects). Otherwise, your Apsara Stack tenant account may be compromised.

```
DefaultProfile profile = DefaultProfile.getProfile(
  "<your-region-id>", // Your region ID
  "<your-access-key-id>", //  AccessKey ID of your Apsara Stack tenant account
  "<your-access-key-secret>"); // AccessKey Secret of your Apsara Stack tenant account
```

2.13.2.1.2.3. Initiate a call

This topic describes how to use the SLB Java SDK to initiate a call.

Procedure

1. Create an AcsClient instance.

```
IAcsClient client = new DefaultAcsClient(profile);
```

2. Create a request.

   The naming convention for requests is `${apiName}Request`, where ${apiName} is the API name such as *DescribeLoadBalancers*.

   When the SDKs of multiple services are used, different requests may have the same name. Differentiate the requests by SDK package.

```
DescribeLoadBalancersRequest request = new DescribeLoadBalancersRequest();
request.setPageSize(10);
```

3. Initiate a call and handle the response.

```
DescribeLoadBalancersResponse response;
try {
   response = client.getAcsResponse(request);
   for (DescribeLoadBalancersResponse.Instance instance:response.getInstances()) {
      System.out.println(instance.getPublicIpAddress());
   }
} catch (ServerException e) {
   e.printStackTrace();
} catch (ClientException e) {
   e.printStackTrace();
}
```

   In normal cases, all returned fields are deserialized into the response. You can directly call `response.getXXX()` to obtain the response fields.

```
instanceStatus := response.getStatus()
```

   If an exception occurs or you need the original HTTP response, use `doAction()` to obtain the original response.

```
HttpResponse response = client.doAction(request);
```

2.13.2.1.2.4. Handle errors

Alibaba Cloud Apsara Stack SLB Java SDK returns error messages when errors occur on the server or SDK side. The messages contain error details, including error codes and error messages.

Among the errors returned by the SLB Java SDK, you do not need to handle the SDK errors, but must solve the server errors.

- `ServerException` indicates a server error.

- `ClientException` indicates an SDK error.

For example, when the following error occurs, you can modify the AccessKey ID based on the error message to solve the problem:

```
com.aliyuncs.exceptions.ClientException: InvalidAccessKeyId.NotFound : Specified access key is not found.
```

If you want to handle the SDK errors returned by the SLB Java SDK, refer to the following example to write your code:

```
try {
    FooResponse response = client.getAcsResponse(request);
    // Handle the response.
    // ...
}catch (ServerException e){
    // You can add your own error handling logic here.
    // For example, display the error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
    // If you are unable to troubleshoot the problem, submit a ticket and provide RequestId to Alibaba Cloud technical support personnel.
    System.out.println("ResponseId=" + e.getRequestId());
}catch (ClientException e){
    // You can add your own error handling logic here.
    // For example, display the error message.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
}
```

2.13.2.1.2.5. Common errors

The following table lists some common errors you may experience when using the SDK, and describes their potential causes and solutions.

Error code	Error message	Cause	Solution

Error code	Error message	Cause	Solution
SDK.CanNotResolveEndpoint	Can not resolve endpoint, please check the user guide	The SDK cannot automatically obtain the endpoint of the called service in the specified region.	Check whether the provided region ID and endpoint are correct. After obtaining the correct endpoint, use the following code to set the endpoint: `DefaultProfile.addEndpoint("cn-hangzhou", "cn-hangzhou", "Ecs", "ecs.example.com");`
SDK.JsonUnmarshalError	Failed to unmarshal response	SDK response deserialization fails. In most cases, the cause is an inconsistency between the API metadata and the response structure received by the SDK, such as mismatched fields or an incorrect format.	You can use the `client.doAction(request)` method to obtain the original HTTP response.
SDK.TimeoutError	*The request timed out 4 times(3 for retry), perhaps we should have the threshold raised a little?*	The request times out and all retry attempts fail.	In scenarios such as poor network quality, we recommend that you prolong the timeout period or increase the maximum number of retries.
SDK.ServerError: InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The API accepts only HTTPS requests, not HTTP requests.	Add the following code before sending a request: `request.setProtocol(ProtocolType.HTTPS)`

2.13.2.2. Python SDK

2.13.2.2.1. Quick start

This topic describes how to install and use Alibaba Cloud Apsara Stack SLB Python SDK.

Preparation

- To use the SLB Python SDK, you must have an Apsara Stack tenant account as well as an Accesskey. For more information about how to obtain and view your AccessKey in the Apsara Stack console, see Obtain an AccessKey pair.
- Obtain the SLB endpoint. For more information, see Obtain an endpoint.

Installation

Complete the following steps to install the SLB Python SDK:

1. Install the SDK core library.
   - For Python V2.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core
     ```

   - For Python V3.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core-v3
     ```

2. Install the SLB Python SDK.

   An example of the command used to install the SLB Python SDK is as follows:

   ```
   pip install aliyun-python-sdk-slb
   ```

Usage

The following code example shows the three main steps to use the SLB Python SDK:

1. Create a client instance. When creating the client instance, you must specify the Region ID, AccessKey ID, and AccessKey Secret parameters.
2. Create an API request and set parameters.
3. Initiate the request and handle the response or exception.

```
#! /usr/bin/env python
#coding=utf-8

from aliyunsdkcore import client
from aliyunsdkslb.request.v20140515 import CreateLoadBalancerRequest
from aliyunsdkcore.profile import region_provider
#region_provider.modify_point('slb', '<regionId>', 'slb.<regionId>.aliyuncs.com')

clt = client.AcsClient('<AccessKey ID>','<AccessKey Secret>','Region ID')

# Set parameters.
request = CreateLoadBalancerRequest.CreateLoadBalancerRequest()
request.set_accept_format('json')




# Initiate a request.
response = clt.do_action(request)

print response
```

2.13.2.2.2. Use the SDK

2.13.2.2.2.1. Install Python SDK

This topic describes how to install and use Alibaba Cloud Apsara Stack SLB Python SDK.

The SLB Python SDK supports Python V2.6.x, V2.7.x, V3.x and later. You can install the SLB Python SDK by using one of the following methods:

- Use pip (recommended)

  Run the following commands to install the SLB Python SDK by using pip:

  ```
  pip install aliyun-python-sdk-core # Install the SDK core library.
  pip install aliyun-python-sdk-rds # Install SLB Python SDK.
  ```

  > **Note** For Python V3.x, replace `pip install aliyun-python-sdk-core` with `pip install aliyun-python-sdk-core-v3`.

- Use GitHub

  Run the following commands to install the SLB Python SDK by using GitHub:

```
git clone https://github.com/aliyun/aliyun-openapi-python-sdk.git
# Install the SDK core library.
cd aliyun-python-sdk-core
python setup.py install
# Install the SLB Python SDK.
cd aliyun-python-sdk-slb
python setup.py install
```

- Use source code
  i. Download the SDK package and decompress it.
  ii. Use one of the following methods to install the SLB Python SDK:
    - Modify sys.path to add the directory in which the SDK package is decompressed. Example:

      ```
      >>> import sys
      >>> sys.path.append('/Users/michael/my_py_scripts')
      ```

      Note This modification is in effect only when the ECS instance is running.
    - Set environment variable PYTHONPATH and add the directory in which the SDK package is decompressed. The content of this environment variable is automatically added to the module search directory.

      The method of setting PYTHONPATH is similar to that of setting environment variable Path.
    - Place the decompressed SDK package in the project. You can then use the SDK directly in the project.

2.13.2.2.2.2. Configure identity verification credentials

When using Alibaba Cloud Apsara Stack SDK to access Apsara Stack services, you must provide your Apsara Stack tenant account for identity verification.

Currently, the SLB Python SDK supports identity verification using AccessKeys. For details about how to obtain an AccessKey, see Obtain an AccessKey pair.

If you use an AccessKey as the access credential, you must configure your credential when initializing the client.

Notice Do not disclose any code containing your AccessKey (for example, do not commit the code to public GitHub projects). Otherwise, your Apsara Stack tenant account may be compromised.

```
clt = client.AcsClient(secret_id, secret_key, region_id)
```

2.13.2.2.2.3. Initiate a call

This topic describes how to use the SLB Python SDK to initiate a call.

Procedure

1. Import the SLB Python SDK.

```
from aliyunsdkcore.client import AcsClient
                from aliyunsdkcore.acs_exception.exceptions import ClientException
                from aliyunsdkcore.acs_exception.exceptions import ServerException
                from aliyunsdkslb.request.v20140515 import CreateLoadBalancerRequest
```

2. Create an AcsClient instance.

```
client = AcsClient(
                "<your-access-key-id>",
                "<your-access-key-secret>",
                "<your-region-id>" );
```

3. Create a Request object.

```
request = CreateLoadBalancerRequest.CreateLoadBalancerRequest()
                request.set_LoadBalancerName('MyLoadBalancer')
                request.set_AddressType('internet')
                request.set_InternetChargeType('paybytraffic')
```

4. Initiate a call and handle the response.

```
response = client.do_action_with_exception(request)
                print response
```

2.13.2.2.2.4. Set HTTPS requests

Alibaba Cloud Apsara Stack Python SDK allows you to initiate API requests over HTTP and HTTPS.

You can specify a protocol (HTTP or HTTPS) for a specific request, or set a global default protocol.

> **Note** The default protocol of the service takes precedence over the global default protocol.

Add OpenSSL support

The HTTPS protocol support of Alibaba Cloud Apsara Stack Python SDK is based on the OpenSSL support in Python. To use Alibaba Cloud Apsara Stack Python SDK to send HTTP requests, you must add OpenSSL support in Python.

Run the `python -c "import ssl"` command to check whether OpenSSL is supported in Python. If `ImportError: No module named ssl` is not displayed in the command output, OpenSSL is already supported.

If OpenSSL is not supported, run the following command to install it:

```
pip install pyopenssl
```

Set the protocol to HTTP or HTTPS for a request

The following code example shows how to set the protocol to HTTPS for a request:

```
request = CreateLoadBalancerRequest.CreateLoadBalancerRequest()
request.set_protocol_type("https")
# Valid value: https or http
```

Set a global default protocol

The following code example shows how to set a global default protocol:

```
import aliyunsdkcore.request
aliyunsdkcore.request.set_default_protocol_type("https")
# Create a request and call client.do_action_with_exception() to send the request.
```

2.13.2.2.2.5. Handle errors

If an error occurs on the server side or SDK side when you use the Python SDK, the Python SDK returns the corresponding exception message. An exception message contains the detailed error information, namely the error code and the error message.

Generally, you are not required to handle the errors returned by the Python SDK. You are only required to handle the errors on the server side according to the error message.

- `ServerException` is the error message on the server side.
- `ClientException` is the error message on the SDK side.

For example, if the following error occurs, modify the ID of AccessKey according to the detailed error message.

```
aliyunsdkcore.acs\_exception.exceptions.ServerException: HTTP Status: 404 Error:InvalidAccessKeyId.N
otFound Specified access key is not found.
```

To handle the errors returned by the Python SDK, see the following code example for reference:

```
try:
    response = client.do_action_with_exception(request)
except ServerException as e:
    # Add your own error handling logic here.
    # For example, print the detailed error message.
    print e.get_http_status()
    print e.get_error_code()
    print e.get_error_msg()
```

2.13.2.2.2.6. Common errors

This topic describes the common errors when you use the Python SDK. Troubleshoot the problems based on the corresponding causes and solutions.

Error code	Error message	Cause	Solution

SDK.InvalidRegionId	Can not find endpoint to access.	SDK cannot automatically obtain the endpoint (domain name) of the called product in the specified region.	Check if the provided region ID and endpoint are correct. Obtain the endpoint and then use the following code to configure the endpoint:
			`from aliyunsdkcore.profile import region_provider`
			`region_provider.modify_point('product_name', 'region_id', 'endpoint')`

SDK.TimeoutError	—	The request times out and all retries fail.	If the network quality is low, we recommend that you extend the timeout or increase the maximum number of retries.
SDK.ServerError:InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend: https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	This API only accepts HTTPS requests, instead of HTTP requests.	Before sending a request, add the following code: `request.set_protocol_type('https')`

2.13.2.3. PHP SDK

2.13.2.3.1. Quick start

Alibaba Cloud Apsara Stack SLB PHP SDK allows you to access SLB without performing complicated programming operations. This topic describes how to install and use the SLB PHP SDK.

Preparation

- To use the SLB PHP SDK, you must have an Apsara Stack tenant account as well as an AccessKey. For more information about how to obtain and view your AccessKey in the Apsara Stack console, see Obtain an AccessKey pair.
- Obtain the SLB endpoint. For more information, see Obtain an endpoint.
- The SLB PHP SDK supports PHP V5.3, V5.4, V5.5, V5.6, V7.0, and V7.1. (You can use the **php -v** command to obtain the current PHP version number.)

Installation

Complete the following steps to install the SLB PHP SDK:

1. Download the PHP SDK source code from the Apsara Stack official website.
2. Add the PHP SDK reference to your code.

   Assume that the PHP SDK source code is downloaded to the `/path/to/aliyun-openapi-php-sdk` directory, and run the following command to add the PHP SDK reference:

   ```
   require_once '/path/to/aliyun-openapi-php-sdk/aliyun-php-sdk-core/Config.php';
   ```

Usage

The following code example shows the three main steps to use the SLB PHP SDK:

1. Create and initialize a DefaultAcsClient instance.

   When creating and initializing the DefaultAcsClient instance, you must specify the Region ID, AccessKey ID, and AccessKey Secret parameters.

2. Create an API request and set parameters.
3. Initiate the request and handle the response or exception.

```
<? php

use Slb\Request\V20140515\DescribeLoadBalancersRequest;

// Create a DefaultAcsClient instance and initialize it.
$clientProfile = DefaultProfile::getProfile(
    "<your-region-id>",              # Your region ID
    "<your-access-key-id>",          #  Your AccessKey ID
    "<your-access-key-secret>"       # Your AccessKey Secret
);
$client = new DefaultAcsClient($clientProfile);

# Create an API request and set parameters.
$request = new DescribeLoadBalancersRequest();
$request->setPageSize(10);

# Initiate the request and handle the response.
try {
    $response = $client->getAcsResponse($request);
    print_r($response);
} catch(ServerException $e) {
    print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
} catch(ClientException $e) {
    print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
}
? >
```

2.13.2.4. Go SDK

2.13.2.4.1. Quick start

Alibaba Cloud Apsara Stack SLB Go SDK allows your to access SLB without performing complicated programming operations. This topic describes how to obtain and use the SLB Go SDK.

Preparation

- To use the SLB Go SDK, you must have an Apsara Stack tenant account as well as an AccessKey. For more information about how to obtain and view your AccessKey in the Apsara Stack console, see Obtain an AccessKey pair.
- Obtain the SLB endpoint. For more information, see Obtain an endpoint.

Installation

1. Download the Go SDK source code from the Apsara Stack official website.

2. Decompress the source code to the directory specified by *GO_PATH*.

Usage

The following code example shows the three main steps to use the SLB Go SDK:

1. Create a client instance.
2. Create an API request and set parameters.
3. Initiate the request and handle the response or exception.

```
package main

import (
    "github.com/aliyun/alibaba-cloud-sdk-go/services/slb"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "fmt"
)

func main() {
    // Create an slbClient instance.
    slbClient, err := slb.NewClientWithAccessKey(
        "<your-region-id>", // Your region ID
        "<your-access-key-id>", // Your AccessKey ID
        "<your-access-key-secret>") // Your AccessKey Secret
    if err != nil {
        // Handle the exception.
        panic(err)
    }
    // Create an API request and set parameters.
    request := slb.CreateDescribeLoadBalancersRequest()
    // Set request.PageSize to 10.
    request.PageSize = requests.NewInteger(10)
    // Initiate the request and handle the exception.
    response, err := slbClient.DescribeLoadBalancers(request)
    if err != nil {
        // Handle the exception.
        panic(err)
    }
    fmt.Println(response)
}
```

2.13.2.4.2. Use the SDK

2.13.2.4.2.1. Install Go SDK

This topic describes how to install Alibaba Cloud Apsara Stack SLB Go SDK.

Context

The SLB Go SDK supports Go V1.7 and later. You can install the SLB Go SDK by using the following methods:

Procedure

1. Download the Go SDK source code from the Apsara Stack official website.
2. Decompress the source code to the directory specified by *GO_PATH*.

2.13.2.4.2.2. Configure identity verification credentials

When using Alibaba Cloud Apsara Stack SDK to access Apsara Stack services, you must provide your Apsara Stack tenant account for identity verification.

Currently, the SLB Go SDK supports identity verification using AccessKeys. For details on how to obtain an AccessKey, see Obtain an AccessKey pair.

If you use an AccessKey as the access credential, you must configure your credential when initializing the client.

> **Notice** Do not disclose any code containing your AccessKey (for example, do not commit the code to public GitHub projects). Otherwise, your Apsara Stack tenant account may be compromised.

```
// Create an slbClient instance.
client, err := slb.NewClientWithAccessKey(
    "<your-region-id>", // Your region ID
    "<your-access-key-id>", // Your AccessKey ID
    "<your-access-key-secret>") // Your AccessKey Secret
```

If you want to use the custom *Config* or credentials other than AccessKeys, you must first create a `Credential` object to store the credentials, and then submit the `Credential` object when initializing the client.

```
// Customize configurations.
config := NewConfig()
// Create a Credential object.
credential := &credentials.BaseCredential{
   AccessKeyId:     "<your-access-key-id>",
   AccessKeySecret: "<your-access-key-secret>",
}
// Initialize the client.
client, err := NewClientWithOptions("cn-hangzhou", config, credential)
```

2.13.2.4.2.3. Initiate a call

This topic describes how to use the SLB Go SDK to initiate a call.

Procedure

1. Import the SLB Go SDK.

```
import github.com/aliyun/alibaba-cloud-sdk-go/services/slb
```

2. Create an slbClient instance that contains all the SLB APIs.

```
slbClient := slb.NewClientWithAccessKey(
   "<your-region-id>",
   "<your-access-key-id>",
   "<your-access-key-secret>")
```

3. Use the `xxx.CreateXXXRequest` method to create a request.

   The naming convention for the method is `${service}. Create${apiName}Request`, where

   - ${service} is a service name in lowercase letters such as *slb*.
   - ${apiName} is an API name such as *DescribeLoadBalancers*.

```
request := slb.CreateDescribeLoadBalancersRequest()
request.InstanceId = ""
```

4. Initiate a call.

```
response, err := slbClient.DescribeLoadBalancers(request)
```

5. Handle the response.

   In normal cases, all returned fields are deserialized into the response. You can directly call `response.getXXX()` to obtain the response fields.

```
instanceStatus := response.Status
```

   If an error `(err ! = nil)` occurs or you need the original HTTP response, you can use the following methods to obtain the original data:

```
// Obtain the original HTTP response. The response type is *http.Response.
httpResponse := response.GetOriginHttpResponse()

// Obtain the status code of the original HTTP response. The response type is int.
statusCode := response.GetHttpStatus()

// Obtain the header of the original HTTP response. The response type is map[string][]string.
headers := response.GetHttpHeaders()

// Obtain the content of the original HTTP response. The response type is []byte.
contentBytes := response.GetHttpContentBytes()

// Obtain the original HTTP response content and convert the content to a UTF-8 string. The respon
se type is string.
contentString := response.GetHttpContentString()
```

2.13.2.4.2.4. Handle errors

Alibaba Cloud Apsara Stack SLB Go SDK returns error messages when errors occur on either the server or SDK side. The messages contain error details, that is, `ClientError` and `ServerError` in `sdk.errors`. The errors conform to the standard Go error interface, so they can be handled in a similar way as standard Go errors.

ClientError

When an error occurs to any call in the SLB Go SDK and cannot be handled automatically, the SLB Go SDK returns a `ClientError`.

You can use the following code to determine and obtain error information from the `ClientError`:

```
response, err := slbClient.DescribeLoadBalancers(request)
if clientError, ok := err.(*errors.ClientError); ok{
    // Obtain the error code.
    clientError.ErrorCode()
    // Obtain the error description.
    clientError.Message()
    // Obtain the original error, which may be nil.
    clientError.OriginError()
}
```

ServerError

When a server returns an error response, the SLB Go SDK encapsulates the error response into a `ServerError` and returns it.

Note In this case, you can still obtain the original HTTP response from the encapsulated response.

You can execute the following code to determine and obtain error information from ServerError and Response:

```
response, err := slbClient.DescribeLoadBalancers(request)
if serverError, ok := err.(*errors.ServerError); ok{
   // Obtain the error code.
   serverError.ErrorCode()
   // Obtain the error description.
   serverError.Message()
   // Obtain the original HTTP response.
   response.GetOriginHttpResponse()
}
```

2.13.2.4.2.5. Customize configurations

The topic lists the custom configurations supported by Alibaba Cloud Apsara Stack SLB Go SDK.

Method

You can use the config module of the SLB Go SDK to customize configurations.

```
config := NewConfig().
      WithEnableAsync(true).
      WithGoRoutinePoolSize(5).
      WithMaxTaskQueueSize(1000)
client, err := slb.NewClientWithOptions("<region-id>", config, credential)
```

Note Currently, the `config` module of the SLB Go SDK does not support the following calling method:

```
config := &Config{EnableAsync: true,}
```

Supported custom configurations

The following table shows the supported custom configurations currently.

Configuration	Default value	Description
AutoRetry	true	Whether to enable the automatic retry

Configuration	Default value	Description
MaxRetryTime	3	The maximum number of retries With the automatic retry enabled, the maximum time consumption for a single call is Timeout (MaxRetryTime + 1).
Timeout	10time.Second	Timeout value. Full-link timeout value, containing establishing connection, redirecting, and reading response If the value is *0*, no timeout occurs.
HttpTransport	nil	Enable the configuration of the underlying `net/http.client` You can configure the original `http.client` of Go with this configuration, such as persistent connection.
EnableAsync	false	Whether to enable the asynchronous feature
MaxTaskQueueSize	1000	The length of the asynchronous queue, which takes effect only when `EnableAsync=true` If the queue is full, new calls are congested.
GoRoutinePoolSize	5	The maximum number of concurrent connections, which takes effect only when `EnableAsync=true`

2.13.2.4.2.6. Asynchronous calls

With the concurrent characteristic of the Go language, we recommend that you control the concurrent requests of SDK on the application layer. For your convenience, the Alibaba Cloud Go SDK provides the concurrent calling method that can be directly used. The related concurrency control is achieved within SDK.

Enable the concurrent function for a client

In the following example, the `Credential` object is used to set up user credentials.

```
// The maximum number of concurrent connections.
poolSize := 10

// The maximum number of cacheable requests.
maxTaskQueueSize := 10000

// Enable the asynchronous feature when creating a client.
config := sdk.NewConfig().
   WithEnableAsync(true).
   WithGoRoutinePoolSize(poolSize).          // Optional. Default value: 5.
   WithMaxTaskQueueSize(maxTaskQueueSize)     // Optional. Default value: 1000

// Use the custom configuration to initialize the client.
slbClient, err := slb.NewClientWithOptions("<your-region-id>", config, credential)

// Alternatively, enable the asynchronous feature after initializing the client.
client.EnableAsync(poolSize, maxTaskQueueSize)
```

Initiate asynchronous calls

The Alibaba Cloud Go SDK supports two methods of initiating asynchronous calls as follows:

- Use channel as the returned value.

```
// this will not block
responseChannel, errChannel := client.FooWithChan(request)
// this will block
response := <-responseChannel
err = <-errChanne
```

- Use callback to control the response.

```
// this will not block
blocker := client.FooWithCallback(request, func(response *FooResponse, err error) {
       // handle the response and err
    }
  )
// The blocker is (chan int) and is used to control the synchronization. If the returned value is 1, the a
ction succeeds. If the returned value is 0, the action fails.
// If <-blocker returns 0 and the action fails, the error message is transmitted to callback by means of
err.
// this will block
result := <-blocker
```

2.13.2.4.2.7. Use CommonRequest

If the product API that you want to call does not have the corresponding SDK, you can use the generic calling method (CommonRequest) to call the product APIs. By using the CommonRequest calling method, you can call any APIs.

Example: Call a RESTful API

The following code example shows how to use CommonRequest to call the API that lists all the Container Service cluster instances:

```
package main

import (
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk"
    "fmt"
)

func main() {
    client, err := sdk.NewClientWithAccessKey("{your_region_id", "{your_access_key_id}", "{your_access_ke
y_id}")
    if err != nil {
        panic(err)
    }

    request := requests.NewCommonRequest()
    request.Domain = "cs.aliyuncs.com"
    request.Version = "2015-12-15"
    //  Because the API is a RESTful API, you must specify the value of the PathPattern field.
    request.PathPattern = "/clusters"
    response, err := client.ProcessCommonRequest(request)
    if err != nil {
        panic(err)
    }
    fmt.Print(response.GetHttpContentString())
}
```

2.13.2.4.2.8. Common errors

This topic describes the common errors when you use the Go SDK. Troubleshoot the problems based on the corresponding causes and solutions.

Error code	Error message	Cause	Solution
SDK.CanNotResolveEndpoint	Can not resolve endpoint, please check the user guide	The SDK cannot automatically obtain the endpoint of the called service in the specified region.	Check whether the specified region ID and endpoint are correct. After obtaining the correct endpoint, use the following code to set the endpoint: `request.Domain = "<endpoint>"`
SDK.JsonUnmarshalError	Failed to unmarshal response, but you can get the data via response.GetHttpStatusCode() and response.GetHttpContentString()	SDK response deserialization fails. In most cases, the cause is an inconsistency between the API metadata and the response structure received by the SDK, such as mismatched fields or an incorrect format.	For more information, see Response parsing.
SDK.TimeoutError	*The request timed out 4 times(3 for retry), perhaps we should have the threshold raised a little?*	The request times out and all retry attempts fail.	• In scenarios such as cross-region calls or poor network quality, we recommend that you prolong the timeout period or increase the maximum number of retries. • If the problem persists and there are no issues with the network quality, we recommend that you submit a ticket.
SDK.AsyncFunctionNotEnabled	Async function is not enabled in client, please invoke 'client.EnableAsync()' function	An asynchronous API is called when the asynchronous request switch is not turned on.	Enable the asynchronous feature. For more information, see Asynchronous calls.

Response parsing

Ignore SDK deserialization failures and obtain the response attributes by extracting the original HTTP response.

> **Note** Alibaba Cloud Apsara Stack Go SDK depends on JMESPath. Therefore, if the response content is in JSON format, you can directly use JMESPath to parse the response.

```
response, err := client.CreateInstance(request)
    if err ! = nil {
        // Handle the exception.
        if clientErr, isClientErr := err.(*errors.ClientError); isClientErr {
            if clientErr.ErrorCode() == errors.JsonUnmarshalErrorCode {
                // You can obtain the original response data through our encapsulation methods.
                // The HTTP status code in the response. Type: int.
                statusCode := response.GetHttpStatus()
                // The HTTP header in the response. Type: map[string][]string.
                responseHeader := response.GetHttpHeaders()
                // The packet content in the response. Type: []byte.
                responseBytes := response.GetHttpContentBytes()
                // The packet content in the response. Type: string, equivalent to string(response.GetHttpCont
entBytes())`.
                responseContent := response.GetHttpContentString()
                // You can also directly obtain the original response. Type: net/http.Response.
                httpResponse := response.GetOriginHttpResponse()
            }
        }
    }
```

2.13.2.5. .NET SDK

2.13.2.5.1. Quick start

Alibaba Cloud Apsara Stack SLB .NET SDK allows your to access SLB without performing complicated programming operations. This topic describes how to install and use the SLB .NET SDK.

Preparation

- To use the SLB .NET SDK, you must have an Apsara Stack tenant account as well as an AccessKey. For more information about how to obtain and view your AccessKey in the Apsara Stack console, see Obtain an AccessKey pair.
- Obtain the SLB endpoint. For more information, see Obtain an endpoint.
- The SLB .Net SDK applies to .NET Framework V4.0 and later.

Install SLB .NET SDK

To use the SDK of a service, you must install both the SDK and SDK core library. For example, to use the SLB .NET SDK, you must install both the SDK and the SDK core library. Install the SLB .NET SDK by using either of the following methods:

- Add DLL reference
    i. Download the DLL package from .NET SDK, and decompress it to get the DLL files.
    ii. Right-click your project in the Solution Explorer of Visual Studio and click **Reference**.

iii. In the menu that appears, click **Add Reference**.

iv. In the dialog box that appears, click **Browse**. Then select the downloaded DLL file and click **Confirm**.

- Add project reference
  i. Download the .NET SDK source code from the Apsara Stack official website .
  ii. You can find a *aliyun-net-openapi-XXX* folder in the folder of the downloaded source code, and then locate a **.csproj* file, which is the .NET project file. For example, find the `aliyun-net-openapi-slb` folder and then the `aliyun-net-sdk-slb.csproj` file.
  iii. In Visual Studio, right-click your solution.
  iv. Choose **Add** > **Existing Project**.
  v. In the dialog box that appears, select the .NET project file such as `aliyun-net-sdk-slb.csproj` and click **Open**.
  vi. Right-click your project and choose **Reference** > **Add Reference** from the shortcut menu.

Usage

The following code example shows the three main steps to use the SLB .NET SDK:

1. Create and initialize a DefaultAcsClient instance.
2. Create an API request and set parameters.
3. Initiate the request and handle the response or exception.

```
using Aliyun.Acs.Core;
using Aliyun.Acs.Core.Profile;
using Aliyun.Acs.Core.Exceptions;
using Aliyun.Acs.Slb.Model.V20140526;

class TestProgram
{
   static void Main(string[] args)
   {
      // Construct a client for initiating requests.
      IClientProfile profile = DefaultProfile.GetProfile(
         "<your-region-id>",
         "<your-access-key-id>",
         "<your-access-key-secret>");
      DefaultAcsClient client = new DefaultAcsClient(profile);
      try
      {
         // Construct a request.
         DescribeLoadBalancersRequest request = new DescribeLoadBalancersRequest();
         request.PageSize = 10;
         // Initiate the request and obtain a response.
         DescribeLoadBalancersResponse response = client.GetAcsResponse(request);
         System.Console.WriteLine(response.TotalCount);
      }
      catch (ServerException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
      catch (ClientException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
   }
}
```

2.13.2.5.2. Use the SDK

2.13.2.5.2.1. Install .NET SDK

This topic describes how to install Alibaba Cloud Apsara Stack SLB .NET SDK.

You can install the SLB .NET SDK by using either of the following methods:

- Add DLL reference
  i. Download the package containing the DLL file from .NET SDK and then extract the package to obtain the DLL file.
  ii. In the Solution Explorer of Visual Studio, right-click your project and then select **Reference**.
  iii. In the displayed menu, click **Add Reference**.
  iv. In the displayed dialog box, click **Browse**. Select the downloaded DLL file and click **Confirm**.
- Add project reference
  i. Download the .NET SDK source code from the Apsara Stack official website .
  ii. You can find an *aliyun-net-openapi-XXX* folder in the folder of the downloaded source code and then locate a **.csproj* file, which is the .NET project file in the folder. For example, find the `aliyun-net-openapi-slb` folder and then the `aliyun-net-sdk-slb.csproj` file.
  iii. In Visual Studio, right-click your solution.
  iv. Choose **Add** > **Existing Project**.
  v. In the displayed dialog box, select the .NET project file such as the `aliyun-net-sdk-slb.csproj` file, and click **Open**.
  vi. Right-click your project and choose **Reference** > **Add Reference** from the shortcut menu.

2.13.2.5.2.2. Configure identity verification credentials

When using the Alibaba Cloud .NET SDK to access Alibaba Cloud Apsara Stack services, you must provide an Alibaba Cloud account for authentication.

Currently, the SLB .NET SDK supports identity verification using AccessKeys. For details about how to obtain an AccessKey, see Obtain an AccessKey pair.

If you use an AccessKey as the access credential, you must configure your credential when initializing the client.

> **Notice** Do not disclose any code containing your AccessKey (for example, do not commit the code to public GitHub projects). Otherwise, your Apsara Stack tenant account may be compromised.

```
IClientProfile clientProfile = DefaultProfile.GetProfile(
  "<your-region-id>", // Your region ID
  "<your-access-key-id>", //  AccessKey ID of your Apsara Stack tenant account
  "<your-access-key-secret>"); // AccessKey Secret of your Apsara Stack tenant account
```

2.13.2.5.2.3. Initiate a call

This topic describes how to use the SLB .NET SDK to initiate a call.

1. Create a DefaultAcsClient instance.

   ```
   DefaultAcsClient client = new DefaultAcsClient(clientProfile);
   ```

2. Create a request.

The naming convention for requests is `${apiName}Request`, where ${apiName} is the API name such as *DescribeLoadBalancers*.

When the SDKs of multiple services are used, different requests may have the same name. Differentiate the requests by SDK package.

```
DescribeLoadBalancersRequest request = new DescribeLoadBalancersRequest();
request.PageSize = 10;
```

3. Initiate a call and handle the response.

```
DescribeLoadBalancersResponse response = client.GetAcsResponse(request);
```

In normal cases, all returned fields are deserialized into the response. You can directly call `response.getXXX()` to obtain the response fields.

```
System.Console.WriteLine(response.TotalCount);
```

2.13.2.5.2.4. Handle errors

If an error occurs on the server side or SDK side when you use Alibaba Cloud .NET SDK, the .NET SDK returns the corresponding exception message. An exception message contains the detailed error information, namely the error code and the error message.

Generally, you are not required to handle the errors returned by the Alibaba Cloud .NET SDK. You are only required to handle the errors on the server side according to the error message.

- `ServerException` is the error message on the server side.
- `ClientException` is the error message on the SDK side.

For example, if the following error occurs, modify the ID of AccessKey according to the detailed error message.

```
InvalidAccessKeyId.NotFound : Specified access key is not found.
```

To handle the errors returned by the .NET SDK, see the following code example for reference:

```
try
{
    CreateInstanceResponse response = client.GetAcsResponse(request);
    // Handle the response.
    // ...
}
catch (ServerException e)
{
    // Add your own error handling logic here.
    // For example, print the detailed error message.
    Console.WriteLine("ErrorCode=" + e.ErrorCode);
    Console.WriteLine("ErrorMessage=" + e.ErrorMessage);
    // If the problem is tricky, open a ticket and provide the RequestId for us.
    Console.WriteLine("ErrorCode=" + e.RequestId);
}
catch (ClientException e)
{
    // Add your own error handling logic here.
    // For example, print the detailed error message.
    Console.WriteLine("ErrorCode=" + e.ErrorCode);
    Console.WriteLine("ErrorMessage=" + e.ErrorMessage);
}
```

2.13.2.5.2.5. Use CommonRequest

If the product API that you want to call does not have the corresponding SDK, you can use the generic calling method (CommonRequest) to call the product APIs. By using the CommonRequest calling method, you can call any APIs.

Characteristics of CommonRequest calling

The CommonRequest calling method has the following characteristics:

- Light weight: You only need the core package to initiate the call, without downloading or installing the SDK of each product.
- Easy and convenient: You can call the latest API without updating the SDK.
- Fast iteration

Call an API by using CommonRequest

To make a CommonRequest request, you must specify the following parameters. You can obtain the values of these parameters from the API documents.

- Domain: specifies the service endpoint.
- Version: specifies the API version, in the format of YYYY-MM-DD.

You can get the API version from the common parameters in the API documents.

- Action: specifies the name of the API to be called.

  You must obtain the Action parameter value and specify the API name in the form of `request.ApiName = "<Action>"`.

  For example, to call the RunInstances API, initiate a CommonRequest request with `request.ApiName = "RunInstances"`.

Example: Call a RESTful API

The following code example shows how to use CommonRequest to call the API that lists all the Container Service cluster instances:

```
using Aliyun.Acs.Core;
using Aliyun.Acs.Core.Exceptions;
using Aliyun.Acs.Core.Profile;

class Sample
{
   static void Main(string[] args)
   {
      // Construct a client instance for initiating requests.
      IClientProfile profile = DefaultProfile.GetProfile(
         "<your-region-id>",
         "<your-access-key-id>",
         "<your-access-key-secret>");
      DefaultAcsClient client = new DefaultAcsClient(profile);

      try
      {
         // Construct a request.
         CommonRequest request = new CommonRequest();
         request.Domain = "cs.aliyuncs.com";
         request.Version = "2015-12-15";

         // Because the API is a RESTful API, you must specify the value of the UriPattern field.
         request.UriPattern = "/clusters";

         // Initiate the request and obtain a response.
         CommonResponse response = client.GetCommonResponse(request);
         System.Console.WriteLine(response.Data);
      }
      catch (ServerException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
      catch (ClientException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
   }
}
```

2.13.2.5.2.6. Common errors

This topic describes the common errors when you use the .NET SDK. Troubleshoot the problems based on the corresponding causes and solutions.

Error code	Cause	Solution
SDK.InvalidRegionId	SDK cannot automatically obtain the endpoint of the called product in the specified region.	Check if your endpoint is correct.
InvalidAccessKeyId.NotFound	The configured AccessKey ID is invalid.	Check if your AccessKey ID is correct.
SDK.ConnectionReset	The endpoint cannot be connected when you initiate a request.	Check if your network is available.
SDK.InvalidProfile	The DefaultProfile parameter that you provided when initializing DefaultAcsClient is invalid.	Make sure that the provided DefaultProfile parameter object is properly initialized and configured with corresponding parameters.
SDK.SessionTokenExpired	The DefaultProfile parameter that you provided when initializing DefaultAcsClient is invalid.	Make sure that the provided SessionToken parameter is in the validity period, which is generally one hour.
SignatureDoesNotMatch	The provided SessionToken is invalid or has expired.	Make sure that the provided DefaultProfile parameter object is properly initialized and configured with corresponding parameters.
SDK.InvalidProfile	The AccessKey Secret does not match the AccessKey ID.	Make sure that the provided AccessKey Secret is valid.

2.13.2.6. Obtain an AccessKey pair

You can obtain an AccessKey pair in the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center > Department**

Management.

3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**.

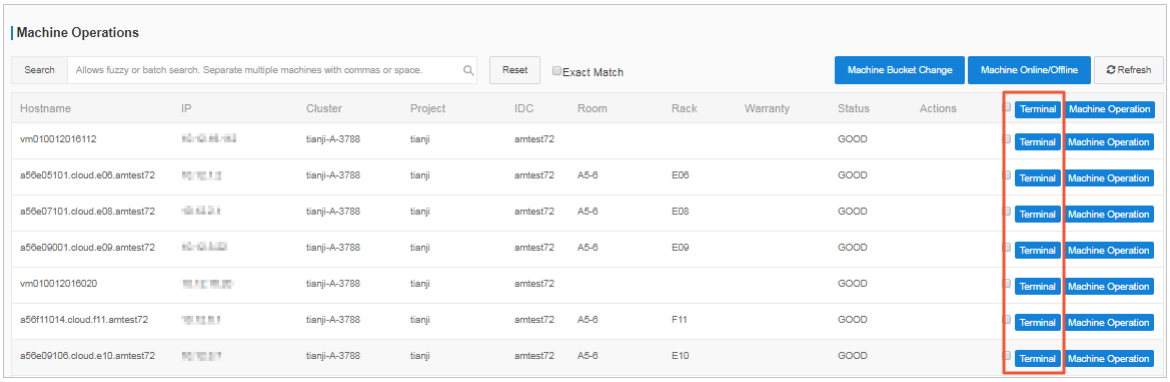
   The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.13.2.7. Obtain an endpoint

You can obtain an endpoint of SLB in Apsara Stack Operations.

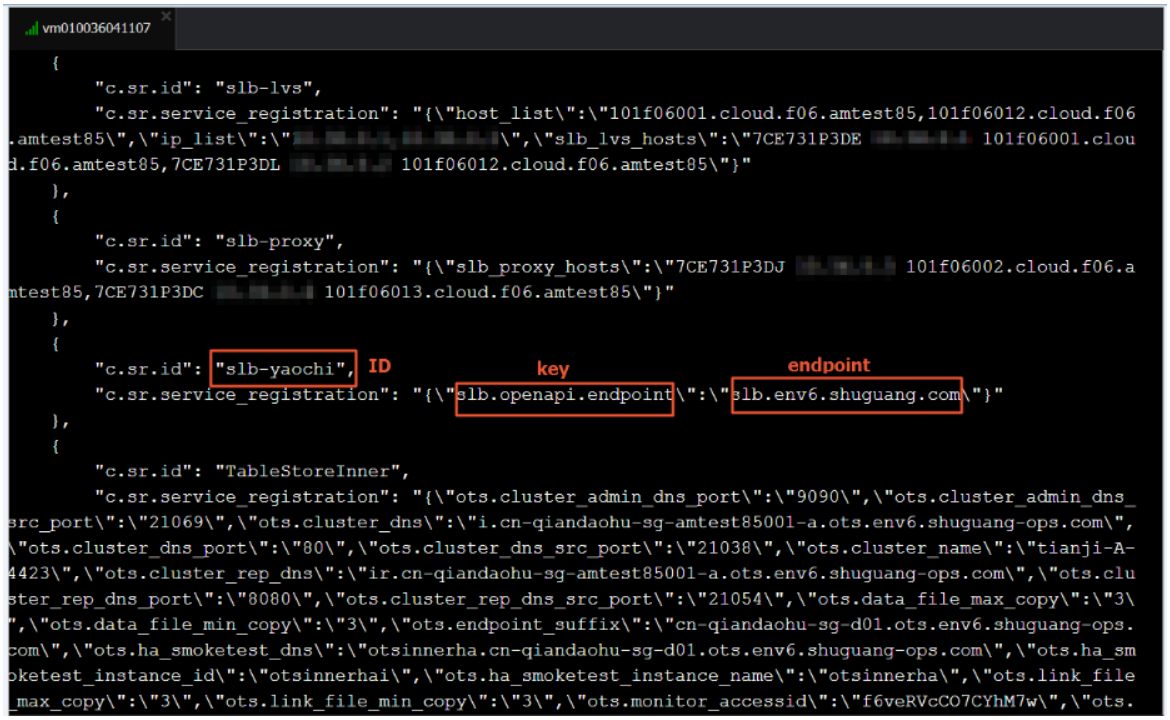
Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms > Apsara Stack Operations > Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. Choose **Operations > Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the command **curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration"** to obtain JSON data.

7. Find the endpoint of *SLB* according to the product ID (*slb-yaochi*) and key (*slb.openapi.endpoint*) of *SLB*.



2.14. Virtual Private Cloud (VPC)

2.14.1. API reference

2.14.1.1. List of operations by function

The following tables list API operations available for use in a VPC.

VPC operations

Operation	Description
CreateVpc	Creates a VPC.
DeleteVpc	Deletes a VPC.
DescribeVpcs	Queries created VPCs.
ModifyVpcAttribute	Modifies the name and description of a VPC.

VSwitch operations

Operation	Description
CreateVSwitch	Creates a VSwitch.
DeleteVSwitch	Deletes a VSwitch.
ModifyVSwitchAttribute	Modifies the name and description of a VSwitch.
DescribeVSwitches	Queries created VSwitches.

VRouter operations

Operation	Description
ModifyVRouterAttribute	Modifies the name and description of a VRouter.
DescribeVRouters	Queries VRouters in a specified region.
CreateRouteEntry	Creates a custom route entry on a VRouter or VBR.
DeleteRouteEntry	Deletes a route entry in the routing table of a VRouter or VBR.
DescribeRouteTables	Queries route entries in a routing table.

EIP operations

Operation	Description
AllocateEipAddress	Creates an Elastic IP address (EIP).
AssociateEipAddress	Binds an EIP to a VPC instance in the same region.
UnassociateEipAddress	Unbinds an EIP from a VPC instance.

Operation	Description
ModifyEipAddressAttribute	Modifies the name, description, and peak bandwidth of an EIP.
ReleaseEipAddress	Releases a specified EIP.
DescribeEipAddresses	Queries created EIPs.

Router interface operations

Operation	Description
CreateRouterInterface	Creates a router interface.
ConnectRouterInterface	The initiator router interface initiates a connection to the receiver router interface.
DeactivateRouterInterface	Deactivates a router interface.
ModifyRouterInterfaceSpec	Modifies the specifications of a router interface.
DeleteRouterInterface	Deletes a router interface.
DescribeRouterInterfaces	Queries router interfaces in a specified region.
ActivateRouterInterface	Activates an inactive router interface.
ModifyRouterInterfaceAttribute	Modifies the configurations of a router interface.

Physical connection operations

Operation	Description
CreatePhysicalConnection	Creates a physical connection.
CancelPhysicalConnection	Cancels a physical connection before it is enabled. After you cancel the physical connection, it enters the Canceled state.
DeletePhysicalConnection	Deletes a physical connection.
ModifyPhysicalConnectionAttribute	Modifies the configurations of a physical connection.
DescribePhysicalConnections	Queries physical connections in a specified region.
TerminatePhysicalConnection	Terminates a physical connection after it is enabled.
EnablePhysicalConnection	Enables a physical connection that is in the Confirmed state. After you have enabled the physical connection, it enters the Enabled state.

VBR operations

Operation	Description
CreateVirtualBorderRouter	Creates a virtual border router (VBR).
DeleteVirtualBorderRouter	Deletes a VBR.
DescribeVirtualBorderRouters	Queries created VBRs.
DescribeVirtualBorderRoutersForPhysicalConnection	Queries the VBRs created for a physical connection, including VBRs that belong to the physical connection owner and other accounts.
ModifyVirtualBorderRouterAttribute	Modifies the configurations of a VBR.
TerminateVirtualBorderRouter	Terminates a VBR.
RecoverVirtualBorderRouter	Recovers a terminated VBR.

NAT Gateway operations

Operation	Description
CreateNatGateway	Creates a NAT Gateway.
DeleteNatGateway	Deletes a NAT specified Gateway.
ModifyNatGatewaySpec	Modifies the type of a NAT Gateway.
ModifyNatGatewayAttribute	Modifies the configurations of a NAT Gateway.
DescribeNatGateways	Queries created NAT Gateways.
CreateBandwidthPackage	Creates a NAT service plan.
ModifyBandwidthPackageSpec	Modifies the bandwidth of a specified NAT service plan.
DescribeBandwidthPackages	Queries NAT service plans in a specified region.
ModifyBandwidthPackageAttribute	Modifies the name and description of a specified NAT service plan.
DeleteBandwidthPackage	Deletes a specified NAT service plan.
AddBandwidthPackageIps	Adds public IP addresses to a NAT service plan.
RemoveBandwidthPackageIps	Removes public IP addresses from a NAT service plan.

Operation	Description
CreateForwardEntry	Adds DNAT entries to a DNAT table.
DeleteForwardEntry	Deletes a specified DNAT entry.
ModifyForwardEntry	Modifies a specified DNAT entry.
DescribeForwardTableEntries	Queries DNAT entries in a specified DNAT table.
CreateSnatEntry	Adds SNAT entries to a SNAT table.
DeleteSnatEntry	Deletes a specified SNAT entry.
ModifySnatEntry	Modifies the SNATed IP address (public IP address) in a specified SNAT entry.
DescribeSnatTableEntries	Queries SNAT entries in a specified SNAT table.

2.14.1.2. Call VPC APIs

2.14.1.2.1. Request structure

When you call a VPC operation, an HTTP GET request is sent to the endpoint of the VPC operation. You must add the relevant request parameters to the request based on the operation description. After the operation is called, the system returns the processing result. Requests and responses are encoded in UTF-8.

VPC uses the RPC API. You can call VPC API operations by sending HTTP GET requests.

The request structure is as follows:

```
http://Endpoint/?Action=xx&Parameters
```

In the request,

- Endpoint: The endpoint for the VPC API is `vpc.example.com`.

  > **Note** `example.com` is a custom domain name. You can obtain endpoints in Apsara Stack Operations console. For more information, see Obtain an endpoint.

- Action: The operation that you want to perform. For example, you can call DescribeVpcs to query all created VPC instances.
- Version: The version of the API that you want to use. The current VPC API version is *2016-04-28*.
- Parameters: Request parameters that are separated with ampersands (&).

  Request parameters consist of common parameters and custom API parameters. Common parameters include the API version and authentication information. For more information, see Common parameters.

The following code provides an example of how to call the DescribeVpcs operation to query the created VPCs.

Note To improve readability, the API request is displayed in the following format:

```
https://vpc.example.com/?Action=DescribeVpcs
&Format=xml
&Version=2014-05-15
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2012-06-01T12:00:00Z
```

2.14.1.2.2. API authorization

To ensure the security of your account, we recommend that you call VPC APIs as a RAM user. Before you can use a RAM account to call a VPC API, you must create a RAM account and assign corresponding permissions to it.

For more information about VPC resources and APIs you can assign permissions on, see RAM authentication.

2.14.1.2.3. Request signature

To ensure the security of your API, you must sign the API request. Apsara Stack uses the signature in the request for identity verification.

Apsara Stack implements symmetric encryption through an AccessKey pair (AccessKey ID and AccessKey Secret) to authenticate the request sender. AccessKey pairs are an identity credential issued to Apsara Stack tenant accounts and RAM users (similar to the login password). The AccessKey ID is used to identify the user. The AccessKey Secret is used to encrypt the signature string on the client side and to verify the signature string on the server side. The AccessKey Secret must be kept strictly confidential. For more information about how to create an AccessKey pair, see Obtain an AccessKey pair.

For an RPC API, you must add the signature to the API request in the following format:

```
https://endpoint/?SignatureVersion=1.0&SignatureMethod=HMAC-SHA1&Signature=xxxx%xxxx%3D&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
```

Take DescribeVpcs as an example. If the AccessKey ID is `testid` and the AccessKey Secret is `testsecret`, the original request URL is as follows:

```
http://vpc.example.com/?Action=DescribeVpcs
&Timestamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2016-04-28
&SignatureVersion=1.0
```

Follow these steps to calculate the signature:

1. Use the request parameters to create the string to be signed.

   ```
   GET&%2F&AccessKeyId%3Dtestid&Action%3DDescribeVpcs&Format%3DXML&SignatureMethod%3DH
   MAC-SHA1&SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&SignatureVersion%3D1.0&Ti
   meStamp%3D2016-02-23T12%253A46%253A24Z&Version%3D2014-05-15
   ```

2. Calculate the HMAC value of the string to be signed.

   Append an ampersand (&) to the AccessKey Secret, which will be used as the key to calculate the HMAC value. In this example, the key is `testsecret&` .

   ```
   CT9X0VtwR86fNWSnsc6v8YGOjuE=
   ```

3. Add the signature to the request parameters:

   ```
   http://vpc.example.com/?Action=DescribeVpcs
   &Timestamp=2016-02-23T12:46:24Z
   &Format=XML
   &AccessKeyId=testid
   &SignatureMethod=HMAC-SHA1
   &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
   &Version=2016-04-28
   &SignatureVersion=1.0
   &Signature=xxxx%xxxx%3D
   ```

2.14.1.2.4. Obtain an AccessKey pair

You can obtain an AccessKey pair in the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department**

Management.

3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> **Note** The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**.

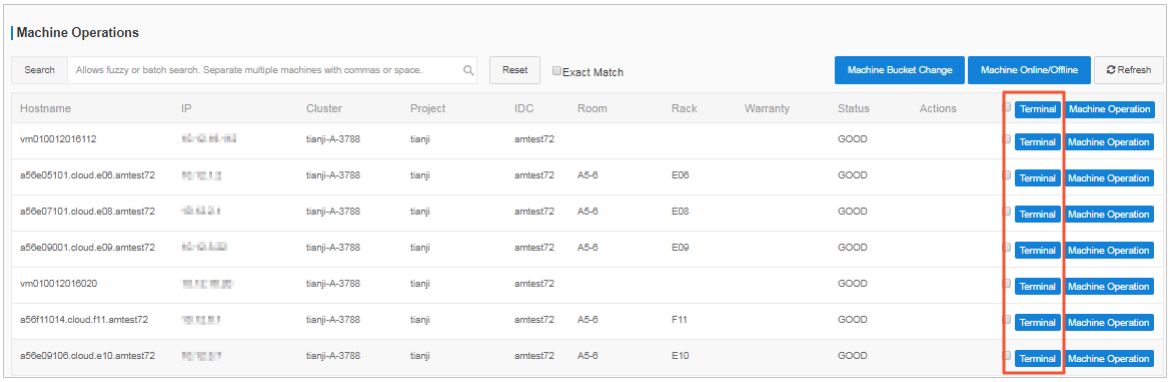
   The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.14.1.2.5. Obtain an endpoint

You can obtain the endpoint of a VPC in Apsara Stack Operations.

Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms > Apsara Stack Operations > Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara Infrastructure Management Framework page.
4. Choose **Operations > Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the following command to obtain the JSON data:

```
curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration
"
```

7. Obtain the endpoint of a VPC based on the ID (vpc-yaochi) and the key value (vpc.openapi.endpoint) of the VPC service.

2.14.1.3. RAM authentication

Before calling a VPC API using a RAM user, you must use an Apsara Stack tenant account to create an authorization policy to assign permissions to the RAM user. In the authorization policy, an Alibaba Cloud Resource Name (ARN) is used as the unique identifier of the resource to authorize.

VPC resources

The following table lists the VPC resources that can be authorized and their corresponding ARN formats.

Resource type	ARN format
Virtual Private Cloud (VPC)	acs:vpc:$regionid:$accountid:vpc/$vpcid
	acs:vpc:$regionid:$accountid:vpc/*
	acs:vpc:*:$accountid:vpc/*
VRouter	acs:vpc:$regionid:$accountid:vrouter/$vrouterid
	acs:vpc:$regionid:$accountid:vrouter/*
	acs:vpc:*:$accountid:vrouter/*
VSwitch	acs:vpc:$regionid:$accountid:vswitch/$vswitchid
	acs:vpc:$regionid:$accountid:vswitch/*
	acs:vpc:*:$accountid:vswitch/*
	acs:vpc:$regionid:$accountid:routetable/$routetableid

Resource type	ARN format
Routing table	
	acs:vpc:$regionid:$accountid:routetable/*
	acs:vpc:*:$accountid:routetable/*
Elastic IP Address (EIP)	acs:vpc:$regionid:$accountid:eip/$allocationid
	acs:vpc:$regionid:$accountid:eip/*
	acs:vpc:*:$accountid:eip/*
NAT Gateway	acs:vpc:$regionid:$accountid:natgateway/$natgatewayid
	acs:vpc:$regionid:$accountid:natgateway/*
	acs:vpc*:$accountid:vpc/*
NAT Gateway service plan	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
	acs:vpc:$regionid:$accountid:bandwidthpackage/*
	aacs:vpc:*:$accountid:vpc/*
Forwarding table	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
	acs:vpc:$regionid:$accountid:forwardtable/*
	acs:vpc:*:$accountid:vpc/*
SNAT table	acs:vpc:$regionid:$accountid:snattable/$snattableid
	acs:vpc:$regionid:$accountid:snattable/*
	acs:vpc:*:$accountid:vpc/*
General resource	acs:vpc:$regionid:$accountid:*
	acs:vpc:*:$accountid:*

`$regionid/ accoutid/ vrouterid` are IDs of the specific resources, `*` represents all resources.

VPC API operations

The following table lists the API operations that can be authorized and their corresponding ARN formats.

Operation	ARN format
vpc:CreateVpc	acs:vpc:$regionid:$accountid:vpc/*
vpc:DeleteVpc	acs:vpc:$regionid:$accountid:vpc/$vpcid
vpc:DescribeVpcs	vpc:$regionid:$accountid:vpc/*
vpc:ModifyVpcAttribute	acs:vpc:$regionid:$accountid:vpc/$vpcid
vpc:DescribeVRouters	acs:vpc:$regionid:$accountid:vrouter/*
	The VRouter ID is specified: "vpc:Vpc":"acs:vpc:$regionid:$accountid:vpc/$vpcid"
	The VRouter ID is not specified: "vpc:Vpc":"acs:vpc:$regionid:$accountid:vpc/*"
vpc:ModifyVRouterAttribute	acs:vpc:$regionid:$accountid:vrouter/$vrouterid
vpc:CreateVSwitch	acs:vpc:$regionid:$accountid:vswitch/*
	acs:vpc:$regionid:$accountid:vpc/$vpcid
vpc:DeleteVSwitch	acs:vpc:$regionid:$accountid:vswitch/$vswitchid
vpc:DescribeVSwitches	acs:vpc:$regionid:$accountid:vswitch/*
	"vpc:Vpc":"acs:vpc:$regionid:$accountid:vpc/$vpcid"
vpc:ModifyVSwitchAttribute	acs:vpc:$regionid:$accountid:vswitch/$vswitchid
vpc:CreateRouteEntry	acs:vpc:$regionid:$accountid:routetable/$routetableid
vpc:DeleteRouteEntry	acs:vpc:$regionid:$accountid:routetable/$routetableid
vpc:DescribeRouteTables	acs:vpc:$regionid:$accountid:routetable/*
	"vpc:VRouter":"acs:vpc$regionid:$accountid:vrouter/$vrouterid"
vpc:AllocateEipAddress	acs:vpc:$regionid:$accountid:eip/*
	acs:vpc:$regionid:$accountid:eip/*

Operation	ARN format
vpc:AssociateEipAddres	Bind an ECS instance acs:vpc:$regionid:$accountid:eip/$allocationid acs:ecs:$regionid:$accountid:instance/$instanceid
vpc:DescribeEipAddresses	acs:vpc:$regionid:$accountid:eip/*
vpc:UnassociateEipAddress	Bind an ECS instance acs:vpc:$regionid:$accountid:eip/$allocationid acs:ecs:$regionid:$accountid:instance/$instanceid
vpc:ReleaseEipAddress	acs:vpc:$regionid:$accountid:eip/$allocationid
vpc:DescribeEipMonitorData	acs:vpc:$regionid:$accountid:eip/$allocationid acs:ecs:$regionid:$accountid:instance/$instanceid
vpc:CreateNatGateway	acs:vpc:$regionid:$accountid:natgateway/*
vpc:DescribeNatGateways	acs:vpc:$regionid:$accountid:natgateway/$natgatewayid acs:vpc:$regionid:$accountid:natgateway/*
vpc:ModifyNatGatewaySpec	acs:vpc:$regionid:$accountid:natgateway/$natgatewayid
vpc:ModifyNatGatewayAttribute	acs:vpc:$regionid:$accountid:natgateway/$natgatewayid acs:ecs:$regionid:$accountid:instance/$instanceid
vpc:DeleteNatGateway	acs:vpc:$regionid:$accountid:natgateway/$natgatewayid acs:ecs:$regionid:$accountid:instance/$instanceid
vpc:CreateBandwidthPackage	acs:vpc:$regionid:$accountid:bandwidthpackage/*
vpc:DescribeBandwidthPackages	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid acs:vpc:$regionid:$accountid:bandwidthpackage/*
vpc:ModifyBandwidthPackageSpec	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid

Operation	ARN format
vpc:ModifyBandwidthPackageAttribute	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
vpc:AddBandwidthPackageIps	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
vpc:RemoveBandwidthPackageIps	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
vpc:DeleteBandwidthPackage	acs:vpc:$regionid:$accountid:bandwidthpackage/$bandwidthpackageid
vpc:CreateForwardEntry	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
vpc:DeleteForwardEntry	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
vpc:ModifyForwardEntry	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
vpc:DescribeForwardTableEntries	acs:vpc:$regionid:$accountid:forwardtable/$forwardtableid
vpc:CreateSnatEntry	acs:vpc:$regionid:$accountid:snattable/*
vpc:ModifySnatEntry	acs:vpc:$regionid:$accountid:snattable/$snattableid
vpc:DescribeSnatTableEntries	acs:vpc:$regionid:$accountid:snattable/$snattableid
vpc:DeleteSnatEntry	acs:vpc:$regionid:$accountid:snattable/$snattableid

2.14.1.4. Common parameters

Common request parameters

Common request parameters are request parameters that you must use when you call each API.

Common request parameters

Name	Type	Required	Description
Format	String	No	The format of the response. Valid values: *JSON (default) / XML*
Version	String	Yes	The API version in the format of `YYYY-MM-DD`. Valid value: *2016-04-28*

Name	Type	Required	Description
AccessKeyId	String	Yes	The AccessKey ID that you use to call an API.
Signature	String	Yes	The signature result string.
SignatureMethod	String	Yes	The algorithm used to create the request signature. Valid value: *HMAC-SHA1*
Timestamp	String	Yes	The timestamp of the request. The timestamp uses UTC and it complies with the ISO 8601 standard. Its format is `YYYY-MM-DDThh:mm:ssZ`. For example, 20:00:00 on January 10, 2013 in China Standard Time (UTC +8) is written as 2013-01-10T12:00:00Z.
SignatureVersion	String	Yes	The version of the signature algorithm. Valid value: 1.0
SignatureNonce	String	Yes	A unique random number that is used to prevent network replay attacks. You must use different random numbers for different requests.

Example

```
http://vpc.example.com/?Action=DescribeVpcs
&Timestamp=2016-02-23T12:46:24Z
&Format=XML
&AccessKeyId=testid
&SignatureMethod=HMAC-SHA1
&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf
&Version=2016-04-28
&SignatureVersion=1.0
```

Common response parameters

API responses use a unified format. 2xx HTTP status codes indicate a successful invocation. 4xx or 5xx HTTP status codes indicate a failed invocation. The responses can be returned in JSON or XML format. The XML format is used by default. You can specify the format when calling an API.

Each time you send a request to call an API, the system returns a unique identifier RequestId, regardless of whether the invocation is successful or not.

- XML format

```
<? xml version="1.0" encoding="utf-8"? >
    <!—Result root node-->
    <API name+Response>
    <!—Returned request tag-->
    <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
    <!—Returned results-->
    </API name+Response>
```

- JSON format

```
{
    "RequestId":"4C467B38-3910-447D-87BC-AC049166F216",
    /*Returned results*/
 }
```

2.14.1.5. VPC

2.14.1.5.1. CreateVpc

You can call this operation to create a VPC in a specified region.

When you call this operation, take note of the following items:

- You must specify the IP address range of the VPC in the form of a CIDR block. You can use the standard private IP address ranges and their subsets as the IP address range of the VPC. The standard IP address ranges include 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. The allowed block size is between a /24 netmask and a /8 netmask. The default IP address range is 172.16.0.0/12.
- The CIDR block cannot be modified after the VPC is created.
- Each VPC can contain a maximum of 15,000 cloud instances.
- A VRouter and a routing table are automatically created after a VPC is created.
- A maximum of three client-side CIDR blocks can be added to a VPC. If a client-side CIDR block is a subset of another client-side CIDR block, the one with the shorter netmask takes effect. For example, if there are two CIDR blocks 10.0.0.0/8 and 10.1.0.0/16, only 10.0.0.0/8 takes effect.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateVpc*.

Parameter	Type	Required	Description
RegionId	String	Yes	The region ID of the VPC. You can call the DescribeRegions operation to query the latest region list.
CidrBlock	String	No	The IP address range of the VPC in CIDR block form. The following IP address ranges and their subsets can be used: • *10.0.0.0/8* • *172.16.0.0/12* (default) • *192.168.0.0/16*
VpcName	String	No	The name of the VPC. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the VPC. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.
UserCidr	String	No	The client-side CIDR block. Separate multiple CIDR blocks with commas (,). You can configure a maximum of three CIDR blocks.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
VpcId	String	The ID of the VPC.
VRouterId	String	The ID of the VRouter.

Parameter	Type	Description
RouteTableId	String	The ID of the routing table.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateVpc
&RegionId=cn-hangzhou
&CidrBlock=10.10.0.0/24
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
 <CreateVpcResponse>
        <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
        <RouteTableId>vtb-bp145q7glnuzdxxxxxxxx</RouteTableId>
        <VRouterId>vrt-bp1lhl0taikrtxxxxxxxx</VRouterId>
        <VpcId>vpc-bp15zckdt37xxxxxxxx</VpcId>
</CreateVpcResponse>
```

- JSON format

```
{
    "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0",
    "RouteTableId": "vtb-bp145q7glnuzdxxxxxxxx",
    "VRouterId": "vrt-bp1lhl0taikrtxxxxxxxx",
    "VpcId": "vpc-bp15zckdt37pqxxxxxxxx"
 }
```

2.14.1.5.2. DeleteVpc

You can call this operation to delete a VPC.

When you call this operation, make sure that the following requirements are met:

- Before you delete a VPC, ensure that you have released or removed all resources in the VPC, such as VSwitches, cloud instances, and router interfaces.
- Only VPCs in the Available state can be deleted.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteVpc*.
VpcId	String	Yes	The ID of the VPC to delete.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteVpc
&VpcId=vpc-25eq58pl3xxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteVpcResponse>
   <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
 </DeleteVpcResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.5.3. DescribeVpcs

You can call this operation to query created VPCs in a specified region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVpcs*.

Parameter	Type	Required	Description
RegionId	String	No	The region ID of the VPC. You can call the DescribeRegions operation to query the latest region list.
VpcId	String	No	The ID of the VPC. A maximum of 20 VPC IDs can be specified. You can separate multiple VPC IDs with commas (,).
IsDefault	Boolean	No	Specifies whether to query the default VPC in the specified region. Valid values: • *true*: (default) All VPCs in the specified region are queried. • *false*: The default VPC is not queried.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
Vpcs	List	The details about the VPC. For more information, see the Vpcs list.

Vpcs list

Parameter	Type	Description
VpcId	String	The ID of the VPC.
RegionId	String	The region ID of the VPC.

Parameter	Type	Description
Status	String	The status of the VPC. Valid values: • *Pending*: The VPC is being configured. • *Available*: The VPC is available.
VpcName	String	The name of the VPC.
VSwitchIds	String	The list of VSwitches in the VPC.
CidrBlock	String	The CIDR block of the VPC.
VRouterId	String	The ID of the VRouter.
Description	String	The description of the VPC.
CreationTime	String	The time when the VPC was created.
IsDefault	Boolean	Indicates whether the VPC is the default VPC in the region.
UserCidrs	String	The list of client-side CIDR blocks.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeVpcs
&RegionId=cn-hangzhou
&CidrBlock=10.10.0.0/24
&Common request parameters
```

Sample responses

- XML format

```
<<? xml version="1.0" encoding="UTF-8" ? >
<DescribeVpcsResponse>
  <PageNumber>1</PageNumber>
  <Vpcs>
    <Vpc>
      <VpcName>vpc1</VpcName>
      <Description></Description>
      <IsDefault>false</IsDefault>
      <ResourceGroupId>rg-acfmxazb4xxxxxxxx</ResourceGroupId>
      <UserCidrs></UserCidrs>
      <NatGatewayIds></NatGatewayIds>
      <RouterTableIds>
        <RouterTableIds>vtb-bp145q7glnuzdxxxxxxxx</RouterTableIds>
      </RouterTableIds>
      <VpcId>vpc-bp15zckdt37pqxxxxxxxx</VpcId>
      <VRouterId>vrt-bp1lhl0taikrtxxxxxxxx</VRouterId>
      <CreationTime>2018-04-18T15:02:37Z</CreationTime>
      <Status>Available</Status>
      <CidrBlock>10.0.0.0/24</CidrBlock>
      <VSwitchIds></VSwitchIds>
      <RegionId>cn-hangzhou</RegionId>
    </Vpc>
  </Vpcs>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>9B941224-B647-4644-A746-641906D6B954</RequestId>
</DescribeVpcsResponse>
```

- JSON format

```
{
  "PageNumber": 1,
  "Vpcs": {
    "Vpc": [
      {
        "VpcName": "vpc1",
        "Description": "",
        "IsDefault": false,
        "ResourceGroupId": "rg-acfmxazbxxxxxxxx",
        "UserCidrs": {
          "UserCidr": [ ]
        },
        "NatGatewayIds": {
          "NatGatewayIds": [ ]
        },
        "RouterTableIds": {
          "RouterTableIds": [
            "vtb-bp145q7glnuzdxxxxxxxx"
          ]
        },
        "VpcId": "vpc-bp15zckdt37pqxxxxxxxx",
        "VRouterId": "vrt-bp1lhl0taikrxxxxxxxx",
        "CreationTime": "2018-04-18T15:02:37Z",
        "Status": "Available",
        "CidrBlock": "10.0.0.0/24",
        "VSwitchIds": {
          "VSwitchId": [ ]
        },
        "RegionId": "cn-hangzhou"
      }
    ]
  },
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "9B941224-B647-4644-A746-641906D6B954"
}
```


2.14.1.5.4. ModifyVpcAttribute

You can call this operation to modify the name and description of a VPC.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyVpcAttribute*.
VpcId	String	Yes	The ID of the VPC.
VpcName	String	No	The name of the VPC. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the VPC. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyVpcAttribute
&VpcId=vpc-257gq642nxxxxxxxx
&VpcName=Vpc02
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyVpcAttributeResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</ModifyVpcAttributeResponse>
```

- JSON format

```
{
    "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.5.5. DescribeVpcAttribute

You can call this operation to query the configurations of a VPC.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVpcAttribute*.
VpcId	String	Yes	The ID of the VPC to query.
RegionId	String	Yes	The region ID of the VPC.
IsDefault	Boolean	No	Specifies whether the VPC is the default VPC. Valid values: • *false*: The VPC is not the default VPC. • *true*: The VPC is the default VPC.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
VpcName	String	The name of the VPC.
Description	String	The description of the VPC.
IsDefault	Boolean	Indicates whether the VPC is the default VPC.
VRouterId	String	The ID of the VRouter.
VpcId	String	The ID of the VPC.
CidrBlock	String	The CIDR block of the VPC.
VSwitchIds	List	The list of VSwitches in the VPC.
Status	String	The status of the VPC.
CreationTime	String	The time when the VPC was created.

Parameter	Type	Description
CloudResources	List	The list of resources in the VPC.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeVpcAttribute
&VpcId=vpc-bp13cwaie5zzbxxxxxxxx
&RegionId=cn-hangzhou
&CommonParameters
```

Sample responses

XML format

```
<? xml version="1.0" encoding="utf-8"? >
</DescribeVpcAttributeResponse>
  <VpcName>k8s_vpc</VpcName>
  <Description></Description>
  <IsDefault>false</IsDefault>
  <VRouterId>vrt-bp19a5yibawcxxxxxxxxx
</VRouterId>
  <VpcId>vpc-bp13cwaie5zzbxxxxxxxx
</VpcId>
  <CreationTime>2018-04-20T03:02:33Z</CreationTime>
  <CidrBlock>192.168.0.0/16</CidrBlock>
  <Status>Available</Status>
  <VSwitchIds>
    <VSwitchId>vsw-bp1oisthjafqqxxxxxxxx
</VSwitchId>
  </VSwitchIds>
  <RequestId>3FEECC52-51EC-4F0E-B2D4-DA181D50F5B6</RequestId>
  <RegionId>cn-hangzhou</RegionId>
  <CloudResources>
    <CloudResourceSetType>
      <ResourceType>NatGateway</ResourceType>
      <ResourceCount>1</ResourceCount>
    </CloudResourceSetType>
    <CloudResourceSetType>
      <ResourceType>VSwitch</ResourceType>
      <ResourceCount>1</ResourceCount>
    </CloudResourceSetType>
    <CloudResourceSetType>
      <ResourceType>VRouter</ResourceType>
      <ResourceCount>1</ResourceCount>
    </CloudResourceSetType>
    <CloudResourceSetType>
      <ResourceType>RouteTable</ResourceType>
      <ResourceCount>1</ResourceCount>
    </CloudResourceSetType>
  </CloudResources>
</DescribeVpcAttributeResponse>
```

JSON format

```
{
   "VpcName": "k8s_vpc",
   "Description": "",
   "IsDefault": false,
   "VRouterId": "vrt-bp19a5yibawcxxxxxxxxx
",
   "VpcId": "vpc-bp13cwaie5zzbxxxxxxxx
",
   "CreationTime": "2018-04-20T03:02:33Z",
   "CidrBlock": "192.168.0.0/16",
   "Status": "Available",
   "VSwitchIds": {
      "VSwitchId": [
         "vsw-bp1oisthjafqqxxxxxxxx
"
      ]
   },
   "RequestId": "3FEECC52-51EC-4F0E-B2D4-DA181D50F5B6",
   "RegionId": "cn-hangzhou",
   "CloudResources": {
      "CloudResourceSetType": [
         {
            "ResourceType": "NatGateway",
            "ResourceCount": 1
         },
         {
            "ResourceType": "VSwitch",
            "ResourceCount": 1
         },
         {
            "ResourceType": "VRouter",
            "ResourceCount": 1
         },
         {
            "ResourceType": "RouteTable",
            "ResourceCount": 1
         }
      ]
   }
}
```

2.14.1.6. VRouter

2.14.1.6.1. DescribeVRouters

You can call this operation to query VRouters in a specified region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVRouters*.
RegionId	String	No	The region ID of the VPC. You can call the DescribeRegions operation to query the latest region list.
VRouterId	String	No	The ID of the VRouter.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
VRouters	JSON string	The details about the VRouter.
Vpcs elements		
VRouterId	String	The ID of the VRouter.
RegionId	String	The region ID of the VPC.
VpcId	String	The ID of the VPC to which the VRouter belongs.
RouteTableIds	String	The ID of the routing table for the VRouter.

Parameter	Type	Description
VRouterName	String	The name of the VRouter.
Description	String	The description of the VRouter.
CreationTime	String	The time when the VRouter was created.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeVRouters
&RegionId=us-west-1
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeVRoutersResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <VRouters>
    <VRouter>
      <VRouterName></VRouterName>
      <RouteTableIds>
        <RouteTableId>vtb-rj9ybe3y0u41mxxxxxxxx</RouteTableId>
      </RouteTableIds>
      <CreationTime>2018-03-22T07:46:20Z</CreationTime>
      <Description></Description>
      <RegionId>us-west-1</RegionId>
      <VRouterId>vrt-rj98khsezfqpjxxxxxxxx</VRouterId>
      <VpcId>vpc-rj905wotv6y03xxxxxxxx</VpcId>
    </VRouter>
  </VRouters>
  <PageSize>10</PageSize>
  <RequestId>CB2793A8-845F-444C-8E93-76F1BBDF9C78</RequestId>
</DescribeVRoutersResponse>
```

- JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "VRouters": {
    "VRouter": [
      {
        "VRouterName": "",
        "RouteTableIds": {
          "RouteTableId": [
            "vtb-rj9ybe3y0u41mxxxxxxxx"
          ]
        },
        "CreationTime": "2018-03-22T07:46:20Z",
        "Description": "",
        "RegionId": "us-west-1",
        "VRouterId": "vrt-rj98khsezfqpjxxxxxxxx",
        "VpcId": "vpc-rj905wotv6y03xxxxxxxx"
      }
    ]
  },
  "PageSize": 10,
  "RequestId": "CB2793A8-845F-444C-8E93-76F1BBDF9C78"
}
```


2.14.1.6.2. ModifyVRouterAttribute

You can call this operation to modify the name and description of a VRouter.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyVRouterAttribute*.
VRouterId	String	Yes	The ID of the VRouter.
VRouterName	String	No	The name of the VRouter. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.

Parameter	Type	Required	Description
Description	String	No	The description of the VRouter. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyVRouterAttribute
&VRouterId=vrt-25bezkxxxxxxxx
&VRouterName=VRouter2
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyVRouterAttributeResponse>
  <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</ModifyVRouterAttributeResponse>
```

- JSON format

```
{
   "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0",
   "RouteTableId": "vtb-bp145q7glnuzdxxxxxxxx
",
   "VRouterId": "vrt-bp1lhl0taikrtxxxxxxxx
",
    "VpcId": "vpc-bp15zckdt37pqxxxxxxxx
"
}
```

2.14.1.7. VSwitch

2.14.1.7.1. CreateVSwitch

You can call this operation to create a VSwitch in a VPC.

When you call this operation, take note of the following items:

- A maximum of 24 VSwitches can be created in a VPC.
- The first IP address and last three IP addresses of each VSwitch are reserved. For example, if the CIDR block of a VSwitch is 192.168.1.0/24, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved.
- The number of cloud instances under a VSwitch cannot exceed the remaining capacity of the VPC. The remaining capacity is the difference between 15,000 and the current number of cloud instances.
- A cloud instance can belong to only one VSwitch.
- VSwitches do not support broadcasting or multicasting. After a VSwitch is created, its CIDR block cannot be modified.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateVSwitch*.
ZoneId	String	Yes	The ID of the zone to which the VSwitch belongs. You can call the DescribeZones operation to query the latest zone list.
CidrBlock	String	Yes	The CIDR block of the VSwitch. It must meet the following requirements: • The CIDR block size of a VSwitch must be between a /29 netmask and a /16 netmask. • The CIDR block of a VSwitch must be within the range of the CIDR block of the VPC to which the VSwitch belongs. • The CIDR block of a VSwitch cannot be the same as the destination CIDR block in the route entry of the VPC. However, it can be a subset of the destination CIDR block. • If the CIDR blocks of your VSwitch and VPC are the same, only one VSwitch can be created for the VPC.
VpcId	String	Yes	The ID of the VPC to which the VSwitch belongs.

Parameter	Type	Required	Description
VSwitchName	String	No	The name of the VSwitch. The name must be 2 to 128 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the VSwitch. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
VSwitchId	String	The ID of the VSwitch.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateVSwitch
&CidrBlock=172.16.1.0/24
&VpcId=vpc-257gq64xxxxxxxx
&ZoneId=cn-beijing-a
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CreateVSwitchResponse>
   <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
   <VSwitchId>vsw-25nauexxxxxxxx
</VSwitchId>
</CreateVSwitchResponse>
```

- JSON format

```
{
   "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0",
   "VSwitchId": "vsw-25nauexxxxxxxx
"
}
```

2.14.1.7.2. DeleteVSwitch

You can call this operation to delete a VSwitch.

When you call this operation, make sure that the following requirements are met:

- Before you delete a VSwitch, ensure that you have released or removed all resources in the VSwitch, such as cloud instances and router interfaces.
- Only VSwitches in the Available state can be deleted.
- You cannot delete a VSwitch from a VPC in which a VSwitch or route entry is being created or deleted.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteVSwitch*.
VSwitchId	String	Yes	The ID of the VSwitch to delete.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteVSwitch
&VSwitchId=vsw-25naue4xxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteVSwitchResponse>
   <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</DeleteVSwitchResponse>
```

- JSON format

```
{
   "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
 }
```

2.14.1.7.3. ModifyVSwitchAttribute

You can call this operation to modify the name and description of a VSwitch.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyVSwitchAttribute*.
VSwitchId	String	Yes	The ID of the VSwitch.
VSwitchName	String	No	The name of the VSwitch. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the VSwitch. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyVSwitchAttribute
&VSwitchId=vsw-25nauexxxxxxxx
&VSwitchName=VS02
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyVSwitchAttributeResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</ModifyVSwitchAttributeResponse>
```

- JSON format

```
{
 "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.7.4. DescribeVSwitches

You can call this operation to query created VSwitches.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVSwitches*.
RegionId	String	Yes	The region ID of the VPC to which the VSwitch belongs. You can call the DescribeRegions operation to query the latest region list.
VpcId	String	No	The ID of the VPC.

Parameter	Type	Required	Description
ZoneId	String	No	The ID of the zone to which the VSwitch belongs. You can call the DescribeZones operation to query the latest zone list.
VSwitchId	String	No	The ID of the VSwitch.
IsDefault	Boolean	No	Specifies whether to query the default VSwitch in the specified region. Valid values: • *true*: (default) All VSwitches in the specified region are queried. • *false*: The default VSwitch is not queried.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
VSwitches	JSON string	The details about the VSwitch.
VSwitches elements		
VpcId	String	The ID of the VPC to which the VSwitch belongs.
VSwitchId	String	The ID of the VSwitch.
Status	String	The status of the VSwitch. Valid values: • *Pending*: The VSwitch is being configured. • *Available*: The VSwitch is available.
CidrBlock	String	The CIDR block of the VSwitch.
ZoneId	String	The zone to which the VSwitch belongs.

Parameter	Type	Description
AvailableIpAddressCount	Integer	The number of available IP addresses in the VSwitch.
VSwitchName	String	The name of the VSwitch.
Description	String	The description of the VSwitch.
CreationTime	String	The time when the VSwitch was created.
IsDefault	Boolean	Indicates whether the VSwitch is the default VSwitch in the zone.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeVSwitches
&VSwitchId=vsw-25eq58xxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeVSwitchesResponse>
  <RequestId>9A572171-4E27-40D1-BD36-D26C9E71E29E</RequestId>
  <VSwitches>
    <VSwitch>
      <VSwitchId>vsw-25b7pvxxxxxxxx</VSwitchId>
      <Status>Available</Status>
      <CidrBlock>172.16.1.0/24</CidrBlock>
      <ZoneId>cn-beijing-a</ZoneId>
      <AvailableIpAddressCount>246</AvailableIpAddressCount>
      <VpcId>vpc-257gq64xxxxxxxx</VpcId>
      <Description></Description>
      <VSwitchName></VSwitchName>
      <CreationTime> 2014-10-29T15:21:02Z </CreationTime>
    </VSwitch>
  </VSwitches>
</DescribeVSwitchesResponse>
```

- JSON format

```
{
  "PageNumber": 1,
  "PageSize": 10,
  "RequestId": "9A572171-4E27-40D1-BD36-D26C9E71E29E",
  "TotalCount": 1,
  "VSwitches": {
    "VSwitch": [
      {
        "AvailableIpAddressCount": 246,
        "CidrBlock": "172.16.1.0/24",
        "CreationTime": "2014-10-29T15:21:02Z",
        "Description": "",
        "Status": "Available",
        "VSwitchId": "vsw-25b7pvxxxxxxxx",
        "VSwitchName": "",
        "VpcId": "vpc-257gq64xxxxxxxx",
        "ZoneId": "cn-beijing-a"
      }
    ]
  }
}
```


2.14.1.7.5. DescribeVSwitchAttributes

You can call this operation to query the configurations of a VSwitch.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVSwitchAttributes*.
VSwitchId	String	Yes	The ID of the VSwitch to query.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
RouteTable	List	The routing table information of the VSwitch.
Description	String	The description of the VSwitch.

Parameter	Type	Description
IsDefault	Boolean	Indicates whether the VSwitch is the default VSwitch.
ZoneId	String	The zone to which the VSwitch belongs.
AvailableIpAddressCount	Integer	The number of available IP addresses.
VSwitchId	String	The ID of the VSwitch.
VpcId	String	The ID of the VPC to which the VSwitch belongs.
CidrBlock	String	The CIDR block of the VSwitch.
Status	String	The status of the VSwitch.
VSwitchName	String	The name of the VSwitch.
CreationTime	String	The time when the VSwitch was created.
CloudResources	String	The cloud resources under the VSwitch.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeVSwitchAttributes
&Common request parameters
```

Sample responses

XML format

```
<? xml version="1.0" encoding="utf-8"? >
</DescribeVSwitchAttributesResponse>
  <RouteTable>
    <RouteTableId>vtb-bp1vbpghqvkhxxxxxxxx</RouteTableId>
    <RouteTableType>System</RouteTableType>
  </RouteTable>
  <Description></Description>
  <IsDefault>false</IsDefault>
  <AvailableIpAddressCount>65532</AvailableIpAddressCount>
  <ZoneId>cn-hangzhou-e</ZoneId>
  <VSwitchId>vsw-bp1pkt1fba8e8xxxxxxxx</VSwitchId>
  <VpcId>vpc-bp1kcm36tevkpxxxxxxxx</VpcId>
  <CreationTime>2018-05-11T02:45:46Z</CreationTime>
  <CidrBlock>192.168.0.0/16</CidrBlock>
  <Status>Available</Status>
  <RequestId>55BAAD8E-F1FA-4B46-BF6B-DF1E51555F52</RequestId>
  <VSwitchName>HBase_verification</VSwitchName>
  <CloudResources></CloudResources>
</DescribeVSwitchAttributesResponse>
```

JSON format

```
{
  "RouteTable": {
    "RouteTableId": "vtb-bp1vbpghqvkhbxxxxxxxxo",
    "RouteTableType": "System"
  },
  "Description": "",
  "IsDefault": false,
  "AvailableIpAddressCount": 65532,
  "ZoneId": "cn-hangzhou-e",
  "VSwitchId": "vsw-bp1pkt1fba8e8xxxxxxxx",
  "VpcId": "vpc-bp1kcm36tevkpxxxxxxxx",
  "CreationTime": "2018-05-11T02:45:46Z",
  "CidrBlock": "192.168.0.0/16",
  "Status": "Available",
  "RequestId": "55BAAD8E-F1FA-4B46-BF6B-DF1E51555F52",
  "VSwitchName": "HBase_verification",
  "CloudResources": {
    "CloudResourceSetType": [ ]
  }
}
```


2.14.1.8. Routing table

2.14.1.8.1. CreateRouteEntry

You can call this operation to create route entries in a VRouter or VBR.

When you call this operation to create route entries in a VRouter, make sure that the following requirements are met:

- A routing table can contain a maximum of 48 custom route entries.
- The destination CIDR block (DestinationCidrBlock) of a custom route entry and the CIDR block of a VSwitch in the VPC cannot be the same as each other nor a subset of each other.
- The destination CIDR block (DestinationCidrBlock) of a custom route entry cannot be 100.64.0.0/10 or a subset of 100.64.0.0/10.
- The destination CIDR blocks (DestinationCidrBlock) of route entries in the same routing table cannot be the same.
- If the specified destination CIDR block (DestinationCidrBlock) is an IP address, the /32 netmask is used.
- Multiple custom route entries can be destined for the same next hop (NextHopId).
- The next hop (NextHopId) of the custom route entry must belong to the same VPC as the routing table.
- ECMP route entries can be configured through the NextHopList parameter.

- When adding a normal custom route entry (non-ECMP route entry), you must specify DestinationCidrBlock, NextHopType, and NextHopId, and you cannot specify NextHopList.
- When adding an ECMP route entry, you must specify DestinationCidrBlock and NextHopList, and you cannot specify NextHopType and NextHopId.

When you call this operation to create route entries in a VBR, make sure that the following requirements are met:

- A routing table can contain a maximum of 48 custom route entries.
- The NextHopList parameter is not supported.
- The destination CIDR block (DestinationCidrBlock) of a custom route entry cannot be 100.64.0.0/10 or a subset of 100.64.0.0/10.
- The destination CIDR blocks (DestinationCidrBlock) of route entries in the same routing table cannot be the same.
- If the specified destination CIDR block (DestinationCidrBlock) is an IP address, the /32 netmask is used.
- Multiple custom route entries can be destined for the same next hop (NextHopId).
- The next hop (NextHopId) of a custom route entry must be a router interface associated with the VBR.
- Route entries can be created only when the VBR is in the Active state and the physical connection corresponding to the VBR is in the Enabled state. Route entries cannot be created if the physical connection has overdue payments.
- When adding a normal custom route entry (non-ECMP route entry), you must specify DestinationCidrBlock, NextHopType, and NextHopId, and you cannot specify NEXTHopList.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateRouteEntry*.
RouteTableId	String	Yes	The ID of the routing table.
DestinationCidrBlock	String	Yes	The destination CIDR block of the custom route entry, which must meet the following requirements: • The destination CIDR block of a route entry cannot be 100.64.0.0/10 or a subset of 100.64.0.0/10. • The destination CIDR blocks of route entries in the same routing table cannot be the same. • If the specified destination CIDR block is an IP address, the /32 netmask is used.

Parameter	Type	Required	Description
NextHopType	String	No	The type of the next hop. Valid values: • *Instance*: (default) The next hop is an ECS instance. • *RouterInterface*: The next hop is a router interface. Note You must specify this parameter when creating normal route entries (non-ECMP route entries).
NextHopId	String	No	The ID of the next-hop instance. The next-hop instance must be in the VPC or VBR to which the routing table belongs. Note You must specify this parameter when creating normal route entries (non-ECMP route entries).
NextHopList	String	No	The list of next hops. The next hops must meet the following requirements: • ECMP route entries are only supported for the VPC routing table. • The number of next hops must be 2, 3, or 4. • The next hops must be VRouter interfaces that are destined for VBRs. Note You must specify this parameter when creating ECMP route entries.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.
NextHopList elements Note You must specify this parameter when creating ECMP route entries.			

Parameter	Type	Required	Description
NextHopType	String	No	The type of the next hop. Valid values: • *Instance*: (default) The next hop is an ECS instance. • *RouterInterface*: The next hop is a router interface.
NextHopId	String	No	The ID of the next-hop instance.
Enabled	Integer	No	Specifies whether the next-hop is available. • *1*: The next hop is available. • *0*: The next hop is unavailable.
Weight	Integer	No	The routing weight of the next hop.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateRouteEntry
&VpcId=vpc-257gq6xxxxxxxx
&RouteTableId=vrt-5citwfxxxxxxxx
&DestinationCidrBlock=0.0.0.0/0
&NextHopId=i-25skktxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CreateRouteEntryResponse>
   <RequestId>12D086F6-8F31-4658-84C1-006DED011A85</RequestId>
</CreateRouteEntryResponse>
```

- JSON format

```
{
   "RequestId": "12D086F6-8F31-4658-84C1-006DED011A85"
}
```

2.14.1.8.2. DeleteRouteEntry

You can call this operation to delete route entries from the routing table of a VRouter or VBR.

When you call this operation, make sure that the following requirements are met:

- Only route entries in the Available state can be deleted.
- You cannot delete route entries from a VPC in which a VSwitch or route entry is being created or deleted.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteRouteEntry*.
RouteTableId	String	Yes	The ID of the routing table to which the route entry belongs.
DestinationCidrBlock	String	Yes	The destination CIDR block of the route entry.
NextHopId	String	No	The ID of the next-hop instance. You must specify this parameter when deleting normal route entries (non-ECMP route entries).
NextHopList	String	No	The list of next hops. You must specify this parameter when deleting ECMP route entries.

NextHopList list

Parameter	Type	Required	Description
NextHopType	String	No	The type of the next hop. Valid values: • *Instance*: (default) The next hop is an ECS instance. • *RouterInterface*: The next hop is a router interface.
NextHopId	String	No	The ID of the next-hop instance.
Enabled	Integer	No	Specifies whether the next-hop is available. • *1*: The next hop is available. • *0*: The next hop is unavailable.
Weight	Integer	No	The routing weight of the next hop.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteRouteEntry
&RouterTableId=vtb-25vtxlxxxxxxxx
&DestinationCidrBlock=192.168.1.0/24
&NextHopId=i-25skktxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteRouteEntryResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</DeleteRouteEntryResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.8.3. DescribeRouteTables

You can call this operation to query route entries in a routing table.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeRouteTables*.
RouterType	String	No	The type of the router to which the routing table belongs. Valid values: • *VRouter* • *VBR*

Parameter	Type	Required	Description
RouterId	String	No	The ID of the VRouter or VBR to which the routing table belongs.
VRouterId	String	No	The ID of the VRouter to which the routing table belongs. The value of the RouterType parameter is set to *VRouter* automatically when this parameter is specified.
RouteTableId	String	No	The ID of the routing table.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
RouteTables	List	The details about the routing table. For more information, see the RouteTables list.

RouteTables list

Parameter	Type	Description
RouterType	String	The type of the router to which the routing table belongs. Valid values: • *VRouter* • *VBR*
RouterId	String	The ID of the VRouter or VBR to which the routing table belongs.
VRouterId	String	The ID of the VRouter.
RouteTableId	String	The ID of the routing table.

Parameter	Type	Description
RouteTableType	String	The type of the routing table.
CreationTime	String	The time when the routing table was created.
RouteEntrys	List	The details about the route entry. For more information, see the RouteEntrys list.

RouteEntrys list

Parameter	Type	Description
Type	String	The type of the route entry. Valid value: • *Custom*: custom route entry
RouteTableId	String	The ID of the routing table to which the route entry belongs.
DestinationCidrBlock	String	The destination CIDR block of the route entry.
NextHopType	String	The type of the next hop.
InstanceId	String	The ID of the next-hop instance.
Status	String	The status of the route entry. Valid values: • *Pending*: The route entry is being configured. • *Available*: The route entry is available. • *Modifying*: The route entry is being modified.
RouterId	String	The ID of the VRouter or VBR to which the routing table belongs.
NextHops	List	The next-hop list of ECMP routes. For more information, see the NextHops list.

NextHops list

Parameter	Type	Description
NextHopType	String	The type of the next hop. Valid values: • *Instance*: (default) The next hop is an ECS instance. *RouterInterface*: The next hop is a router interface.
NextHopId	String	The ID of the next-hop instance.

Parameter	Type	Description
Enabled	Integer	Indicates whether the next-hop is available. • *1*: The next hop is available. • *0*: The next hop is unavailable.
Weight	Integer	The routing weight of the next hop.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeRouteTables
&RouteTableId=vtb-2zevpmy9th8cxmwtarqg4
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeRouteTablesResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>DC668356-BCB4-42FD-9BC3-FA2B2E04B634</RequestId>
  <RouteTables>
    <RouteTable>
      <CreationTime>2017-08-22T10:40:25Z</CreationTime>
      <RouteEntrys>
        <RouteEntry>
          <NextHops></NextHops>
          <Status>Available</Status>
          <Type>System</Type>
          <InstanceId></InstanceId>
          <NextHopType>service</NextHopType>
          <RouteTableId>vtb-2zevpmy9th8cxxxxxxxxx</RouteTableId>
          <DestinationCidrBlock>100.64.0.0/10</DestinationCidrBlock>
        </RouteEntry>
      </RouteEntrys>
      <RouteTableId>vtb-2zevpmy9th8cxxxxxxxxx</RouteTableId>
      <RouteTableType>System</RouteTableType>
      <VRouterId>vrt-2zefso23vmu6xxxxxxxxx</VRouterId>
    </RouteTable>
  </RouteTables>
</DescribeRouteTablesResponse>
```

- JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "DC668356-BCB4-42FD-9BC3-FA2B2E04B634",
  "RouteTables": {
    "RouteTable": [
      {
        "CreationTime": "2017-08-22T10:40:25Z",
        "RouteEntrys": {
          "RouteEntry": [
            {
              "NextHops": {
                "NextHop": [ ]
              },
              "Status": "Available",
              "Type": "System",
              "InstanceId": "",
              "NextHopType": "service",
              "RouteTableId": "vtb-2zevpmy9th8cxxxxxxxxx",
              "DestinationCidrBlock": "100.64.0.0/10"
            }
          ]
        },
        "RouteTableId": "vtb-2zevpmy9th8cxxxxxxxxx",
        "RouteTableType": "System",
        "VRouterId": "vrt-2zefso23vmu6xxxxxxxxx"
      }
    ]
  }
}
```


2.14.1.9. Elastic IP Address (EIP)

2.14.1.9.1. AllocateEipAddress

You can call this operation to create an Elastic IP address (EIP).

An EIP in the Available state is randomly allocated in the specified region after this operation is called. EIP supports only ICMP, TCP, and UDP at the transport layer.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *AllocateEipAddress*.
RegionId	String	Yes	The region ID of the EIP. You can call the DescribeRegions operation to query the latest region list.
Bandwidth	String	No	The peak bandwidth of the EIP. Unit: Mbit/s. Default value: *5*.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
EipAddress	String	The allocated EIP.
AllocationId	String	The ID of the EIP.

Examples

Sample requests

```
https://vpc.example.com/?Action=AllocateEipAddress
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<AllocateEipAddressResponse>
      <AllocationId>eip-25877c7xxxxxxxx</AllocationId>
      <EipAddress>123.xx.xx. 206</EipAddress>
      <RequestId>B6B9F518-60F8-4D81-9242-1207B356754D</RequestId>
</AllocateEipAddressResponse>
```

- JSON format

```
{
   "AllocationId": "eip-25877c70x",
    "EipAddress": "123.xx.xx. 206",
    "RequestId": "B6B9F518-60F8-4D81-9242-1207B356754D"
 }
```

2.14.1.9.2. AssociateEipAddress

You can call this operation to bind an EIP to a cloud instance in the same region.

When you call this operation, make sure that the following requirements are met:

- Only EIPs in the Available state can be bound.
- An EIP can only be bound to one cloud instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *AssociateEipAddress*.
AllocationId	String	Yes	The ID of the EIP.
InstanceType	String	No	The type of the cloud instance to bind. Valid value: • *EcsInstance*: (default) an ECS instance of the VPC network Only the ECS instance in the running or stopped state can be bound. After the EIP is bound, the SLB instance can forward requests from the public network.
InstanceId	String	Yes	The ID of the cloud instance to bind.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=AssociateEipAddress
&AllocationId=eip-25877cxxxxxxxx
&InstanceId=i-25skktxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<AssociateEipAddressResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</AssociateEipAddressResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.9.3. UnassociateEipAddress

You can call this operation to unbind an EIP from a cloud instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *UnassociateEipAddress*.
AllocationId	String	Yes	The ID of the EIP.
InstanceType	String	No	The type of the cloud instance to unbind. Valid value: *EcsInstance*: (default) an ECS instance of the VPC network
InstanceId	String	Yes	The ID of the cloud instance to unbind.

Parameter	Type	Required	Description

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=UnassociateEipAddress
&AllocationId=eip-25877c7xxxxxxxx
&InstanceId=i-25skktxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<UnassociateEipAddressResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</UnassociateEipAddressResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.9.4. ModifyEipAddressAttribute

You can call this operation to modify the name, description, and peak bandwidth of an EIP.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyEipAddressAttribute*.
AllocationId	String	Yes	The ID of the EIP.

Parameter	Type	Required	Description
Bandwidth	String	No	The peak bandwidth of the EIP. Unit: Mbit/s.
Name	String	No	The name of the EIP. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the EIP. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyEipAddressAttribute
&AllocationId=eip-25877c7xxxxxxxx
&Name=eip1
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyEipAddressAttributeResponse>
   <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</ModifyEipAddressAttributeResponse>
```

- JSON format

```
{
   "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
 }
```

2.14.1.9.5. ReleaseEipAddress

You can call this operation to release an EIP.

When you call this operation, make sure that the following requirements are met:

- Only EIPs in the Available state can be released.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ReleaseEipAddress*.
AllocationId	String	Yes	The ID of the EIP.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ReleaseEipAddress
&AllocationId=eip-25877c7xxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ReleaseEipAddressResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</ReleaseEipAddressResponse>
```

- JSON format

```
{
   "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
 }
```

2.14.1.9.6. DescribeEipAddresses

You can call this operation to query the EIPs that have been created for the specified region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeEipAddresses*.
RegionId	String	Yes	The region ID of the EIP. You can call the DescribeRegions operation to query the latest region list.
Status	String	No	The status of the EIP. Valid values: • Associating: The EIP is being bound to a cloud instance. • Unassociating: The EIP is being unbound from a cloud instance. • InUse: The EIP has been bound to a cloud instance. • Available: The EIP is not bound to any cloud instances.
AllocationId	String	No	The ID of the EIP.
AssociatedInstanceType	String	No	The type of the cloud instance to bind. Valid value: *EcsInstance*: (default) an ECS instance of the VPC network
AssociatedInstanceId	String	No	The ID of the cloud instance to bind.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.

Parameter	Type	Description
PageSize	String	The number of entries on each page.
EipAddresses	List	The details about the queried EIPs.

EipAddresses list

Parameter	Type	Description
RegionId	String	The region ID of the EIP.
IpAddress	String	The address of the EIP.
AllocationId	String	The ID of the EIP.
Status	String	The status of the EIP. Valid values: • Associating: The EIP is being bound to a cloud instance. • Unassociating: The EIP is being unbound from a cloud instance. • InUse: The EIP has been bound to a cloud instance. • Available: The EIP is not bound to any cloud instances.
InstanceType	String	The type of the cloud instance that the EIP is bound.
InstanceId	String	The ID of the cloud instance that the EIP is bound.
Bandwidth	String	The peak bandwidth of the EIP. Unit: Mbit/s.
InternetChargeType	String	The billing method of the EIP.
AllocationTime	String	The time when the EIP was created.
OperationLocks	String	The reason why the EIP is locked. Valid values: • financial: The EIP is locked due to overdue payments. • security: The EIP is locked due to security reasons.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeEipAddresses
&RegionId=cn-hangzhou-1
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeEipAddressesResponse>
  <RequestId>7EEF2D6B-D207-4197-AE37-01279C888757</RequestId>
  <PageNumber>1</PageNumber>
  <EipAddresses>
    <EipAddress>
      <ChargeType>PostPaid</ChargeType>
      <AllocationTime>2018-01-15T11:17:30Z</AllocationTime>
      <ResourceGroupId>rg-acfmxazb4xxxxxxxx</ResourceGroupId>
      <InstanceId></InstanceId>
      <Description></Description>
      <IpAddress>59.xx.xx. 11</IpAddress>
      <AllocationId>eip-2ze88m67qx5zxxxxx</AllocationId>
      <InternetChargeType>PayByTraffic</InternetChargeType>
      <InstanceType></InstanceType>
      <Name></Name>
      <Status>Available</Status>
      <BandwidthPackageId></BandwidthPackageId>
      <InstanceRegionId></InstanceRegionId>
      <BandwidthPackageType></BandwidthPackageType>
      <RegionId>cn-beijing</RegionId>
      <OperationLocks></OperationLocks>
      <ExpiredTime></ExpiredTime>
      <AvailableRegions>
        <AvailableRegion>cn-beijing</AvailableRegion>
      </AvailableRegions>
            <Bandwidth>1</Bandwidth>
    </EipAddress>
  </EipAddresses>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
</DescribeEipAddressesResponse>
```

- JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "DC668356-BCB4-42FD-9BC3-FA2B2E04B634",
  "RouteTables": {
    "RouteTable": [
```

```
        {
          "CreationTime": "2017-08-22T10:40:25Z",
          "RouteEntrys": {
            "RouteEntry": [
              {
                "NextHops": {
                  "NextHop": [ ]
                },
                "Status": "Available",
                "Type": "Custom",
                "InstanceId": "ri-2zeo3xzyf38rxxxxxxxx",
                "NextHopType": "RouterInterface",
                "RouteTableId": "vtb-2zevpmy9th8cxxxxxxxx",
                "DestinationCidrBlock": "10.10.0.0/24"
              },
              {
                "NextHops": {
                  "NextHop": [ ]
                },
                "Status": "Available",
                "Type": "System",
                "InstanceId": "",
                "NextHopType": "service",
                "RouteTableId": "vtb-2zevpmy9th8xxxxxxxx",
                "DestinationCidrBlock": "100.64.0.0/10"
              }
            ]
          },
          "RouteTableId": "vtb-2zevpmy9th8cxxxxxxxx",
          "RouteTableType": "System",
          "VRouterId": "vrt-2zefso23vmu6xxxxxxxx"
        }
      ]
    }
}
```


2.14.1.10. Router interface

2.14.1.10.1. ConnectRouterInterface

You can call this operation to connect the initiator router interface to the receiver router interface.

After this operation is called, the router interface enters the Connecting state. When the connection is established, the router interface enters the Active state.

When you call this operation, make sure that the following requirements are met:

- Only an initiator router interface in the Idle state can initiate a connection.
- A maximum of one pair of interconnected router interfaces can be created between any two routers.
- You cannot initiate a connection if your account contains any router interface that has overdue payments.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ConnectRouterInterface*.
RegionId	String	Yes	The region ID of the router interface. You can call the DescribeRegions operation to query the latest region list.
RouterInterfaceId	String	Yes	The ID of the initiator router interface.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ConnectRouterInterface
&RegionId=cn-hangzhou
&RouterInterfaceId=ri-sf3rxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ConnectRouterInterfaceResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</ConnectRouterInterfaceResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.10.2. DeactivateRouterInterface

You can call this operation to deactivate a router interface.

After the operation is called, the router interface enters the Deactivating state. Once deactivated, the router interface enters the Inactive state.

> **Note** You cannot deactivate a router interface that has overdue payments.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeactivateRouterInterface*.
RegionId	String	Yes	The region ID of the router interface. You can call the DescribeRegions operation to query the latest region list.
RouterInterfaceId	String	Yes	The ID of the router interface.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeactivateRouterInterface
&RegionId=cn-hangzhou
&RouterInterfaceId=ri-sf3rxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeactivateRouterInterfaceResponse>
   <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</DeactivateRouterInterfaceResponse>
```

- JSON format

```
{
   "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
 }
```

2.14.1.10.3. ModifyRouterInterfaceSpec

You can call this operation to modify the specification of a router interface.

After the operation is called, the router interface enters the Activating state. Once activated, the router interface enters the Active state.

> **Note** You cannot modify the specification of a router interface that has overdue payments.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyRouterInterfaceSpec*.
RegionId	String	Yes	The region ID of the router interface. You can call the DescribeRegions operation to query the latest region list.
RouterInterfaceId	String	Yes	The ID of the router interface.
Spec	String	Yes	The specification of the router interface.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
Spec	String	The specification of the router interface.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyRouterInterfaceSpec
&RegionId=cn-hangzhou
&Spec=Middle. 2
&RouterInterfaceId=ri-2ze7fbuohm7pcxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyRouterInterfaceSpecResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
    <Spec>Middle. 2</Spec>
</ModifyRouterInterfaceSpecResponse>
```

- JSON format

```
{
    "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0",
    "Spec":"Middle. 2"
}
```

2.14.1.10.4. DeleteRouterInterface

You can call this operation to delete a router interface.

When you call this operation, make sure that the following requirements are met:

- You can only delete a router interface that is in the Idle or Inactive state.
- Before deleting a router interface, you must delete all custom route entries destined for the router interface.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteRouterInterface*.
RegionId	String	Yes	The region ID of the router interface. You can call the DescribeRegions operation to query the latest region list.
RouterInterfaceId	String	Yes	The ID of the router interface.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteRouterInterface
&RegionId=cn-hangzhou
&RouterInterfaceId=ri-sf3rxxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteRouterInterfaceResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</DeleteRouterInterfaceResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.10.5. DescribeRouterInterfaces

You can call this operation to query router interfaces in a specified region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeRouterInterfaces*.
RegionId	String	Yes	The region ID of the router interface. You can call the DescribeRegions operation to query the latest region list.
Filter.n.Key	String	No	Specifies filter condition n. You can specify a maximum of five filter conditions. Valid values of n: 1 to 5. You can specify multiple values for each filter condition. If you use "or" to separate multiple values, the system returns results that match at least one of the filter conditions. If you use "and" to separate multiple values, the system returns results that match all filter conditions. The following filter conditions are available: • *RouterInterfaceId*: the ID of the router interface. • RouterId: the ID of the VRouter or VBR. • *RouterType*: the type of the router associated with the router interface. • *RouterInterfaceOwnerId*: the account ID of the router interface. • *OppositeInterfaceId*: the ID of the peer router interface. • *OppositeRouterType*: the type of the router associated with the peer router interface. • *OppositeRouterId*: the ID of the peer router (VRouter or VBR). • *OppositeInterfaceOwnerId*: the account ID of the peer router interface. • *Status*: the status of the router interface. • *Name*: the name of the router interface.

Parameter	Type	Required	Description
Filter.n.Value.m	String	No	Specifies value m of filter condition n. Valid values of *m*: 1 to 5.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
RouterInterfaceSet	List	The details about the router interface. For more information, see the RouterInterfaceType list.

RouterInterfaceType list

Parameter	Type	Description
RouterType	String	The type of the router to which the routing table belongs. Valid values: • *VRouter* • *VBR*
RouterInterfaceId	String	The ID of the router interface.
RouterId	String	The ID of the router to which the routing table belongs.
VRouterId	String	The ID of the VRouter.
Spec	String	The specification of the router interface.
Role	String	The role of the router interface: connection initiator or connection receiver.
CreationTime	String	The time when the router interface was created.
OppositeInterfaceOwnerId	String	The account ID of the owner of the peer router interface.

Parameter	Type	Description
OppositeRouterType	String	The type of the router associated with the peer router interface.
OppositeRouterId	String	The ID of the router associated with the peer router interface.
OppositeInterfaceId	String	The ID of the peer router interface.
VpcInstanceId	String	The ID of the instance of the VPC network to connect to.
InstanceId	String	The ID of the next-hop instance.
Status	String	The status of the router interface.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeRouterInterfaces
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeRouterInterfacesResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>2</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>FC2B35C9-15C5-4972-94B7-F529A1620AE0</RequestId>
  <RouterInterfaceSet>
    <RouterInterfaceType>
      <ChargeType>AfterPay</ChargeType>
      <OppositeInterfaceBusinessStatus>Normal</OppositeInterfaceBusinessStatus>
      <RouterInterfaceId>ri-2zepoga55p33dxxxxxxxx</RouterInterfaceId>
      <OppositeInterfaceStatus>Active</OppositeInterfaceStatus>
      <Spec>Small. 1</Spec>
      <OppositeInterfaceOwnerId>12315790xxxxxxxx</OppositeInterfaceOwnerId>
      <OppositeInterfaceSpec>Negative</OppositeInterfaceSpec>
      <CreationTime>2018-04-19T07:35:00Z</CreationTime>
      <RouterType>VRouter</RouterType>
      <Status>Active</Status>
      <OppositeRouterType>VRouter</OppositeRouterType>
      <OppositeRouterId>vrt-m5ey5a8d65bmxxxxxxx</OppositeRouterId>
```

```
        <OppositeRouterId>vrt-m5ey5a8ud5bnxxxxxxxx</OppositeRouterId>
        <OppositeInterfaceId>ri-m5eo6ht5pu2fxxxxxxxxx</OppositeInterfaceId>
        <VpcInstanceId>vpc-2zeugdd0wut2rhxxxxxxxx</VpcInstanceId>
        <RouterId>vrt-2zefso23vmu6xxxxxxxxx</RouterId>
        <ConnectedTime>2018-04-19T07:35:07Z</ConnectedTime>
        <OppositeRegionId>cn-qingdao</OppositeRegionId>
        <BusinessStatus>Normal</BusinessStatus>
        <Role>InitiatingSide</Role>
        <OppositeVpcInstanceId>vpc-m5ep989i7ocrtnxxxxxxxx</OppositeVpcInstanceId>
        <EndTime>2999-09-08T16:00:00Z</EndTime>
      </RouterInterfaceType>
      <RouterInterfaceType>
        <ChargeType>Prepaid</ChargeType>
        <OppositeInterfaceBusinessStatus>Normal</OppositeInterfaceBusinessStatus>
        <RouterInterfaceId>ri-2zegbp7nhj0mxxxxxxxx</RouterInterfaceId>
        <OppositeInterfaceStatus>Deleted</OppositeInterfaceStatus>
        <Spec>Small. 1</Spec>
        <OppositeInterfaceOwnerId>1231579085529123</OppositeInterfaceOwnerId>
        <OppositeInterfaceSpec>Negative</OppositeInterfaceSpec>
        <CreationTime>2017-12-27T06:31:30Z</CreationTime>
        <RouterType>VRouter</RouterType>
        <Status>Inactive</Status>
        <OppositeRouterType>VRouter</OppositeRouterType>
        <OppositeRouterId>vrt-bp1d3bxtdv68txxxxxxxx</OppositeRouterId>
        <OppositeInterfaceId>ri-bp12dxgw8gmoxxxxxxxx</OppositeInterfaceId>
        <VpcInstanceId>vpc-2ze3tq4uxhysg7xxxxxxxx</VpcInstanceId>
        <RouterId>vrt-2zeazning6tbzkxxxxxxxx</RouterId>
        <ConnectedTime>2017-12-27T06:31:36Z</ConnectedTime>
        <OppositeRegionId>cn-hangzhou</OppositeRegionId>
        <BusinessStatus>Normal</BusinessStatus>
        <Role>InitiatingSide</Role>
        <OppositeVpcInstanceId>vpc-bp15k6sx6fhdzxxxxxxxx</OppositeVpcInstanceId>
        <EndTime>2018-07-27T16:00:00Z</EndTime>
      </RouterInterfaceType>
    </RouterInterfaceSet>
</DescribeRouterInterfacesResponse>
```

- JSON format

```
{
    "PageNumber": 1,
    "TotalCount": 2,
    "PageSize": 10,
```

```
"RequestId": "FC2B35C9-15C5-4972-94B7-F529A1620AE0",
"RouterInterfaceSet": {
  "RouterInterfaceType": [
    {
      "ChargeType": "AfterPay",
      "OppositeInterfaceBusinessStatus": "Normal",
      "RouterInterfaceId": "ri-2zepoga55p33djxxxxxxxx",
      "OppositeInterfaceStatus": "Active",
      "Spec": "Small. 1",
      "OppositeInterfaceOwnerId": "123157908xxxxxxxx",
      "OppositeInterfaceSpec": "Negative",
      "CreationTime": "2018-04-19T07:35:00Z",
      "RouterType": "VRouter",
      "Status": "Active",
      "OppositeRouterType": "VRouter",
      "OppositeRouterId": "vrt-m5ey5a8d65bmauxxxxxxxx",
      "OppositeInterfaceId": "ri-m5eo6ht5pu2fxxxxxxxxx",
      "VpcInstanceId": "vpc-2zeugdd0wut2rhxxxxxxxx",
      "RouterId": "vrt-2zefso23vmu6xi3xxxxxxxx",
      "ConnectedTime": "2018-04-19T07:35:07Z",
      "OppositeRegionId": "cn-qingdao",
      "BusinessStatus": "Normal",
      "Role": "InitiatingSide",
      "OppositeVpcInstanceId": "vpc-m5ep989i7ocrxxxxxxxx",
      "EndTime": "2999-09-08T16:00:00Z"
    },
    {
      "ChargeType": "Prepaid",
      "OppositeInterfaceBusinessStatus": "Normal",
      "RouterInterfaceId": "ri-2zegbp7nhj0mnxxxxxxxx",
      "OppositeInterfaceStatus": "Deleted",
      "Spec": "Small. 1",
      "OppositeInterfaceOwnerId": "1231579085xxxxxxxx",
      "OppositeInterfaceSpec": "Negative",
      "CreationTime": "2017-12-27T06:31:30Z",
      "RouterType": "VRouter",
      "Status": "Inactive",
      "OppositeRouterType": "VRouter",
      "OppositeRouterId": "vrt-bp1d3bxtdv68xxxxxxxx",
      "OppositeInterfaceId": "ri-bp12dxgw8gmomxxxxxxxx",
      "VpcInstanceId": "vpc-2ze3tq4uxhysgxxxxxxxx",
```

```
            "RouterId": "vrt-2zeazning6tbzkxxxxxxxx",
            "ConnectedTime": "2017-12-27T06:31:36Z",
            "OppositeRegionId": "cn-hangzhou",
            "BusinessStatus": "Normal",
            "Role": "InitiatingSide",
            "OppositeVpcInstanceId": "vpc-bp15k6sx6fhdzxxxxxxxx",
            "EndTime": "2018-07-27T16:00:00Z"
        }
      ]
    }
}
```


2.14.1.10.6. ActivateRouterInterface

You can call this operation to activate an inactive router interface.

After the operation is called, the router interface enters the Activating state. Once activated, the router interface enters the Active state.

> **Note** You cannot activate a router interface that has overdue payments.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ActivateRouterInterface*.
RegionId	String	Yes	The region ID of the router interface. You can call the DescribeRegions operation to query the latest region list.
RouterInterfaceId	String	Yes	The ID of the router interface.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ActivateRouterInterface
&RegionId=cn-hangzhou
&RouterInterfaceId=ri-sf3rxsfxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ActivateRouterInterfaceResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</ActivateRouterInterfaceResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.10.7. ModifyRouterInterfaceAttribute

You can call this operation to modify the configurations of a router interface.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyRouterInterfaceAttribute*.
RegionId	String	Yes	The region ID of the router interface. You can call the DescribeRegions operation to query the latest region list.
RouterInterfaceId	String	Yes	The ID of the router interface.
AccessPointId	String	No	The ID of the access point to which the VBR belongs. You can call the DescribeAccessPoints operation to query the latest access point list. **Note** You must specify this parameter in the scenario of physical connection access.

Parameter	Type	Required	Description
RouterId	String	Yes	The ID of the router associated with the router interface.
DeleteHealthCheckIp	Boolean	No	Specifies whether to delete the IP address for health check configured on the router interface. Valid values: • true: deletes the IP address for health check. • false: (default) does not delete the IP address for health check.
OppositeRouterId	String	No	The ID of the peer router.
OppositeInterfaceId	String	No	The ID of the peer router interface.
OppositeInterfaceOwnerId	String	No	The ID of the owner of the peer router interface.
HealthCheckSourceIp	String	No	The source IP address used to perform health check on the physical connection. It must be an unused IP address within the VPC. Note You can specify this parameter in the scenario of physical connection access.
HealthCheckTargetIp	String	No	The destination IP address used to perform health check on the physical connection. Note This parameter is required when the HealthCheckSourceIp parameter is specified.
Name	String	No	The name of the router interface. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the router interface. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyRouterInterfaceAttribute
&Name=test
&RouterInterfaceId=ri-2ze7fbuohm7pc3xxxxxxxx
&RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyRouterInterfaceAttributeResponse>
   <RequestId>980960B0-2969-40BF-8542-EBB34FD358AB</RequestId>
</ModifyRouterInterfaceAttributeResponse>
```

- JSON format

```
{
   "RequestId": "980960B0-2969-40BF-8542-EBB34FD358AB"
 }
```

2.14.1.10.8. CreateRouterInterface

You can call this operation to create a router interface.

When you call this operation, make sure that the following requirements are met:

- A maximum of one pair of interconnected router interfaces can be created between two routers.
- A maximum of five router interfaces can be created for a router.
- If your account contains any router interface that has overdue payments, you cannot create new router interfaces.
- The destination CIDR blocks (DestinationCidrBlock) of route entries in the same routing table cannot be the same.
- The router interface created for a virtual border router (VBR) must act as the connection initiator.
- If you want to create a router interface for a VBR, the VBR must be in the Active state.

> **Note** A router interface created by using the API operation is billed on a daily basis.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateRouterInterface*.
RegionId	String	Yes	The region ID of the router interface. You can call the DescribeRegions operation to query the latest region list.
RouterType	String	Yes	The type of the router associated with the router interface. Valid values: • VRouter • VBR
AccessPointId	String	No	The ID of the access point to which the VBR belongs. You can call the DescribeAccessPoints operation to query the latest access point list. **Note** You must specify this parameter in the scenario of physical connection access.
RouterId	String	Yes	The ID of the router associated with the router interface.
Role	String	Yes	The role of the router interface. Valid values: • InitiatingSide: connection initiator • AcceptingSide: connection receiver

Parameter	Type	Required	Description
Spec	String	Yes	The specification of the router interface. The available specifications and the corresponding bandwidths are as follows: • Mini.2: 2 Mbit/s • Mini.5: 5 Mbit/s • Small.1: 10 Mbit/s • Small.2: 20 Mbit/s • Small.5: 50 Mbit/s • Middle.1: 100 Mbit/s • Middle.2: 200 Mbit/s • Middle.5: 500 Mbit/s • Large.1: 1,000 Mbit/s • Large.2: 2,000 Mbit/s • Large.5: 5,000 Mbit/s • Xlarge.1: 10,000 Mbit/s
OppositeRegionId	String	Yes	The region ID of the connection receiver.
OppositeAccessPointId	String	No	The ID of the access point of the peer router interface. Note This parameter must be specified when the peer router interface is on a VBR and cannot be modified after the router interface is created.
OppositeRouterType	String	No	The type of the router associated with the peer router interface. Valid values: • VRouter • VBR
OppositeRouterId	String	No	The ID of the peer router.
OppositeInterfaceId	String	No	The ID of the peer router interface.
OppositeInterfaceOwnerId	String	No	The ID of the owner of the peer router interface.

Parameter	Type	Required	Description
HealthCheckSourceIp	String	No	The source IP address used to perform health check on the physical connection. It must be an unused IP address within the VPC. Note You can specify this parameter in the scenario of physical connection access.
HealthCheckTargetIp	String	No	The destination IP address used to perform health check on the physical connection. Note This parameter is required when the HealthCheckSourceIp parameter is specified.
Name	String	No	The name of the router interface. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the router interface. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
RouterInterfaceId	String	The ID of the router interface.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateRouterInterface
&RegionId=cn-beijing
&Role=InitiatingSide
&OppositeRegionId=cn-beijing
&Spec=Mini.5
&RouterType=VRouter
&RouterId=vrt-2zepuy8qbrq6yxxxxxxxx
&OppositeRouterId= vrt-2zefso23vmuxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CreateRouterInterfaceResponse>
   <RequestId>980960B0-2969-40BF-8542-EBB34FD358AB</RequestId>
   <RouterInterfaceId>ri-2ze7fbuohmxxxxxx</RouterInterfaceId>
</CreateRouterInterfaceResponse>
```

- JSON format

```
{
   "RequestId": "980960B0-2969-40BF-8542-EBB34FD358AB"
   "RouterInterfaceId": "ri-2ze7fbuohmxxxxxx"
}
```

2.14.1.11. Physical connection

2.14.1.11.1. CreatePhysicalConnection

You can call this operation to create a physical connection.

After the physical connection enters the Initial state, contact the carrier to begin construction.

When you call this operation, make sure that the following requirements are met:

- The number of physical connections that are not in the Enabled state cannot exceed five.
- If your account contains any physical connection that has overdue payments, you cannot create new physical connections.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreatePhysicalConnection*.

Parameter	Type	Required	Description
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.
AccessPointId	String	Yes	The ID of the access point that is associated with the physical connection. You can call the DescribeAccessPoints operation to query the latest access point list.
CircuitCode	String	No	The circuit code provided by the carrier for the physical connection.
LineOperator	String	Yes	The carrier that provides the physical connection. Valid values: • *CT*: China Telecom • *CU*: China Unicom • *CM*: China Mobile • *CO*: Other providers in China • *Equinix*: Equinix • *Other*: Other providers outside China
PeerLocation	String	Yes	The geographical location of the on-premise IDC.
Bandwidth	String	No	The bandwidth of the NAT service plan. Unit: Mbit/s. Valid values: 2 to 10240. Default value: *100*.
PortType	String	No	The access port type of the physical connection. Valid values: • *100Base-T*: 100M electrical port • *1000Base-T*: (default) 1 GE electrical port • *1000Base-LX*: 1 GE single-mode optical port (10 km) • *10GBase-T*: 10 GE electrical port • *10GBase-LR*: 10 GE single-mode optical port (10 km)
RedundantPhysicalConnectionId	String	No	The ID of the redundant physical connection. The redundant physical connection must be in the Allocated, Confirmed, or Enabled state.

Parameter	Type	Required	Description
Name	String	No	The name of the physical connection. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the physical connection. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
PhysicalConnectionId	String	The ID of the VPC.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreatePhysicalConnection
&RegionId=cn-beijing
&AccessPointId=ap-cn-beijing-ft-A
&LineOperator=CT
&PeerLocation=XXX
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
 <CreatePhysicalConnectionResponse>
    <RequestId>8A6A5EC5-6F6C-4906-9689-56ACE58A13E0"</RequestId>
    <PhysicalConnectionId>pc-*************</PhysicalConnectionId>
</CreatePhysicalConnectionResponse>
```

- JSON format

```
{
   "PhysicalConnectionId": "pc-**************",
   "RequestId": "8A6A5EC5-6F6C-4906-9689-56ACE58A13E0"
 }
```

2.14.1.11.2. CancelPhysicalConnection

You can call this operation to cancel a physical connection before it is enabled. After you cancel the physical connection, it enters the Canceled state.

You can only cancel a physical connection that is in the Initial, Approved, Allocated, or Confirmed state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CancelPhysicalConnection*.
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.
PhysicalConnectionId	String	Yes	The ID of the physical connection.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=CancelPhysicalConnection
&PhysicalConnectionId=pc-2zeoaxkq3xxxx
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CancelPhysicalConnectionResponse>
   <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</CancelPhysicalConnectionResponse>
```

- JSON format

```
{
   "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
 }
```

2.14.1.11.3. DeletePhysicalConnection

You can call this operation to delete a physical connection.

You can only delete a physical connection that is in the Rejected, Canceled, AllocationFailed, or Terminated state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeletePhysicalConnection*.
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.
PhysicalConnectionId	String	Yes	The ID of the physical connection.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeletePhysicalConnection
&PhysicalConnectionId=pc-2zeoaxkq3xxxx
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeletePhysicalConnectionResponse>
   <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</DeletePhysicalConnectionResponse>
```

- JSON format

```
{
   "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.11.4. ModifyPhysicalConnectionAttribute

You can call this operation to modify the configurations of a physical connection.

When you call this operation, make sure that the following requirements are met:

- If you want to modify the specification or the redundant physical connection ID, the corresponding physical connection must be in the Initial or Rejected state.
- You cannot modify the attributes of the physical connection that is in the Canceled, Allocating, AllocationFailed, or Terminated state.
- After modification, the physical connection in the Rejected state will enter the Initial state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyPhysicalConnectionAttribute*.
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.

Parameter	Type	Required	Description
PhysicalConnectionId	String	Yes	The ID of the physical connection.
LineOperator	String	No	The carrier that provides the physical connection. Valid values: • *CT*: China Telecom • *CU*: China Unicom • *CM*: China Mobile • *CO*: Other providers in China • *Equinix*: Equinix • *Other*: Other providers outside China
CircuitCode	String	No	The circuit code provided by the carrier for the physical connection.
PeerLocation	String	No	The geographical location of the local IDC.
Bandwidth	String	No	The bandwidth of the physical connection. Unit: Mbit/s. Valid values: 2 to 10240. Default value: *100*.
PortType	String	No	The access port type of the physical connection. Valid values: • *100Base-T*: 100M electrical port • *1000Base-T*: (default) 1 GE electrical port • *1000Base-LX*: 1 GE single-mode optical port (10 km) • *10GBase-T*: 10 GE electrical port • *10GBase-LR*: 10 GE single-mode optical port (10 km)
RedundantPhysicalConnectionId	String	No	The ID of the redundant physical connection. The redundant physical connection must be in the Allocated, Confirmed, or Enabled state.
Name	String	No	The name of the physical connection. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the physical connection. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Parameter	Type	Required	Description
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyPhysicalConnectionAttribute
&PhysicalConnectionId=pc-2zeoaxkq3xxxxx
&RegionId=cn-beijing
&Name=test3
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyPhysicalConnectionAttributeResponse>
   <RequestId>8A6A5EC5-6F6C-4906-9689-56ACE58A13E0"</RequestId>
</ModifyPhysicalConnectionAttributeResponse>
```

- JSON format

```
{
    "RequestId": "8A6A5EC5-6F6C-4906-9689-56ACE58A13E0"
 }
```

2.14.1.11.5. DescribePhysicalConnections

You can call this operation to query physical connections in a specified region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribePhysicalConnections*.
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.
Filter.n.Key	String	No	Specifies filter condition n. You can specify a maximum of five filter conditions. Valid values of n: 1 to 5. You can specify multiple values for each filter condition. If you use "or" to separate multiple values, the system returns results that match at least one of the filter conditions. If you use "and" to separate multiple values, the system returns results that match all filter conditions. The following filter conditions are available: • *PhysicalConnectionId*: The ID of the physical connection. • AccessPointId: The ID of the access point. • *Type*: The type of the physical connection. Default value: *VPC*. • *LineOperator*: The carrier of the physical connection. • *Status*: The status of the physical connection. • *Spec*: The specification of the physical connection. • *Name*: The name of the physical connection.
Filter.n.Value.m	String	No	Specifies value m of filter condition n. Valid values of *m*: 1 to 5.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.

Parameter	Type	Description
PageSize	String	The number of entries on each page.
PhysicalConnectionSet	List	The details about the physical connection. For more information, see the PhysicalConnectionSet list.

PhysicalConnectionSet list

Parameter	Type	Description
PhysicalConnectionId	String	The ID of the physical connection.
AccessPointId	String	The ID of the access point that is associated with the physical connection.
Status	String	The status of the physical connection. Valid values: • *Initial*: application in progress • *Approved*: approved • *Allocating*: resource allocation in progress • *Allocated*: under construction • *Confirmed*: pending user confirmation • *Enabled*: enabled • *Rejected*: rejected • *Canceled*: canceled • *Allocation Failed*: resource allocation failed • *Terminated*: terminated
BusinessStatus	String	The payment status of the physical connection. Valid values: • *Normal*: The payment status is normal. • *FinancialLocked*: The physical connection is locked due to overdue payments. • *SecurityLocked*: The physical connection is locked due to security reasons.
CreationTime	String	The time when the physical connection was created.
EnabledTime	String	The time when the physical connection was enabled.

Parameter	Type	Description
LineOperator	String	The carrier that provides the physical connection. Valid values: • *CT*: China Telecom • *CU*: China Unicom • *CM*: China Mobile • *CO*: Other providers in China • *Equinix*: Equinix • *Other*: Other providers outside China
Spec	String	The specification of the physical connection.
PeerLocation	String	The geographical location of the local IDC.
PortType	String	The access port type of the physical connection. Valid values: • *100Base-T*: 100M electrical port • *1000Base-T*: (default) 1 GE electrical port • *1000Base-LX*: 1 GE single-mode optical port (10 km) • *10GBase-T*: 10 GE electrical port • *10GBase-LR*: 10 GE single-mode optical port (10 km)
RedundantPhysicalConnectionId	String	The ID of the redundant physical connection.
Name	String	The name of the physical connection.
Description	String	The description of the physical connection.
ADLocation	String	The location of the physical access device.
PortNumber	String	The port number of the physical access device.
CircuitCode	String	The circuit code provided by the carrier for the physical connection.
Bandwidth	String	The bandwidth of the physical connection.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribePhysicalConnections
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribePhysicalConnectionsResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>7C07B0AF-4FC0-4BB2-9667-F75812824BCD</RequestId>
  <PhysicalConnectionSet>
    <PhysicalConnectionType>
      <Type>VPC</Type>
      <PhysicalConnectionId>pc-2zeoaxkq3jot5pxxxxxxxx</PhysicalConnectionId>
      <PeerLocation>XXX-XX District--XXX Road </PeerLocation>
      <CreationTime>2017-12-13T02:28:42Z</CreationTime>
      <Name>TEST</Name>
      <Status>Enabled</Status>
      <AdLocation>XXX--XX-XXX Datacenter XX Network Cabinet XXU</AdLocation>
      <EnabledTime>2017-12-18T04:01:30Z</EnabledTime>
      <BusinessStatus>Normal</BusinessStatus>
      <LineOperator>CT</LineOperator>
      <PortNumber>1/1/4</PortNumber>
      <AccessPointId>ap-cn-beijing-xx-x</AccessPointId>
      <PortType>100Base-T</PortType>
      <Bandwidth>2</Bandwidth>
    </PhysicalConnectionType>
  </PhysicalConnectionSet>
</DescribePhysicalConnectionsResponse>
```

- JSON format

```
{
 "PageNumber": 1,
 "TotalCount": 1,
 "PageSize": 10,
 "RequestId": "7C07B0AF-4FC0-4BB2-9667-F75812824BCD",
 "PhysicalConnectionSet": {
  "PhysicalConnectionType": [
   {
    "Type": "VPC",
    "PhysicalConnectionId": "pc-2zeoaxkq3jot5xxxxxxxx",
    "PeerLocation": "XXX-XX District--XXX Road",
    "CreationTime": "2017-12-13T02:28:42Z",
    "Name": "TEST",
    "Status": "Enabled",
    "AdLocation": "XXX--XX-XXX Datacenter XX Network Cabinet XXU",
    "EnabledTime": "2017-12-18T04:01:30Z",
    "BusinessStatus": "Normal",
    "LineOperator": "CT",
    "PortNumber": "1/1/4",
    "AccessPointId": "ap-cn-beijing-xx-x",
    "PortType": "100Base-T",
    "Bandwidth": 2
   }
  ]
 }
}
```


2.14.1.11.6. TerminatePhysicalConnection

You can call this operation to terminate a physical connection after it is enabled.

The physical connection enters the Terminating state after the operation is called. The connection enters the Terminated state when the process is completed.

When you call this operation, make sure that the following requirements are met:

- You can only terminate a physical connection in the Enabled state.
- Before terminating a physical connection, you must delete the virtual border routers (VBRs) associated with the physical connection.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *TerminatePhysicalConnection*.
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.
PhysicalConnectionId	String	Yes	The ID of the physical connection.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=TerminatePhysicalConnection
&PhysicalConnectionId=pc-2zeoaxkq3xxxxx
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<TerminatePhysicalConnectionResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</TerminatePhysicalConnectionResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.11.7. EnablePhysicalConnection

You can call this operation to enable a physical connection that is in the Confirmed state. After you have enabled the physical connection, it enters the Enabled state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *EnablePhysicalConnection*.
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.
PhysicalConnectionId	String	Yes	The ID of the physical connection.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=EnablePhysicalConnection
&PhysicalConnectionId=pc-2zeoaxkq3xxxxx
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<EnablePhysicalConnectionResponse>
   <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</EnablePhysicalConnectionResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.12. Virtual border router

2.14.1.12.1. CreateVirtualBorderRouter

You can call this operation to create a virtual border router (VBR).

Each physical connection can associate with two VBRs. One belongs to your own account and the other belongs to a different account. If you create a VBR by using your account, the VBR is in the Enabled state after the operation is called. If you create a VBR by using another account, the VBR is in the Unconfirmed state after the operation is called.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateVirtualBorderRouter*.
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.
PhysicalConnectionId	String	Yes	The ID of the physical connection.
VbrOwnerId	String	No	The account ID of the VBR owner. The default value is the account ID of the user who is calling the operation.
VlanId	String	Yes	The VLAN ID of the VBR. Valid values: 1 to 2999. **Note** Only the owner of the physical connection can specify this parameter. The VLAN IDs of the two VBRs that are associated with the same physical connection must be different.

Parameter	Type	Required	Description
CircuitCode	String	Yes	The circuit code provided by the carrier for the physical connection. Note Only the owner of the physical connection can specify this parameter.
LocalGatewayIp	String	Yes	The IP address of the Alibaba Cloud-side gateway. The IP address is configured for the VBR to interconnect your VPC and your on-premises data center.
PeerGatewayIps	String	Yes	The IP address of your on-premises gateway. The IP address is configured for the VBR to interconnect your VPC and your on-premises data center.
PeeringSubnetMask	String	No	The netmask for the Alibaba Cloud-side IP address and the on-premises IP address. The two IP addresses must be located in the same subnet.
Name	String	No	The name of the VBR. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the VBR. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Parameter	Type	Description
VbrId	String	The ID of the VBR.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateVirtualBorderRouter
&PhysicalConnectionId=pc-2zeoaxkq3jotxxxxxxxx
&RegionId=cn-hangzhou
&VlanId=10
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<CreateRouterInterfaceResponse>
      <RequestId>980960B0-2969-40BF-8542-EBB34FD358AB</RequestId>
      <VbrId>vbr-2zecmmvg5gvu8xxxxxxxx</VbrId>
</CreateRouterInterfaceResponse>
```

- JSON format

```
{
    "RequestId": "980960B0-2969-40BF-8542-EBB34FD358AB"
    "VbrId": "vbr-2zecmmvg5gvu8xxxxxxxx"
 }
```

2.14.1.12.2. DeleteVirtualBorderRouter

You can call this operation to delete a VBR.

Before you call this operation, make sure that the following requirements are met:

- Before deleting a VBR, you must delete all router interfaces on the VBR.
- You can only delete a VBR that is in the Unconfirmed, Enabled, or Terminated state.
- If the owner of a physical connection wants to delete a VBR under another account, the VBR must be in the Unconfirmed state.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteVirtualBorderRouter*.
RegionId	String	Yes	The region ID of the VBR. You can call the DescribeRegions operation to query the latest region list.
VbrId	String	Yes	The ID of the VBR.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteVirtualBorderRouter
&VbrId=pc-2zeoaxkq3xxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteVirtualBorderRouterResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</DeleteVirtualBorderRouterResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
 }
```

2.14.1.12.3. DescribeVirtualBorderRouters

You can call this operation to query created VBRs.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVirtualBorderRouters*.
RegionId	String	Yes	The region ID of the VBR. You can call the DescribeRegions operation to query the latest region list.
Filter.n.Key	String	No	Specifies filter condition n. You can specify a maximum of five filter conditions. Valid values of n: 1 to 5. You can specify multiple values for each filter condition. If you use "or" to separate multiple values, the system returns results that match at least one of the filter conditions. If you use "and" to separate multiple values, the system returns results that match all filter conditions. The following filter conditions are available: • *PhysicalConnectionId*: The ID of the physical connection. • VbrId: The ID of the VBR. • *Status*: The status of the VBR. • *AccessPointId*: The ID of the access point that is associated with the physical connection. • *Name*: The name of the VBR.
Filter.n.Value.m	String	No	Specifies value m of filter condition n. Valid values of *m*: 1 to 5.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.

Parameter	Type	Description
VirtualBorderRouterSet	List	The list of VBRs. For more information, see the VirtualBorderRouterType list.

VirtualBorderRouterType list

Parameter	Type	Description
VbrId	String	The ID of the VBR.
VbrOwnerUid	String	The account ID of the VBR owner. When the VBR owner and the owner of the physical connection are the same, this parameter is empty.
CreationTime	Integer	The time when the VBR was created.
ActivationTime	String	The time when the VBR was activated for the first time.
TerminationTime	String	The last time when the VBR was terminated.
RecoveryTime	String	The last time when the VBR was recovered from the Terminated state to the Active state.
Status	String	The status of the VBR.
VlanId	String	The VLAN ID of the VBR.
CircuitCode	String	The circuit code provided by the carrier for the physical connection.
RouteTableId	String	The ID of the routing table of the VBR.
VlanInterfaceId	String	The ID of the router interface of the VBR.
LocalGatewayIp	String	The Alibaba Cloud-side IP address The IP address of the Alibaba Cloud-side gateway. The IP address is configured for the VBR to interconnect your VPC and your on-premises data center.
PeerGatewayIp	String	The IP address of your on-premises gateway. The IP address is configured for the VBR to interconnect your VPC and your on-premises data center.
PeeringSubnetMask	String	The netmask for the Alibaba Cloud-side IP address and the on-premises IP address.
Name	String	The name of the VBR.
Description	String	The description of the VBR.
PhysicalConnectionId	String	The ID of the physical connection that the VBR connects to.
AccessPointId	String	The ID of the access point that is associated with the physical connection.

Parameter	Type	Description
Status	String	The status of the physical connection. Valid values: • *Initial*: application in progress • *Approved*: approved • *Allocating*: resource allocation in progress • *Allocated*: under construction • *Confirmed*: pending user confirmation • *Enabled*: enabled • *Rejected*: rejected • *Canceled*: canceled • *Allocation Failed*: resource allocation failed • *Terminated*: terminated
BusinessStatus	String	The payment status of the physical connection. Valid values: • *Normal*: The payment status is normal. • *FinancialLocked*: The physical connection is locked due to overdue payments. • *SecurityLocked*: The physical connection is locked due to security reasons.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeVirtualBorderRouters
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeVirtualBorderRoutersResponse>
  <RequestId>AE65530E-8436-4FB1-8217-DCD35712AC89</RequestId>
  <PageNumber>1</PageNumber>
  <VirtualBorderRouterSet>
    <VirtualBorderRouterType>
      <LocalGatewayIp>10.xx.xx. 1</LocalGatewayIp>
      <PeerGatewayIp>10.xx.xx. 2</PeerGatewayIp>
      <Description></Description>
      <PhysicalConnectionOwnerUid>1231579085529123</PhysicalConnectionOwnerUid>
      <VlanId>10</VlanId>
      <RecoveryTime></RecoveryTime>
      <PhysicalConnectionStatus>Enabled</PhysicalConnectionStatus>
      <PhysicalConnectionId>pc-2zeoaxkq3jot5p71qcnuy</PhysicalConnectionId>
      <RouteTableId>vtb-2ze9hmd6yofwvb1dd79j9</RouteTableId>
      <PeeringSubnetMask>255.0.0.0</PeeringSubnetMask>
      <TerminationTime></TerminationTime>
      <Name></Name>
      <CreationTime>2018-03-06T11:16:34Z</CreationTime>
      <ActivationTime>2018-03-06T11:16:34Z</ActivationTime>
      <CircuitCode></CircuitCode>
      <Status>active</Status>
      <PhysicalConnectionBusinessStatus>Normal</PhysicalConnectionBusinessStatus>
      <VlanInterfaceId>ri-2zeum6rgu0586gjrocikm</VlanInterfaceId>
      <AccessPointId>ap-cn-beijing-dx-A</AccessPointId>
      <VbrId>vbr-2zecmmvg5gvu8i4telkhw</VbrId>
    </VirtualBorderRouterType>
  </VirtualBorderRouterSet>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
</DescribeVirtualBorderRoutersResponse>
```

- JSON format

```
{
 "PageNumber": 1,
 "VirtualBorderRouterSet": {
  "VirtualBorderRouterType": [
   {
    "LocalGatewayIp": "10.xx.xx. 1",
    "PeerGatewayIp": "10.xx.xx. 2",
    "Description": "",
    "PhysicalConnectionOwnerUid": "1231579085xxxx",
    "VlanId": 10,
    "RecoveryTime": "",
    "PhysicalConnectionStatus": "Enabled",
    "PhysicalConnectionId": "pc-2zeoaxkq3jotxxxxx",
    "RouteTableId": "vtb-2ze9hmd6yofwxxxxxx",
    "PeeringSubnetMask": "255.0.0.0",
    "TerminationTime": "",
    "Name": "",
    "CreationTime": "2018-03-06T11:16:34Z",
    "ActivationTime": "2018-03-06T11:16:34Z",
    "CircuitCode": "",
    "Status": "active",
    "PhysicalConnectionBusinessStatus": "Normal",
    "VlanInterfaceId": "ri-2zeum6rgu058xxxxxx",
    "AccessPointId": "ap-cn-beijing-dx-A",
    "VbrId": "vbr-2zecmmvg5gvuxxxxxx"
   }
 "TotalCount": 1,
 "PageSize": 10,
 "RequestId": "98B24329-ADC9-4725-A5F8-6C1B282DA17D"
}
```


2.14.1.12.4.

DescribeVirtualBorderRoutersForPhysicalConnection

You can call this operation to query the VBRs connected to a specified physical connection, including VBRs that belong to the physical connection owner and other accounts.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVirtualBorderRoutersForPhysicalConnection*.
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.
PhysicalConnectionId	String	No	The ID of the physical connection.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
VirtualBorderRouterForPhysicalConnectionSet	List	The list of VBRs. For more information, see the VirtualBorderRouterForPhysicalConnectionType list.

VirtualBorderRouterForPhysicalConnectionType list

Parameter	Type	Description
VbrId	String	The ID of the VBR.
VbrOwnerUid	String	The account ID of the VBR owner. When the VBR owner and the owner of the physical connection are the same, this parameter is empty.
CreationTime	Integer	The time when the VBR was created.
ActivationTime	String	The time when the VBR was activated for the first time.

Parameter	Type	Description
TerminationTime	String	The last time when the VBR was terminated.
RecoveryTime	String	The last time when the VBR was recovered from the Terminated state to the Active state.
VlanId	String	The VLAN ID of the VBR.
CircuitCode	String	The circuit code provided by the carrier for the physical connection.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeVirtualBorderRoutersForPhysicalConnection
&RegionId=cn-beijing
&PhysicalConnectionId=pc-2zeoaxkqxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeVirtualBorderRoutersForPhysicalConnectionResponse>
  <RequestId>03E8CB87-5876-4034-BBB2-6E0851281C37</RequestId>
  <PageNumber>1</PageNumber>
  <TotalCount>2</TotalCount>
  <PageSize>10</PageSize>
  <VirtualBorderRouterForPhysicalConnectionSet>
    <VirtualBorderRouterForPhysicalConnectionType>
      <ActivationTime>2018-03-06T11:16:34Z</ActivationTime>
      <CreationTime>2018-03-06T11:16:34Z</CreationTime>
      <CircuitCode></CircuitCode>
      <VlanId>10</VlanId>
      <RecoveryTime></RecoveryTime>
      <VbrOwnerUxxx231579085529123
      </VbrOwnerUid>
      <TerminationTime></TerminationTime>
      <VbrId>Vbrxxxxx-2zecmmvg5gvu8ixxxxxxxx</VbrId>
    </VirtualBorderRouterForPhysicalConnectionType>
    <VirtualBorderRouterForPhysicalConnectionType>
      <ActivationTime>2018-01-04T13:34:18Z</ActivationTime>
      <CreationTime>2018-01-04T13:34:18Z</CreationTime>
      <CircuitCode></CircuitCode>
      <VlanId>100</VlanId>
      <RecoveryTime></RecoveryTime>
      <VxxxbrOwnerUid>12315790xxxxxxxx
      </VbrOwnerUid>
      <TerminationTime></TerminationTime>
      <VbrId>vbr-2zee2e2cwetx4xxxxxxxx</VbrId>
    </VirtualBorderRouterForPhysicalConnectionType>
 </DescribeVirtualBorderRoutersForPhysicalConnectionResponse>
```

- JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 2,
  "PageSize": 10,
  "RequestId": "03E8CB87-5876-4034-BBB2-6E0851281C37",
  "VirtualBorderRouterForPhysicalConnectionSet": {
    "VirtualBorderRouterForPhysicalConnectionType": [
      {
        "ActivationTime": "2018-03-06T11:16:34Z",
        "CreationTime": "2018-03-06T11:16:34Z",
        "CircuitCode": "",
        "VlanId": 10,
        "RecoveryTime": "",
        "VbrOwnerUid": "1231579085xxxxxx529123",
        "TerminationTime": "",
        "VbrId": "vbr-2zecmmvg5gvxxxxxxxx"
      },
      {
        "ActivationTime": "2018-01-04T13:34:18Z",
        "CreationTime": "2018-01-04T13:34:18Z",
        "CircuitCode": "",
        "VlanId": 100,
        "RecoveryTime": "",
        "VbrOwnerUid": "12315xxxxxxxx",
        "TerminationTime": "",
        "VbrId": "vbr-2zee2e2cwetx4k0xxxxxxxx"
      }
    ]
  }
}
```


2.14.1.12.5. ModifyVirtualBorderRouterAttribute

You can call this operation to modify the configurations of a VBR.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyVirtualBorderRouterAttribute*.

Parameter	Type	Required	Description
RegionId	String	Yes	The region ID of the physical connection. You can call the DescribeRegions operation to query the latest region list.
VbrId	String	Yes	The ID of the VBR.
VlanId	String	Yes	The VLAN ID of the VBR. Valid values: 1 to 2999. Note Only the owner of the physical connection can specify this parameter. The VLAN IDs of two VBRs of the same physical connection must be different.
CircuitCode	String	Yes	The circuit code provided by the carrier for the physical connection. Note Only the owner of the physical connection can specify this parameter.
LocalGatewayIp	String	Yes	The IP address of the Alibaba Cloud-side gateway. The IP address is configured for the VBR to interconnect your VPC and your on-premises data center.
PeerGatewayIps	String	Yes	The IP address of your on-premises gateway. The IP address is configured for the VBR to interconnect your VPC and your on-premises data center.
PeeringSubnetMask	String	No	The netmask for the Alibaba Cloud-side IP address and the on-premises IP address. The two IP addresses must be located in the same subnet.
Name	String	No	The name of the VBR. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.

Parameter	Type	Required	Description
Description	String	No	The description of the VBR. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyVirtualBorderRouterAttribute
&VbrId=vbr-2zee2e2cwetxxxxxxxxx
&Name=test
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<ModifyVirtualBorderRouterAttributeResponse>
   <RequestId>980960B0-2969-40BF-8542-EBB34FD358AB</RequestId>
</ModifyVirtualBorderRouterAttributeResponse>
```

- JSON format

```
{
   "RequestId": "980960B0-2969-40BF-8542-EBB34FD358AB"
 }
```

2.14.1.12.6. TerminateVirtualBorderRouter

You can call this operation to terminate a VBR.

After the operation is called, the state of the VBR will be changed from Enabled to Terminated. Before you call this operation, make sure that the following requirements are met:

- Only the owner of the physical connection that the VBR connects to can call this operation.
- If the VBR has been in the Terminated state for seven days or longer, its VLAN ID can be occupied by other VBRs.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *TerminateVirtualBorderRouter*.
RegionId	String	Yes	The region ID of the VBR. You can call the DescribeRegions operation to query the latest region list.
VbrId	String	Yes	The ID of the VBR.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=TerminateVirtualBorderRouter
&VbrId=pc-2zeoaxkq3xxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<TerminateVirtualBorderRouterResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</TerminateVirtualBorderRouterResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.12.7. RecoverVirtualBorderRouter

You can call this operation to recover a terminated VBR.

After the operation is called, the state of the VBR will be changed from Terminated to Recovering. When the operation is completed, the VBR status will be changed to the Enabled state. Before you call this operation, make sure that the following requirements are met:

- Only the owner of the physical connection that the VBR connects to can call this operation.
- The physical connection that the VBR connects to must be in the Enabled state.
- If the VBR has been in the Terminated state for seven days or longer, its VLAN ID can be occupied by other VBRs. In this case, the recover fails.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *RecoverVirtualBorderRouter*.
RegionId	String	Yes	The region ID of the VBR. You can call the DescribeRegions operation to query the latest region list.
VbrId	String	Yes	The ID of the VBR.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=RecoverVirtualBorderRouter
&VbrId=pc-2zeoaxkq3xxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<RecoverVirtualBorderRouterResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</RecoverVirtualBorderRouterResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.13. NAT Gateway

2.14.1.13.1. CreateNatGateway

You can call this operation to create a NAT Gateway.

When you call this operation, make sure that the following requirements are met:

- A NAT Gateway and a self-built SNAT Gateway (by using an ECS instance as the SNAT Gateway) cannot coexist in a VPC.
- After you have created a NAT Gateway, a route entry is automatically added to the routing table of the VPC. The destination CIDR block is 0.0.0.0/0 and the next-hop is the NAT Gateway. The route entry ensures that traffic is routed to the NAT Gateway.
- If the VPC routing table already contains a route entry with a destination CIDR block of 0.0.0.0/0, delete this route entry. Otherwise, you cannot create a NAT Gateway.

Types of NAT Gateway

You can specify the type of a NAT Gateway as needed. The type of a NAT Gateway determines its SNAT performance (maximum connections and the number of new connections per second), but does not affect the data throughput.

The relationships between NAT Gateway types and SNAT performance metrics are as follows.

Type	Maximum connection	New connection per second
Small	10,000	1,000
Middle	50,000	5,000
Large	200,000	10,000

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateNatGateway*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
VpcId	String	Yes	The ID of the VPC.

Parameter	Type	Required	Description
Spec	String	No	The type of the NAT Gateway. Valid values: • *Small* (default) • *Middle* • *Large*
BandwidthPackage.n.IpCount	String	No	The number of public IP addresses in the NAT service plan n. Valid values: 1 to 50. n indicates the sequence of the service plan. Valid values: 1 to 4. **Note** This parameter can only be specified if the NAT service plan is included in your account before November 3, 2017. If the NAT service plan is not included in your account before November 3, 2017, bind an EIP.
BandwidthPackage.n.Bandwidth	String	No	The bandwidth of the NAT service plan n. Valid values: 5 to 5000. You can use the client to generate this value, but you must ensure that it is unique among different requests. The bandwidth can contain only ASCII characters, and cannot exceed 64 characters in length. **Note** This parameter can only be specified if the NAT service plan is included in your account before November 3, 2017. If the NAT service plan is not included in your account before November 3, 2017, bind an EIP.
BandwidthPackage.n.Zone	String	No	The zone to which the NAT service plan n belongs. If you do not specify this parameter, the bandwidth package is randomly allocated to a zone. Connectivity is not affected when the IP addresses of the NAT service plan and the back-end ECS instance belong to different zones. However, if the IP addresses belong to the same zone, the latency can be shortened. **Note** This parameter can only be specified if the NAT service plan is included in your account before November 3, 2017. If the NAT service plan is not included in your account before November 3, 2017, bind an EIP.

Parameter	Type	Required	Description
Name	String	No	The name of the NAT Gateway. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the NAT Gateway. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
NatGatewayId	String	The ID of the NAT Gateway.
SnatTableIds	List	The SNAT table of the NAT Gateway.
ForwardTableIds	List	The DNAT table of the NAT Gateway.
BandwidthPackageIds	String	The NAT service plan of the NAT Gateway.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateNatGateway
&VpcId=vpc-11af8xxxxxxxx
&Name=MyNatGW
&BandwidthPackage. 1.IpCount=5
&RegionId=cn-shanghai
&BandwidthPackage. 1.Bandwidth=150
&BandwidthPackage. 1.Zone=cn-shanghai-a
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<CreateNatGatewayResponse>
  <BandwidthPackageIds></BandwidthPackageIds>
  <RequestId>C44F62BE-9CE7-4277-B117-69243F3988BF</RequestId>
  <SnatTableIds>
    <SnatTableId>stb-2zeal45my4svybxxxxxxxx</SnatTableId>
  </SnatTableIds>
  <ForwardTableIds>
    <ForwardTableId>ftb-2ze49kghsvq8lxxxxxxxx</ForwardTableId>
  </ForwardTableIds>
  <NatGatewayId>ngw-2zeo05qre24nhxxxxxxxx</NatGatewayId>
</CreateNatGatewayResponse>
```

- JSON format

```
{
  "BandwidthPackageIds": {
    "BandwidthPackageId": [ ]
  },
  "RequestId": "C44F62BE-9CE7-4277-B117-69243F3988BF",
  "SnatTableIds": {
    "SnatTableId": [
      "stb-2zeal45my4svyxxxxxxxx"
    ]
  },
  "ForwardTableIds": {
    "ForwardTableId": [
      "ftb-2ze49kghsvq8xxxxxxxx"
    ]
  },
  "NatGatewayId": "ngw-2zeo05qre24nxxxxxxxx"
}
```


2.14.1.13.2. DeleteNatGateway

You can call this operation to delete a NAT Gateway.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteNatGateway*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
NatGatewayId	String	Yes	The ID of the NAT Gateway.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteNatGateway
&RegionId=cn-beijing
&NatGatewayId=ngw-112za3xxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteNatGatewayResponse>
    <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</DeleteNatGatewayResponse>
```

- JSON format

```
{
  "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.13.3. ModifyNatGatewaySpec

You can call this operation to modify the type of a NAT Gateway.

A NAT Gateway is billed based on the type of the highest specifications that have been used.

You can specify the type of a NAT Gateway as needed. The type of a NAT Gateway determines its SNAT performance (maximum connections and the number of new connections per second), but does not affect the data throughput.

The relationships between NAT Gateway types and SNAT performance metrics are as follows.

Type	Maximum connection	New connection per second
Small	10,000	1,000
Middle	50,000	5,000
Large	200,000	10,000

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyNatGatewaySpec*.

Parameter	Type	Required	Description
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
NatGatewayId	String	Yes	The ID of the NAT Gateway.
Spec	String	No	The type of the NAT Gateway. Valid values: • *Small* (default) • *Middle* • *Large*
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyNatGatewaySpec
&NatGatewayId=ngw-112za33xxxxxxxx
&Spec=Large
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<ModifyNatGatewaySpecResponse>
   <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</ModifyNatGatewaySpecResponse>
```

- JSON format

```
{
  "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
}
```

2.14.1.13.4. ModifyNatGatewayAttribute

You can call this operation to modify the configurations of a NAT Gateway.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyNatGatewayAttribute*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
NatGatewayId	String	Yes	The ID of the NAT Gateway.
Name	String	No	The name of the NAT Gateway. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the NAT Gateway. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyNatGatewayAttribute
&NatGatewayId=ngw-112za3xxxxxxxx
&Spec=Large
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<ModifyNatGatewayAttributeResponse>
   <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</ModifyNatGatewayAttributeResponse>
```

- JSON format

```
{
   "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
 }
```

2.14.1.13.5. DescribeNatGateways

You can call this operation to query created NAT Gateways in a specified region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeNatGateways*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
NatGatewayId	String	No	The ID of the NAT Gateway.
VpcId	String	No	The ID of the VPC.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
NatGateways	List	The details about the NAT Gateway. For more information, see the NatGateway list.

NatGateway list

Parameter	Type	Description
NatGatewayId	String	The region ID of the NAT Gateway.
RegionId	String	The ID of the NAT Gateway.
Description	Integer	The description of the NAT Gateway.
Spec	String	The type of the NAT Gateway.
Status	String	The status of the NAT Gateway. Valid values: • Initiating: The NAT Gateway is being initialized. • Available: The NAT Gateway is available. • Pending: The NAT Gateway is being configured.
ForwardTableIds	List	The DNAT table.
BandwidthPackageIds	List	The NAT bandwidth package list.
SnatTableIds	List	The SNAT table.
BusinessStatus	String	The payment status of the NAT Gateway. Valid values: • Normal: The payment status is normal. • FinancialLocked: The NAT Gateway is locked due to overdue payments. • SecurityLocked: The NAT Gateway is locked due to security reasons.

Parameter	Type	Description
CreationTime	String	The time when the NAT Gateway was created.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeNatGateways
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DescribeNatGatewaysResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>1207C80C-7CAB-4874-A9A0-D19EC9F35490</RequestId>
  <NatGateways>
    <NatGateway>
      <Description></Description>
      <Spec>Small</Spec>
      <IpLists>
        <IpList>
          <IpAddress>118.xx.xx. 181</IpAddress>
          <AllocationId>eip-bp1xyg5ipmh3nxxxxxxxx</AllocationId>
          <UsingStatus>UsedBySnatTable</UsingStatus>
        </IpList>
        <IpList>
          <IpAddress>47.xx.xx. 34</IpAddress>
          <AllocationId>eip-bp19eue77u20cfxxxxxxxx</AllocationId>
          <UsingStatus>UsedByForwardTable</UsingStatus>
        </IpList>
      </IpLists>
      <ForwardTableIds>
        <ForwardTableId>ftb-bp15o9aylj19vxxxxxxxx</ForwardTableId>
      </ForwardTableIds>
      <VpcId>vpc-bp15k6sx6fhdz2xxxxxxxx</VpcId>
      <NatGatewayId>ngw-bp1047e2d4z7kxxxxxxxx</NatGatewayId>
      <CreationTime>2018-01-10T09:48:29Z</CreationTime>
      <BandwidthPackageIds></BandwidthPackageIds>
      <Name></Name>
      <Status>Available</Status>
      <BusinessStatus>Normal</BusinessStatus>
      <RegionId>cn-hangzhou</RegionId>
      <SnatTableIds>
        <SnatTableId>stb-bp1tyr0o48w6wxxxxxxxx</SnatTableId>
      </SnatTableIds>
      <InstanceChargeType>PostPaid</InstanceChargeType>
    </NatGateway>
  </NatGateways>
</DescribeNatGatewaysResponse>
```

- JSON format


```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "1207C80C-7CAB-4874-A9A0-D19EC9F35490",
  "NatGateways": {
    "NatGateway": [
      {
        "Description": "",
        "Spec": "Small",
        "IpLists": {
          "IpList": [
            {
              "IpAddress": "118.xx.xx. 181",
              "AllocationId": "eip-bp1xyg5ipmh3nlxxxxxxxx",
              "UsingStatus": "UsedBySnatTable"
            },
            {
              "IpAddress": "47.xx.xx. 34",
              "AllocationId": "eip-bp19eue77u20cxxxxxxxx",
              "UsingStatus": "UsedByForwardTable"
            }
          ]
        },
        "ForwardTableIds": {
          "ForwardTableId": [
            "ftb-bp15o9aylj19vxxxxxxxx"
          ]
        },
        "VpcId": "vpc-bp15k6sx6fhdzxxxxxxxx",
        "NatGatewayId": "ngw-bp1047e2d4z7xxxxxxxx",
        "CreationTime": "2018-01-10T09:48:29Z",
        "BandwidthPackageIds": {
          "BandwidthPackageId": [ ]
        },
        "Name": "",
        "Status": "Available",
        "BusinessStatus": "Normal",
        "RegionId": "cn-hangzhou",
        "SnatTableIds": {
```

```
            "SnatTableId": [
              "stb-bp1tyr0o48w6wyxxxxxxxx"
            ]
          },
          "InstanceChargeType": "PostPaid"
        }
      ]
    }
}
```


2.14.1.13.6. CreateBandwidthPackage

You can call this operation to create a NAT bandwidth package.

The public IP address and bandwidth of the NAT Gateway are encapsulated into a NAT bandwidth package. You can create a maximum of four NAT bandwidth packages for a NAT Gateway.

A NAT bandwidth package includes:

- A shared bandwidth
- A group of public IP addresses

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateBandwidthPackage*.
RegionId	String	Yes	The region ID of the NAT bandwidth package. You can call the DescribeRegions operation to query the latest region list.
NatGatewayId	String	Yes	The ID of the NAT Gateway.
IpCount	Integer	Yes	The number of public IP addresses in the NAT bandwidth package. Valid values: 1 to 50.
Bandwidth	Integer	Yes	The bandwidth of the NAT bandwidth package. Valid values: 5 to 1000.

Parameter	Type	Required	Description
Zone	String	No	The zone to which the NAT bandwidth package belongs. If you do not specify this parameter, the bandwidth package is randomly allocated to a zone. Note Connectivity is not affected when the IP addresses of the NAT bandwidth package and the back-end ECS instance belong to different zones. However, when the IP addresses belong to the same zone, the latency can be shortened.
Name	String	No	The name of the NAT bandwidth package. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the NAT bandwidth package. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
BandwidthPackageId	String	The ID of the NAT bandwidth package.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateBandwidthPackage
&NatGatewayId=ngw-7mwb327xxxxxxxx
&RegionId=cn-shanghai
&Bandwidth=5
&ZoneId=cn-shanghai-a
&IpCount=1
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<CreateBandwidthPackageResponse>
    <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
    <BandwidthPackageId>bwp-s6lmotmxxxxxxxx</BandwidthPackageId>
</CreateBandwidthPackageResponse>
```

- JSON format

```
{
    "BandwidthPackageId": "bwp-s6lmotmxxxxxxxx",
    "RequestId": "54ED4074-3F89-4F11-B166-837DD3E20FE3"
}
```

2.14.1.13.7. ModifyBandwidthPackageSpec

You can call this operation to modify the bandwidth of a NAT bandwidth package.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyBandwidthPackageSpec*.
RegionId	String	Yes	The region ID of the NAT bandwidth package. You can call the DescribeRegions operation to query the latest region list.
BandwidthPackageId	String	Yes	The ID of the NAT bandwidth package.
Bandwidth	Integer	Yes	The bandwidth of the NAT bandwidth package. Valid values: 5 to 1000.

Parameter	Type	Required	Description
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyBandwidthPackageSpec
&BandwidthPackageId=bwp-11odxu2xxxxxxxx
&RegionId=cn-shanghai
&Bandwidth=200
&IpCount=1
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<ModifyBandwidthPackageSpecResponse>
    <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</ModifyBandwidthPackageSpecResponse>
```

- JSON format

```
{
   "RequestId": "54ED4074-3F89-4F11-B166-837DD3E20FE3"
}
```

2.14.1.13.8. DescribeBandwidthPackages

You can call this operation to query NAT bandwidth packages in a specified region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeBandwidthPackages*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
NatGatewayId	String	No	The ID of the NAT Gateway.
BandwidthPackageId	String	No	The ID of the NAT bandwidth package.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
BandwidthPackages	List	The details about the NAT bandwidth package. For more information, see the BandwidthPackage list.

BandwidthPackage list

Parameter	Type	Description
BandwidthPackageId	String	The ID of the NAT bandwidth package.
RegionId	String	The region ID of the NAT bandwidth package.
Description	Integer	The description of the NAT bandwidth package.
Name	String	The name of the NAT bandwidth package.

Parameter	Type	Description
ZoneId	String	The zone to which the NAT bandwidth package belongs.
GatewayId	String	The ID of the NAT Gateway.
Bandwidth	String	The bandwidth of the NAT bandwidth package. Unit: Mbit/s.
SnatTableIds	List	The SNAT table.
InternetChargeType	String	The billing method of the NAT bandwidth package. Valid value: *PayByBandwidth*.
CreationTime	String	The time when the NAT bandwidth package was created.
ISP	String	The carrier type of the NAT bandwidth package. Valid value: *BGP*.
PublicIpAddresses	String	The public IP address list of the NAT bandwidth package. For more information, see the PublicIpAddresse list.
CreationTime	String	The time when the NAT bandwidth package was created.

BandwidthPackage

Parameter	Type	Description
BandwidthPackageId	String	The ID of the NAT bandwidth package.
RegionId	String	The region ID of the NAT bandwidth package.
Description	Integer	The description of the NAT bandwidth package.
Name	String	The name of the NAT bandwidth package.
ZoneId	String	The zone to which the NAT bandwidth package belongs.
GatewayId	String	The ID of the NAT Gateway.
Bandwidth	String	The bandwidth of the NAT bandwidth package. Unit: Mbit/s.

Parameter	Type	Description
SnatTableIds	List	The SNAT table.
CreationTime	String	The time when the NAT bandwidth package was created.
ISP	String	The carrier type of the NAT bandwidth package. Valid value: *BGP*.
PublicIpAddresses	String	The public IP address list of the NAT bandwidth package.
CreationTime	String	The time when the NAT bandwidth package was created.

PublicIpAddress list

Parameter	Type	Description
AllocationId	String	The ID of the public IP address.
IpAddress	String	The public IP address.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeBandwidthPackages
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeBandwidthPackagesResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <BandwidthPackages>
    <BandwidthPackage>
      <Description></Description>
      <IpCount>2</IpCount>
      <ISP>BGP</ISP>
      <ZoneId>cn-hangzhou-b</ZoneId>
      <InternetChargeType>PayByTraffic</InternetChargeType>
      <NatGatewayId>ngw-bp1uewa15k4iyxxxxxxxx</NatGatewayId>
      <Name></Name>
      <CreationTime>2018-03-06T07:33:51Z</CreationTime>
      <Status>Available</Status>
      <BandwidthPackageId>bwp-bp1xea10o8qxwxxxxxxxx</BandwidthPackageId>
      <BusinessStatus>Normal</BusinessStatus>
      <RegionId>cn-hangzhou</RegionId>
      <InstanceChargeType>PostPaid</InstanceChargeType>
      <PublicIpAddresses>
        <PublicIpAddresse>
          <IpAddress>118.xx.xx. 33</IpAddress>
          <AllocationId>nateip-bp1jb1uijvm9oxxxxxxxx</AllocationId>
          <UsingStatus>Idle</UsingStatus>
        </PublicIpAddresse>
        <PublicIpAddresse>
          <IpAddress>118.xx.xx. 31</IpAddress>
          <AllocationId>nateip-bp1dt4hpe8847xxxxxxxx</AllocationId>
          <UsingStatus>UsedBySnatTable</UsingStatus>
        </PublicIpAddresse>
      </PublicIpAddresses>
      <Bandwidth>5</Bandwidth>
    </BandwidthPackage>
  </BandwidthPackages>
  <PageSize>10</PageSize>
</DescribeBandwidthPackagesResponse>
```

- JSON format

```
{
 "PageNumber": 1,
 "TotalCount": 1,
 "BandwidthPackages": {
  "BandwidthPackage": [
   {
    "Description": "",
    "IpCount": "2",
    "ISP": "BGP",
    "ZoneId": "cn-hangzhou-b",
    "InternetChargeType": "PayByTraffic",
    "NatGatewayId": "ngw-bp1uewa15k4iyxxxxxxxx",
    "Name": "",
    "CreationTime": "2018-03-06T07:33:51Z",
    "Status": "Available",
    "BandwidthPackageId": "bwp-bp1xea10o8qxwxxxxxxxx",
    "BusinessStatus": "Normal",
    "RegionId": "cn-hangzhou",
    "InstanceChargeType": "PostPaid",
    "PublicIpAddresses": {
     "PublicIpAddresse": [
      {
       "IpAddress": "118.xx.xx. 33",
       "AllocationId": "nateip-bp1jb1uijvm9oxxxxxxxx",
       "UsingStatus": "Idle"
      },
      {
       "IpAddress": "118.xx.xx. 33",
       "AllocationId": "nateip-bp1dt4hpe8847xxxxxxxx",
       "UsingStatus": "UsedBySnatTable"
      }
     ]
    },
    "Bandwidth": "5"
   }
  ]
 },
 "PageSize": 10,
 "RequestId": "8909013D-4A64-41A6-93E6-E3FD08A3EAFE"
}
```

2.14.1.13.9. ModifyBandwidthPackageAttribute

You can call this operation to modify the name and description of a NAT bandwidth package.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyBandwidthPackageAttribute*.
RegionId	String	Yes	The region ID of the NAT bandwidth package. You can call the DescribeRegions operation to query the latest region list.
BandwidthPackageId	String	Yes	The ID of the NAT bandwidth package.
Name	String	No	The name of the NAT bandwidth package. The name must be 2 to 128 characters in length. It can contain letters, digits, periods (.), underscores (_), and hyphens (-). It must start with a letter but cannot start with `http://` or `https://`.
Description	String	No	The description of the NAT bandwidth package. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com?Action=ModifyBandwidthPackageAttribute
&BandwidthPackageId=bwp-s6lmotmxxxxxxxx
&Name=modified
&RegionId=cn-shanghai
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<ModifyBandwidthPackageAttributeResponse>
   <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</ModifyBandwidthPackageAttributeResponse>
```

- JSON format

```
{
   "RequestId": "54ED4074-3F89-4F11-B166-837DD3E20FE3"
}
```

2.14.1.13.10. DeleteBandwidthPackage

You can call this operation to delete a NAT bandwidth package.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteBandwidthPackage*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
BandwidthPackageId	String	Yes	The ID of the NAT bandwidth package.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteBandwidthPackage
&BandwidthPackageId=bwp-11odxu2xxxxxxxx
&RegionId=cn-shanghai
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<DeleteBandwidthPackageResponse>
   <RequestId>0ED8D006-F706-4D23-88ED-E11ED28DCAC0</RequestId>
</DeleteBandwidthPackageResponse>
```

- JSON format

```
{
   "RequestId": "0ED8D006-F706-4D23-88ED-E11ED28DCAC0"
}
```

2.14.1.13.11. AddBandwidthPackageIps

You can call this operation to add public IP addresses to a NAT bandwidth package.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *AddBandwidthPackageIps*.
RegionId	String	Yes	The region ID of the NAT bandwidth package. You can call the DescribeRegions operation to query the latest region list.
BandwidthPackageId	String	Yes	The ID of the NAT bandwidth package.
IpCount	String	No	The number of public IP addresses in the NAT bandwidth package. Valid values: 1 to 50.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=AddBandwidthPackageIps
&BandwidthPackageId=bwp-11odxu2xxxxxxxx
&RegionId=cn-shanghai
&IpCount=6
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<AddBandwidthPackageIpsResponse>
   <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</AddBandwidthPackageIpsResponse>
```

- JSON format

```
{
  "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
}
```

2.14.1.13.12. RemoveBandwidthPackageIps

You can call this operation to remove public IP addresses from a NAT bandwidth package.

When you call this operation, make sure that the following requirements are met:

- You cannot remove all public IP addresses from the NAT bandwidth package.
- You cannot remove any IP addresses that are not included in the NAT bandwidth package.
- You cannot remove any IP addresses listed in the DNAT table or the SNAT table.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *RemoveBandwidthPackageIps*.
RegionId	String	Yes	The region ID of the NAT bandwidth package. You can call the DescribeRegions operation to query the latest region list.

Parameter	Type	Required	Description
BandwidthPackageId	String	Yes	The ID of the NAT bandwidth package.
RemovedIpAddresses.n	String	No	The ID of the public IP address n to be removed. Valid values of n: 1 to 20.
ClientToken	String	No	The client token that is used to ensure the idempotence of the request. You can use the client to generate this value, but you must ensure that it is unique among different requests. The token can contain only ASCII characters, and cannot exceed 64 characters in length.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=RemoveBandwidthPackageIps
&RemovedIpAddresses. 1=nateip-1110a2lxxxxxxxx
&RemovedIpAddresses. 2=nateip-11s2jemxxxxxxxx
&BandwidthPackageId=bwp-11odxu2kxxxxxxxx
&RegionId=cn-shanghai
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<RemoveBandwidthPackageIpsResponse>
    <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</RemoveBandwidthPackageIpsResponse>
```

- JSON format

```
{
   "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
 }
```

2.14.1.13.13. CreateForwardEntry

You can call this topic to add DNAT entries to a DNAT table.

Each DNAT entry consists of five elements: ExternalIp, ExternalPort, Protocol, InternalIp, and InternalPort.

After a DNAT entry is added, the NAT Gateway forwards packets of the specified protocol received from [ExternalIp: ExternalPort] to [InternalIp: InternalPort], and sends the response back through the same route.

When you call this operation, make sure that the following requirements are met:

- A NAT Gateway and a user-created SNAT Gateway (using an ECS instance as the SNAT Gateway) cannot coexist in a VPC.
- After you have created a NAT Gateway, a route entry is automatically added to the routing table of the VPC. The destination CIDR block is 0.0.0.0/0 and the next-hop is the NAT Gateway. The entry ensures that traffic is routed to the NAT Gateway.
- If the VPC routing table already contains an entry with a destination CIDR block of 0.0.0.0/0, delete this entry. Otherwise, you cannot create a NAT Gateway.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateForwardEntry*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
ForwardTableId	String	Yes	The ID of the DNAT table.
ExternalIp	String	Yes	The public IP address.
IpProtocol	String	Yes	The protocol type. Valid values: • *TCP* • *UDP* • *Any*
ExternalPort	String	No	The public port. Valid values: 1 to 65535.
InternalIp	String	Yes	The destination private IP address.
InternalPort	String	No	The destination private port. Valid values: 1 to 65535.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
ForwardEntryId	String	The ID of the DNAT entry.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateForwardEntry
&ExternalIp=139.xx.xx. 107
&RegionId=cn-shanghai
&ExternalPort=Any
&InternalIp=192.xx.xx. 1
&ForwardTableId=ftb-11tc6xgmxxxxxxxx
&IpProtocol=Any
&InternalPort=Any
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<CreateForwardEntryResponse>
      <ForwardEntryId>fwd-119smwxxxxxxxx</ForwardEntryId>
      <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</CreateForwardEntryResponse>
```

- JSON format

```
{
    "ForwardEntryId": "fwd-119smxxxxxxxx",
    "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
}
```

2.14.1.13.14. DeleteForwardEntry

You can call this operation to delete a DNAT entry.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteForwardEntry*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
ForwardTableId	String	Yes	The ID of the DNAT table.
ForwardEntryId	String	Yes	The ID of the DNAT entry.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteForwardEntry
&ForwardEntryId=dnat-bs5bexxxxxxxx
&RegionId=cn-shanghai
&ForwardTableId=stb-244xxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DeleteForwardEntryResponse>
    <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</DeleteForwardEntryResponse>
```

- JSON format

```
{
    "RequestId": "69B31D6E-9F34-4A5A-8DBC-230A3918E828"
}
```

2.14.1.13.15. ModifyForwardEntry

You can call this operation to modify a DNAT entry.

> **Note** You cannot modify a DNAT entry if any DNAT entry in the DNAT table is in the Pending or Modifying state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyForwardEntry*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
ForwardTableId	String	Yes	The ID of the DNAT table.
ForwardEntryId	String	Yes	The ID of the DNAT entry.
ExternalIp	String	No	The public IP address.
IpProtocol	String	No	The protocol type. Valid values: • *TCP* • *UDP* • *Any*
ExternalPort	String	No	The public port. Valid values: 1 to 65535.
InternalIp	String	No	The destination private IP address.
InternalPort	String	No	The destination private port. Valid values: 1 to 65535.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
ForwardEntryId	String	The ID of the DNAT entry.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateForwardEntry
&ExternalIp=139.xx.xx. 107
&RegionId=cn-shanghai
&ExternalPort=Any
&InternalIp=192.xx.xx. 1
&ForwardTableId=ftb-11tc6xxxxxxxxx
&IpProtocol=Any
&InternalPort=Any
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<CreateForwardEntryResponse>
    <ForwardEntryId>fwd-119smw5xxxxxxxx</ForwardEntryId>
    <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</CreateForwardEntryResponse>
```

- JSON format

```
{
  "ForwardEntryId": "fwd-119smw5xxxxxxxx",
  "RequestId": "2315DEB7-5E92-423A-91F7-4C1EC9AD97C3"
}
```

2.14.1.13.16. DescribeForwardTableEntries

You can call this operation to query DNAT entries in a DNAT table.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeForwardTableEntries*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
ForwardTableId	String	No	The ID of the DNAT table.

Parameter	Type	Required	Description
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
ForwardTableEntries	List	The details about the NAT Gateway. For more information, see the ForwardTableEntry list.

ForwardTableEntry list

Parameter	Type	Description
ForwardTableId	String	The ID of the DNAT table that the DNAT entry belongs to.
ForwardEntryId	String	The ID of the DNAT entry.
ExternalIp	String	The public IP address.
ExternalPort	String	The public port.
IpProtocol	String	The protocol type.
InternalIp	String	The private IP address.
InternalPort	String	The private port.

Parameter	Type	Description
Status	String	The status of the DNAT entry. Valid values: • *Pending*: The DNAT entry is being configured. *Available*: The DNAT entry is available. *Modifying*: The DNAT entry is being modified.

Examples

Sample requests

```
https://vpc.example.com/?&Action=DescribeForwardTableEntries
&RegionId=cn-shanghai
&ForwardTableId=ftb-11tc6xxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeForwardTableEntriesResponse>
  <PageNumber>1</PageNumber>
  <TotalCount>1</TotalCount>
  <PageSize>10</PageSize>
  <RequestId>74F2BAD8-AF35-4C57-81F1-5E33BFB0F5F2</RequestId>
  <ForwardTableEntries>
    <ForwardTableEntry>
      <Status>Available</Status>
      <IpProtocol>any</IpProtocol>
      <ForwardEntryId>fwd-bp18jpb1tlm55xxxxxxxx</ForwardEntryId>
      <ExternalIp>47.xx.xx. 33</ExternalIp>
      <ForwardTableId>ftb-bp15o9aylj19vfxxxxxxxx</ForwardTableId>
      <ExternalPort>any</ExternalPort>
      <InternalPort>any</InternalPort>
      <InternalIp>192.168.xx.xx</InternalIp>
    </ForwardTableEntry>
  </ForwardTableEntries>
</DescribeForwardTableEntriesResponse>
```

- JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "PageSize": 10,
  "RequestId": "74F2BAD8-AF35-4C57-81F1-5E33BFB0F5F2",
  "ForwardTableEntries": {
    "ForwardTableEntry": [
      {
        "Status": "Available",
        "IpProtocol": "any",
        "ForwardEntryId": "fwd-bp18jpb1tlm55xxxxxxxx",
        "ExternalIp": "47.xx.xx. 33",
        "ForwardTableId": "ftb-bp15o9aylj19vxxxxxxxx",
        "ExternalPort": "any",
        "InternalPort": "any",
        "InternalIp": "192.168.xx.xx"
      }
    ]
  }
}
```


2.14.1.13.17. CreateSnatEntry

You can call this operation to add SNAT entries to a SNAT table.

Each SNAT entry contains a VSwitch ID and a public IP address (SnatIp). After you have added a SNAT entry, ECS instances can access the public network through the public IP address.

When you call this operation, make sure that the VSwitch specified in the SNAT entry meet the following requirements:

- The VSwitch must belong to the same VPC as the NAT Gateway.
- Each VSwitch can belong to only one SNAT entry.
- A public IP address cannot be used by a DNAT entry and a SNAT entry at the same time.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateSnatEntry*.

Parameter	Type	Required	Description
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
SnatTableId	String	Yes	The ID of the SNAT table.
SourceVSwitchId	String	Yes	The ID of the VSwitch.
SourceCIDR	String	Yes	The CIDR block of the VSwitch, such as 10.1.1.0/24. Note You cannot specify this parameter and SourceVSwitchId at the same time.
SnatIp	String	No	The public IP address. You can separate multiple IP addresses with commas (,). Example: 47.XX.XX.98,47.XX.XX.99,47.XX.XX.241

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
SnatEntryId	String	The ID of the SNAT entry.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateSnatEntry
&RegionId=cn-shanghai
&SnatTableId=stb-gz3r3odxxxxxxxx
&SnatIp=139.xx.xx.40
&SourceVSwitchId=vsw-yrv0wixxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<CreateSnatEntryResponse>
    <SnatEntryId>snat-kmd6nvxxxxxxxx</SnatEntryId>
    <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
 </CreateSnatEntryResponse>
```

- JSON format

```
{
  "RequestId": "69B31D6E-9F34-4A5A-8DBC-230A3918E828",
  "SnatEntryId": "snat-kmd6nvxxxxxxxx"
}
```

2.14.1.13.18. DeleteSnatEntry

You can call this operation to delete a SNAT entry.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteSnatEntry*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
SnatTableId	String	Yes	The ID of the SNAT table.
SnatEntryId	String	Yes	The ID of the SNAT entry.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteSnatEntry
&SnatEntryId=snat-bs5bezbxxxxxxxx
&RegionId=cn-shanghai
&SnatTableId=stb-244fxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DeleteSnatEntryResponse>
   <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</DeleteSnatEntryResponse>
```

- JSON format

```
{
   "RequestId": "69B31D6E-9F34-4A5A-8DBC-230A3918E828"
}
```

2.14.1.13.19. ModifySnatEntry

You can call this operation to modify the SNATed IP address (public IP address) of a specified SNAT entry.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifySnatEntry*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
SnatTableId	String	Yes	The ID of the SNAT table.
SnatEntryId	String	Yes	The ID of the SNAT entry.

Parameter	Type	Required	Description
SnatIp	String	No	The public IP address. You can separate multiple IP addresses with commas (,). Example: 47.XX.XX.98,47.XX.XX.99,47.XX.XX.241

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifySnatEntry
&SnatEntryId=snat-bs5bezbmxxxxxxxx
&RegionId=cn-shanghai
&SnatTableId=stb-gz3r3oxxxxxxxx
&SnatIp=139.xx.xx.107
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<ModifySnatEntryResponse>
    <RequestId>2315DEB7-5E92-423A-91F7-4C1EC9AD97C3</RequestId>
</ModifySnatEntryResponse>
```

- JSON format

```
{
   "RequestId": "69B31D6E-9F34-4A5A-8DBC-230A3918E828"
 }
```

2.14.1.13.20. DescribeSnatTableEntries

You can call this operation to query SNAT entries in a SNAT table.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeSnatTableEntries*.
RegionId	String	Yes	The region ID of the NAT Gateway. You can call the DescribeRegions operation to query the latest region list.
SnatTableId	String	Yes	The ID of the SNAT table.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
SnatTableEntries	List	The details about the SNAT entries.

SnatEntry

Parameter	Type	Description
SnatTableId	String	The ID of the SNAT table to which the SNAT entries belong.
SnatEntryId	String	The ID of the SNAT entry.
SourceVSwitchId	String	The ID of the VSwitch that accesses the public network through SNAT.
SourceCIDR	String	The source CIDR block of the SNAT entry.

Parameter	Type	Description
SnatIp	String	The public IP address of the SNAT entry.
Status	String	The status of the SNAT entry. Valid values: • *Pending*: The SNAT entry is being configured. *Available*: The SNAT entry is available. *Modifying*: The SNAT entry is being modified.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeSnatTableEntries
&RegionId=cn-shanghai
&SnatTableId=stb-gz3r3odxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeSnatTableEntriesResponse>
  <PageNumber>1</PageNumber>
  <PageSize>10</PageSize>
  <RequestId>6D7E89B1-1C5B-412B-8585-4908E222EED5</RequestId>
  <SnatTableEntries>
    <SnatTableEntry>
      <SnatEntryId>snat-kmd6nv8xxxxxxxx</SnatEntryId>
      <SnatIp>139.xx.xx. 40</SnatIp>
      <SnatTableId>stb-gz3r3odxxxxxxxx</SnatTableId>
      <SourceCIDR>192.168.1.0/24</SourceCIDR>
      <SourceVSwitchId>vsw-yrv0xxxxx</SourceVSwitchId>
      <Status>Available</Status>
    </SnatTableEntry>
    <SnatTableEntry>
      <SnatEntryId>snat-bs5bezbxxxxxxxx</SnatEntryId>
      <SnatIp>139.xxx.xx. 40</SnatIp>
      <SnatTableId>stb-gz3r3oxxxxxxxx</SnatTableId>
      <SourceCIDR>192.168.3.0/24</SourceCIDR>
      <SourceVSwitchId>vsw-3xbxxxxx</SourceVSwitchId>
      <Status>Available</Status>
    </SnatTableEntry>
  </SnatTableEntries>
  <TotalCount>2</TotalCount>
</DescribeSnatTableEntriesResponse>
```

- JSON format

```
{
 "PageNumber": 1,
 "PageSize": 10,
 "RequestId": "6D7E89B1-1C5B-412B-8585-4908E222EED5",
 "SnatTableEntries": {
  "SnatTableEntry": [
   {
    "SnatEntryId": "snat-kmd6nvxxxxxxxx",
    "SnatIp": "139.xx.xx. 40",
    "SnatTableId": "stb-gz3r3odxxxxxxxx",
    "SourceCIDR": "192.168.1.0/24",
    "SourceVSwitchId": "vsw-yrv0xxxxx",
    "Status": "Available"
   },
   {
    "SnatEntryId": "snat-bs5bezbxxxxxxxx",
    "SnatIp": "139.xx.xx. 40",
    "SnatTableId": "stb-gz3r3odxxxxxxxx",
    "SourceCIDR": "192.168.3.0/24",
    "SourceVSwitchId": "vsw-3xbxxxxx",
    "Status": "Available"
   }
  ]
 },
 "TotalCount": 2
}
```


2.14.1.14. High-Availability Virtual IP

2.14.1.14.1. CreateHaVip

You can call this operation to create a High-Availability Virtual IP (HaVip).

When you call this operation, make sure that the following requirements are met:

- You can create a maximum of five HaVips for a VPC.
- Before you delete a VPC, you must delete the HaVips that you have created for it.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateHaVip*.
RegionId	String	Yes	The region ID of the HaVip instance. You can call the DescribeRegions operation to query the latest region list.
VSwitchId	String	Yes	The ID of the VSwitch to which the HaVip instance belongs.
IpAddress	String	No	The IP address of the HaVip instance. If this parameter is not specified, an idle IP address of the specified VSwitch is randomly allocated.
Description	String	No	The description of the HaVip instance. The description must be 2 to 256 characters in length. It must start with a letter but cannot start with `http://` or `https://`.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
HaVipId	String	The ID of the HaVip instance.

Error codes

Error code	Error message	HTTP status code	Description
`InvalidRegionId.NotFound`	`The RegionId provided does not exist in our records.`	404	The error message returned because the specified RegionId does not exist.
`MissingParameter`	`The input parameter "$ParammeterName" that is mandatory for processing this request is not supplied.`	400	The error message returned because a required parameter is missing.

Error code	Error message	HTTP status code	Description
InvalidVSwitchId.NotFound	The specified VSwitch does not exist in the specified region.	404	The error message returned because the specified VSwitchId does not exist.
InvalidIPAddress.Malformed	The specified IPAddress is wrongly formed.	400	The error message returned because the IP address format is incorrect.
InvalidIPAddress.OutOfRange	The specified IPAddress is out of VSwitch CIDR.	400	The error message returned because the specified IP address is outside the range of the VSwitch CIDR block.
InvalidIPAddress.NotAvailable	The specified IPAddress is not available because it is a system reserved IPAddress.	400	The error message returned because the specified IP address is a system reserved address and is therefore unavailable.
InvalidIPAddress.AlreadyUsed	The specified IPAddress is already used by other resource.	400	The error message returned because the specified IP address is already used by other resources.
InvalidDescription.Malformed	The specified Description is wrongly formed.	403	The error message returned because the format of the Description is invalid.
QuotaExceeded.HaVip	Living HaVip quota exceeded.	403	The error message returned because the number of HaVips for the account has exceeded the upper limit.
CountLimitExceed.HaVipInVpc	Specified Vpc exceeds the quota of max number of ha-vip count.	403	The error message returned because the number of HaVips within the VPC has reached the upper limit.

Examples

Sample requests

```
https://vpc.example.com/?Action=CreateHaVip
&VSwitchId=vsw-25b7pvxxxxxxxx
&amp;RegionId=cn-hangzhou
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<CreateHaVipResponse>
   <RequestId>C44F62BE-9CE7-4277-B117-69243F3988BF</RequestId>
   <HaVipId>havip-2zeo05qre24nhrqpyxxxxxxxx</HaVipId>
</CreateHaVipResponse>
```

- JSON format

```
{
   "RequestId": "C44F62BE-9CE7-4277-B117-69243F3988BF",
   "HaVipId": "havip-2zeo05qre24nhrqpyxxxxxxxx"
}
```

2.14.1.14.2. ModifyHaVipAttribute

You can call this operation to modify the description of a HaVip instance.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyHaVipAttribute*.
RegionId	String	Yes	The region ID of the HaVip instance. You can call the DescribeRegions operation to query the latest region list.
HaVipId	String	Yes	The ID of the HaVip instance that you want to modify.
Description	String	No	The description of the HaVip instance.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Examples

Sample requests

```
https://vpc.example.com/?Action=ModifyHaVipAttribute
&HaVipId=havip-2zeo05qre24nhrqpyfdxxxxxxxx
&RegionId=cn-shanghai
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<ModifyHaVipAttributeResponse>
  <RequestId>C44F62BE-9CE7-4277-B117-69243F3988BF</RequestId>
</ModifyHaVipAttributeResponse>
```

- JSON format

```
{
  "RequestId": "C44F62BE-9CE7-4277-B117-69243F3988BF"
}
```

2.14.1.14.3. DeleteHaVip

You can call this operation to delete a High-Availability Virtual IP (HaVip).

When you call this operation, make sure that the following requirements are met:

- You can only delete a HaVip in the Available state.
- Make sure that there is no route destined for the HaVip that you want to delete.
- Make sure that the HaVip that you want to delete is not bound to an EIP.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteHaVip*.
RegionId	String	Yes	The region ID of the HaVip instance. You can call the DescribeRegions operation to query the latest region list.
HaVipId	String	Yes	The ID of the HaVip instance that you want to delete.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned because the specified RegionId does not exist.
MissingParameter	The input parameter "$ParammeterName" that is mandatory for processing this request is not supplied.	400	The error message returned because a required parameter is missing.
InvalidHaVipId.NotFound	The specified HaVip does not exist in the specified region.	404	The error message returned because the specified HaVip does not exist.
IncorrectStatus	HaVip can be deleted only when it's status is Available.	400	The error message returned because the HaVip instance to be deleted is not in the Available state.
DependencyViolation.HaVipReferedByRouteEntry	HaVip cannot be deleted when it is refered by a route table entry as next hop.	400	The error message returned because the specified HaVip is specified as the next-hop for a route entry.
DependencyViolation.HaVipAssociatedWithEIP	HaVip cannot be deleted when it is associated with a EIP.	400	The error message returned because the specified HaVip is bound to an EIP.

Examples

Sample requests

```
https://vpc.example.com/?Action=DeleteHaVip
&HaVipId=havip-2zeo05qre24nhrqpyfds2
&RegionId=cn-shanghai
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DeleteHaVipResponse>
   <RequestId>C44F62BE-9CE7-4277-B117-69243F3988BF</RequestId>
</DeleteHaVipResponse>
```

- JSON format

```
{
   "RequestId": "C44F62BE-9CE7-4277-B117-69243F3988BF"
}
```

2.14.1.14.4. AssociateHaVip

You can call this operation to bind a HaVip to an ECS instance of the VPC network.

When you call this operation, make sure that the following requirements are met:

- The HaVip takes effect immediately when it is bound to an ECS instance of the VPC network. You do not need to restart the ECS instance. However, you must configure the HaVip on the instance NIC.
- The HaVip and the ECS instances you want to bind must be managed by the same VSwitch.
- You can bind a HaVip to a maximum of two ECS instances.
- You can bind an ECS instance only when it is in the Running or Stopped state.
- You can bind a HaVip instance only when it is in the Available or InUse state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *AssociateHaVip*.
RegionId	String	Yes	The region ID of the HaVip instance. You can call the DescribeRegions operation to query the latest region list.
HaVipId	String	Yes	The ID of the HaVip instance.
InstanceId	String	Yes	The ID of the ECS instance that you want to bind.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
HaVipId	String	The ID of the HaVip instance.

Error codes

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned because the specified RegionId does not exist.
MissingParameter	The input parameter "$ParammeterName" that is mandatory for processing this request is not supplied.	400	The error message returned because a required parameter is missing.
InvalidHaVipId.NotFound	The specified HaVip does not exist in the specified region.	404	The error message returned because the specified HaVip does not exist.
InvalidInstanceId.NotFound	The specified Instance does not exist in the specified region.	404	The error message returned because the specified ECS instance does not exist.
IncorrectHaVipStatus	HaVip can be operated by this action only when it's status is Available or InUse.	400	The error message returned because the HaVip instance that you want to bind is not in the Available or InUse state.
IncorrectInstanceStatus	ECS instance can be operated by this action only when it's status is Running or Stopped.	400	The error message returned because the ECS instance that you want to bind is not in the Running or Stopped state.

Error code	Error message	HTTP status code	Description
CountLimitExceeded.HaVipOnECSInstance	The amount of Instance associated with the specified HaVip reach its limits.	400	You can bind a HaVip to a maximum of two ECS instances. The error message returned because the number of ECS instances bound to the specified HaVip has exceeded the upper limit.
CountLimitExceed.HaVipOnInstance	The amount of HaVip associated with the specified Instance reach its limits.	400	The error message returned because the number of HaVips bound to the specified ECS instance has reached the upper limit.
NotBelongToSameVSwitch	The specified HaVip and ECSInstance do not belong to same VSwitch.	400	The error message returned because the specified HaVip and the ECS instance are not managed by the same VSwitch.

Examples

Sample requests

```
https://vpc.example.com/?Action=AssociateHaVip
&HaVipId=havip-2zeo05qre24nhrxxxxxxxx
&RegionId=cn-shanghai
&InstanceId=i-faf344422ffsxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<AssociateHaVipResponse>
   <RequestId>C44F62BE-9CE7-4277-B117-69243F3988BF</RequestId>
</AssociateHaVipResponse>
```

- JSON format

```
{
   "RequestId": "C44F62BE-9CE7-4277-B117-69243F3988BF"
}
```

2.14.1.14.5. UnassociateHaVip

You can call this operation to unbind a HaVip from an ECS instance of the VPC network.

When you call this operation, make sure that the following requirements are met:

- You can unbind an ECS instance when it is in the Running or Stopped state.
- A HaVip instance can only be unbound when it is in the Available or InUse state.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *UnassociateHaVip*.
RegionId	String	Yes	The region ID of the HaVip instance. You can call the DescribeRegions operation to query the latest region list.
HaVipId	String	Yes	The ID of the HaVip instance.
InstanceId	String	Yes	The ID of the ECS instance that you want to unbind.
Force	String	No	Specifies whether to force an unbinding operation. Valid values: *True and False*. Default value: False. **Note** You cannot unbind the primary instance if the parameter value is *False*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned because the specified RegionId does not exist.

Error code	Error message	HTTP status code	Description
InvalidHaVipId.NotFound	The specified HaVip does not exist in the specified region.	404	The error message returned because the specified HaVip does not exist.
InvalidInstanceId.NotFound	The specified Instance does not exist in the specified region.	404	The error message returned because the specified ECS instance does not exist.
IncorrectHaVipStatus	HaVip can be operated by this action only when it's status is Available or InUse.	400	The error message returned because the HaVip instance that you want to unbind is not in the Available or InUse state.
IncorrectInstanceStatus	ECS instance can be operated by this action only when it's status is Running or Stopped.	400	The error message returned because the ECS instance that you want to unbind is not in the Running or Stopped state.
Forbidden.UnassociateMaste	Unassociating a master instance is not allowed unless the parameter Force is True.	400	The error message returned because the primary instance cannot be unbound. You can unbind the primary instance only after you have set Force to *True*.
NotBelongToSameVSwitch	The specified HaVip and ECSInstance do not belong to same VSwitch.	400	The error message returned because the specified HaVip and the ECS instance are not managed by the same VSwitch.

Examples

Sample requests

```
https://vpc.example.com/?Action=UnassociateHaVip
&HaVipId=havip-2zeo05qre24nhrqxxxxxxxx
&RegionId=cn-shanghai
&InstanceId=i-faf344422ffsxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<UnassociateHaVipResponse>
   <RequestId>C44F62BE-9CE7-4277-B117-69243F3988BF</RequestId>
</UnassociateHaVipResponse>
```

- JSON format

```
{
   "RequestId": "C44F62BE-9CE7-4277-B117-69243F3988BF"
}
```

2.14.1.14.6. DescribeHaVips

You can call this operation to query HaVip instances within a specified region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeHaVips*.
RegionId	String	Yes	The region ID of the HaVip instance. You can call the DescribeRegions operation to query the latest region list.
Filter.n.Key	String	Yes	Specifies filter condition n. You can specify a maximum of five filter conditions. Valid values of n: 1 to 5. You can specify multiple values for each filter condition. If you use "or" to separate multiple values, the system returns results that match at least one of the filter conditions. If you use "and" to separate multiple values, the system returns results that match all filter conditions. The following filter conditions are available: • *VpcId*: the ID of the VPC • VSwitchId: the ID of the VSwitch • *Status*: the status of the HaVip instance • *HaVipId*: the ID of the HaVip instance • *HaVipAddress*: the IP address of the HaVip instance
Filter.n.Value.m	String	Yes	Specifies value m of filter condition n. Valid values of *m*: 1 to 5.

Parameter	Type	Required	Description
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
HaVipItemType	List	The details about the HaVip.

HaVipItemType

Parameter	Type	Description
HaVipId	String	The ID of the HaVip instance.
RegionId	String	The region ID of the HaVip instance.
VpcId	String	The ID of the VPC to which the HaVip instance belongs.
VSwitchId	String	The ID of the VSwitch to which the HaVip instance belongs.
IpAddress	String	The private IP address of the HaVip instance.
Status	String	The status of the HaVip instance.
AssociatedInstances	String	The ECS instances that are bound to the HaVip instance.
MasterInstanceId	String	The ID of the HaVip instance that has been bound to the private IP address.
AssociatedEipAddresses	String	The list of EIPs that are bound to the HaVip instance.
Description	String	The description of the HaVip instance.
CreationTime	String	The time when the HaVip instance was created.

Error codes

Error code	Error message	HTTP status code	Description
InvalidRegionId.NotFound	The RegionId provided does not exist in our records.	404	The error message returned because the specified RegionId does not exist.
MissingParameter	The input parameter "$ParammeterName" that is mandatory for processing this request is not supplied.	400	The error message returned because a required parameter is missing.
RepeatedParameter.$ParammeterName	Specified parameter $ParammeterName is repeated.	400	The error message returned because the specified parameter is repeated.
NonsequenceParameter.{xxx.n.yyy.m}	Specified parameter is not a continuous sequence.	400	The error message returned because the key or value of the Filter does not start from 1 or in a continuous sequence.
InvalidFilterKey.ValueNotSupported	Specified filter key is not supported: Filter.X.key	400	The error message returned because the specified filter condition is not supported.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeHaVips
&RegionId=cn-hangzhou
&Filter=HaVipId.havip-bp149uyvut73dplxxxxxxxx
&Common request parameters
```

Sample responses

- XML format

```
<? xml version="1.0" encoding="UTF-8" ? >
<DescribeHaVipsResponse>
<PageNumber>1</PageNumber>
<TotalCount>1</TotalCount>
<HaVips>
  <HaVip>
  <Status>Available</Status>
  <Description></Description>
  <MasterInstanceId></MasterInstanceId>
  <AssociatedInstances></AssociatedInstances>
  <AssociatedEipAddresses></AssociatedEipAddresses>
  <CreateTime>2018-07-03T14:25:26Z</CreateTime>
  <RegionId>cn-hangzhou</RegionId>
  <IpAddress>192.xx.xx. 27</IpAddress>
  <HaVipId>havip-bp149uyvut73dxxxxxxxx</HaVipId>
  <VSwitchId>vsw-bp1pkt1fba8e8xxxxxxxx</VSwitchId>
  <VpcId>vpc-bp1kcm36tevkpxxxxxxxx</VpcId>
  </HaVip>
</HaVips>
<PageSize>10</PageSize>
<RequestId>33E480C5-B46F-4CA5-B6FD-D77C746E86AB</RequestId>
</DescribeHaVipsResponse>
```

- JSON format

```
{
  "PageNumber": 1,
  "TotalCount": 1,
  "HaVips": {
    "HaVip": [
      {
        "Status": "Available",
        "Description": "",
        "MasterInstanceId": "",
        "AssociatedInstances": {
          "associatedInstance": [ ]
        },
        "AssociatedEipAddresses": {
          "associatedEipAddresse": [ ]
        },
        "CreateTime": "2018-07-03T14:25:26Z",
        "RegionId": "cn-hangzhou",
        "IpAddress": "192.xx.xx. 27",
        "HaVipId": "havip-bp149uyvut73dxxxxxxxx",
        "VSwitchId": "vsw-bp1pkt1fba8e82xxxxxxxx",
        "VpcId": "vpc-bp1kcm36tevkpmxxxxxxxx"
      }
    ]
  },
  "PageSize": 10,
  "RequestId": "33E480C5-B46F-4CA5-B6FD-D77C746E86AB"
}
```


2.14.1.15. DescribeRegions

This topic describes how to query available regions.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeRegions*.

Response parameters

Name	Type	Description
RequestId	String	The request ID.
Regions	List	The list of available regions.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeRegions
&<Common request parameters>
```

Sample responses

XML format

```
<? xml version="1.0" encoding="utf-8"? >
<DescribeRegionsResponse>
 <RequestId>611CB80C-B6A9-43DB-9E38-0B0AC3D9B58F</RequestId>
 <Regions>
  <Region>
   <RegionId>cn-hangzhou</RegionId>
  </Region>
  <Region>
   <RegionId>cn-qingdao</RegionId>
  </Region>
 </Regions>
</DescribeRegionsResponse>
```

JSON format

```
{
  "RequestId": "611CB80C-B6A9-43DB-9E38-0B0AC3D9B58F",
  "Regions": {
    "Region": [
      {
        "RegionId": "cn-hangzhou "
      },
      {
        "RegionId": "cn-qingdao"
      }
    ]
  }
}
```

2.14.1.16. DescribeZones

This topic describes how to query zones in a specific region.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeZones*.
RegionId	String	Yes	The region ID. You can call DescribeRegions to obtain the region ID.

Response parameters

Name	Type	Description
RequestId	String	The request ID.
Zones	List	The list of zones.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeZones
&RegionId=cn-hangzhou
&<Common request parameters>
```

Sample responses

XML format

```
<? xml version="1.0" encoding="utf-8"? >
<DescribeZonesResponse>
 <Zones>
  <Zone>
   <AvailableResourceCreation>
    <ResourceTypes>Instance</ResourceTypes>
    <ResourceTypes>Disk</ResourceTypes>
   </AvailableResourceCreation>
   <LocalName/>
   <ZoneId>cn-hangzhou-d</ZoneId>
   <AvailableDiskCategories>
    <DiskCategories>cloud</DiskCategories>
   </AvailableDiskCategories>
  </Zone>
  <Zone>
   <AvailableResourceCreation>
    <ResourceTypes>Instance</ResourceTypes>
    <ResourceTypes>Disk</ResourceTypes>
   </AvailableResourceCreation>
   <LocalName/>
   <ZoneId>cn-hangzhou-b</ZoneId>
   <AvailableDiskCategories>
    <DiskCategories>cloud</DiskCategories>
   </AvailableDiskCategories>
  </Zone>
 </Zones>
 <RequestId>6DB97BCC-92BA-424D-A7C8-3F6486612BAE</RequestId>
</DescribeZonesResponse>
```

JSON format

```
{
  "RequestId": "A347EF0E-BBCC-4EFA-BD79-27AA3ACFD1BF",
  "Zones": {
    "Zone": [
      {
        "AvailableDiskCategories": {
          "DiskCategories": [
            "cloud"
          ]
        },
        "AvailableResourceCreation": {
          "ResourceTypes": [
            "Instance",
            "Disk"
          ]
        },
        "LocalName": "",
        "ZoneId": "cn-hangzhou-d"
      },
      {
        "AvailableDiskCategories": {
          "DiskCategories": [
            "cloud"
          ]
        },
        "AvailableResourceCreation": {
          "ResourceTypes": [
            "Instance",
            "Disk"
          ]
        },
        "LocalName": "",
        "ZoneId": "cn-hangzhou-b"
      }
    ]
  }
}
```


2.14.1.17. DescribeAccessPoints

You can call this operation to query physical connection access points in a region.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAccessPoints*.
RegionId	String	Yes	The region ID of the access point. You can call the DescribeRegions operation to query the latest region list.
PageNumber	Integer	No	The number of the page to return. Default value: *1*.
PageSize	Integer	No	The number of entries to return on each page. Maximum value: *50*. Default value: *10*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	String	The total number of entries.
PageNumber	Integer	The current page number.
PageSize	String	The number of entries on each page.
AccessPointSet	List	A list of access points.

Examples

Sample requests

```
https://vpc.example.com/?Action=DescribeAccessPoints
&RegionId=cn-beijing
&Common request parameters
```

Sample responses

JSON format

```
{
  "AccessPointSet": {
    "AccessPointType": [
      {
        "Name": "Beijing-Fengtai-A",
        "Status": "recommended",
        "Description": "cn-beijing-ft-cxp32",
        "Type": "VPC",
        "Location": "",
        "HostOperator": "Haokuan",
        "AttachedRegionNo": "cn-beijing",
        "AccessPointId": "ap-cn-beijing-ft-A"
       }
"PageNumber": 1,
"TotalCount": 1,
"PageSize": 10,
"RequestId": "3E85D803-C7CF-4BCD-9CFE-6DBA1DFFA027"
}
```


XML format


```
<? xml version="1.0" encoding="UTF-8" ? >
</DescribeAccessPointsResponse>
    <AccessPointSet>
        <AccessPointType>
        <Name>Beijing-Fengtai-A</Name>
        <Status>recommended</Status>
        <Description>cn-beijing-ft-cxp32</Description>
        <Type>VPC</Type>
        <Location></Location>
        <HostOperator>xxx</HostOperator>
        <AttachedRegionNo>cn-beijing</AttachedRegionNo>
        <AccessPointId>ap-cn-beijing-ft-A</AccessPointId>
        </AccessPointType>
    </AccessPointSet>
    <PageNumber>1</PageNumber>
    <TotalCount>1</TotalCount>
    <PageSize>10</PageSize>
<RequestId>3E85D803-C7CF-4BCD-9CFE-6DBA1DFFA027</RequestId>
</DescribeAccessPointsResponse>
```

2.14.2. SDK reference

2.14.2.1. Call the SDK for Java

2.14.2.1.1. Quick start

This topic describes how to obtain and call the VPC Java SDK.

Environment preparation

- Before using the Java SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to obtain and view your AccessKey in Apsara Stack Management Console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.
- The Apsara Stack Java SDK requires JDK V1.6 and later.

Install the Apsara Stack Java SDK

If you use Apache Maven to manage Java projects, you need only to import the JAR file to *pom.xml* of the project.

To use the service development kit, you must install the SDK core library and the service SDK.

The version of the SDK core library is 3.7.1. The version of the VPC SDK is *1.0*.

```
<dependencies>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-sdk-core</artifactId>
      <version>3.7.1</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-core-3.7.1.jar</systemPath>
    </dependency>
    <dependency>
      <groupId>com.aliyun</groupId>
      <artifactId>aliyun-java-sdk-vpc</artifactId>
      <version>1.0</version>
      <scope>system</scope>
      <systemPath>${project.basedir}/lib/aliyun-java-sdk-vpc-1.0.jar</systemPath>
    </dependency>
  </dependencies>
```

Call the Java SDK

The following code provides an example of how to call the Apsara Stack Java SDK:

1. Create a DefaultAcsClient instance and initialize it.
2. Create an API request and set its parameters.

3. Initiate the request and handle the response or exceptions.

```
import java.util.UUID;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.IAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.exceptions.ServerException;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.vpc.model.v20160428. CreateVpcRequest;
import com.aliyuncs.vpc.model.v20160428. CreateVpcResponse;
public class Demo {
    public static void main(String[] args) {
        // Create a DefaultAcsClient instance and initialize it.
        DefaultProfile profile = DefaultProfile.getProfile(
            "<your-region-id>", // Your region ID.
            "<your-access-key-id>", // Your AccessKey ID.
            "<your-access-key-secret>"); // Your AccessKey Secret.
        IAcsClient client = new DefaultAcsClient(profile);
         // Create an API request and set its parameters.
        CreateVpcRequest request = new CreateVpcRequest();
        request.setVpcName("MyVpc");
        request.setCidrBlock("192.168.0.0/16");
        request.setClientToken(UUID.randomUUID().toString());
        // Initiate the request and handle the response or exceptions.
        CreateVpcResponse response;
        try {
            response = client.getAcsResponse(request);
            String vpcId = response.getVpcId();
            System.out.println("Create vpc success, vpcId = " + vpcId);
        } catch (ServerException e) {
            e.printStackTrace();
        } catch (ClientException e) {
            e.printStackTrace();
        }
    }
}
```

2.14.2.1.2. Usage

2.14.2.1.2.1. Install the SDK for Java

This topic describes how to install and use the VPC SDK for Java.

The VPC SDK for Java supports JDK V1.6 and later. You can import the JAR file to install the JDK.

You can click Here to download the JAR file for VPC.

You can import the JAR file to install the VPC SDK for Java regardless of the IDE (Eclipse or IntelliJ).

The installation method is as follows:

- Use Eclipse

  To install the VPC SDK for Java through Eclipse, perform the following operations:

  i. Copy the downloaded *aliyun-java-sdk-vpc-1.0.jar* file to your project folder.
  ii. Open your project in Eclipse, right-click the project, and choose **Properties** from the shortcut menu.
  iii. In the dialog box that appears, choose **Java Build Path** > **Libraries** > **Add JARs** to add the downloaded JAR file.
  iv. Click **Apply and Close**.

- Use IntelliJ

  To install the VPC SDK for Java through IntelliJ, perform the following operations:

  i. Copy the downloaded *aliyun-java-sdk-vpc-1.0.jar* file to your project folder.
  ii. Open your project in IntelliJ, and choose **File** > **Project Structure** from the menu.
  iii. Click **Apply**, and then click **OK**.

2.14.2.1.2.2. Configure identity verification credentials

When using SDKs to access Apsara Stack resources, you must provide an authorized Apsara Stack tenant account to verify your identity.

The Java SDK supports the use of AccessKey pairs for identity verification. For more information about how to obtain an AccessKey, see Obtain an AccessKey pair.

To use AccessKey pairs as credentials, you must configure your credentials when initializing the client.

> **Notice** Ensure that code containing your AccessKey is kept confidential and is not exposed (such as being uploaded to a public GitHub project). Otherwise, the information security of your Apsara Stack tenant account may become compromised.

```
DefaultProfile profile = DefaultProfile.getProfile(
    "<your-region-id>",         // Your region ID.
    "<your-access-key-id>", // Your AccessKey ID.
    "<your-access-key-secret>"); // Your AccessKey Secret.
```

2.14.2.1.2.3. Call a service

This topic describes how to use the VPC SDK for Java to initiate a request.

Procedure

1. Create an AcsClient instance.

```
IAcsClient client = new DefaultAcsClient(profile);
```

2. Create a request.

   The naming convention for a request is `${apiName}Request`. In the code, ${apiName} is the API name, such as *CreateVpc*.

   When multiple SDKs are used, different requests may have the same name. Differentiate the requests based on the PageSize value.

```
CreateVpcRequest request = new CreateVpcRequest();
request.setPageSize(10);
```

3. Make a call and handle the response.

```
DescribeInstancesResponse response;
try {
   response = client.getAcsResponse(request);
   for (DescribeInstancesResponse.Instance instance:response.getInstances()) {
      System.out.println(instance.getPublicIpAddress());
   }
} catch (ServerException e) {
   e.printStackTrace();
} catch (ClientException e) {
   e.printStackTrace();
}
```

   All the returned fields are deserialized into the response. You can call `response.getXXX()` to obtain the response fields.

```
instanceStatus := response.getStatus()
```

   However, if an exception occurs or you want to obtain the original HTTP response, use `doAction()` to obtain the original response.

```
HttpResponse response = client.doAction(request);
```

2.14.2.1.2.4. Handle exceptions

When you use the Apsara Stack SDK for Java, if the server or SDK encounters an exception, the corresponding exception information is returned. The exception information contains error details, such as error codes and error messages.

Typically, you do not need to handle the exceptions that the SDK for Java returns. You need only to handle exceptions related to the server.

- `ServerException` indicates the error message generated on the server side.
- `ClientException` indicates the error message for SDK exceptions.

For example, if the following exception occurs, you can modify the AccessKey ID based on the error message.

```
com.aliyuncs.exceptions.ClientException: InvalidAccessKeyId.NotFound : Specified access key is not found.
```

If you need to handle SDK exceptions, you can use the following example as a reference:

```
try {
    FooResponse response = client.getAcsResponse(request);
    // Handle the response.
    // ...
}catch (ServerException e){
    // You can add your own exception handling logic here.
    // In this example, an error message is displayed when an exception occurs.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
    // If the problem persists, you can submit a ticket with the request ID included.
    System.out.println("ResponseId=" + e.getRequestId());
}catch (ClientException e){
    // You can add your own exception handling logic here.
    // In this example, an error message is displayed when an exception occurs.
    System.out.println("ErrorCode=" + e.getErrCode());
    System.out.println("ErrorMessage=" + e.getErrMsg());
}
```

2.14.2.1.2.5. Common errors

This topic describes how to troubleshoot common errors you may encounter during the use of SDKs.

Error code	Error message	Cause	Solution
`SDK.CanNotResolveEndpoint`	`Can not resolve endpoint, please check the user guide`	The SDK cannot obtain the region endpoint of the called service.	Check whether the provided region ID and endpoint are correct. After you obtain the correct endpoint, you can run the following code to set the endpoint: `DefaultProfile.addEndpoint("cn-hangzhou", "cn-hangzhou", "Vpc", "vpc.example.com");`

Error code	Error message	Cause	Solution
SDK.JsonUnmarshalError	Failed to unmarshal response	The SDK response fails to be deserialized. In most cases, it is because the structure of the response received by the SDK does not conform to the API metadata, such as mismatched fields or incorrect formatting.	You can use the client.doAction(request) method to obtain the original HTTP response.
SDK.TimeoutError	*The request timed out 4 times (3 for retry), perhaps we should have the threshold raised a little?*	The request has timed out and all retry attempts have failed.	In scenarios such as poor network quality, we recommend that you prolong the timeout period or increase the maximum number of retries.
SDK.ServerError: InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The API only accepts HTTPS requests. It does not accept HTTP requests.	You can add the following code to the request before it is sent: request.setProtocol(ProtocolType.HTTPS)

2.14.2.2. Call the SDK for Python

2.14.2.2.1. Quick start

This topic describes how to obtain and call the VPC Python SDK.

Environment preparation

- Before using the Python SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey in Apsara Stack Management Console, see Obtain an AccessKey pair.

- Obtain the service endpoint. For more information, see Obtain an endpoint.

Install the Python SDK

To install the Python SDK, perform the following operations:

1. Install the SDK core library.
   - If you are using Python V2.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core
     ```

   - If you are using Python V3.x, run the following command to install the SDK core library:

     ```
     pip install aliyun-python-sdk-core-v3
     ```

2. Install the SDK for the VPC.

   The following command provides an example of how to install the VPC SDK:

   ```
   pip install aliyun-python-sdk-cms
   ```

Call the Python SDK

The following example shows you how to call the Python SDK:

1. Create a client instance. When creating the client instance, you must obtain the Region ID, AccessKey ID, and AccessKey Secret.
2. Create an API request and set its parameters.
3. Initiate the request and handle the response or exceptions.

```
#! /usr/bin/env python
#coding=utf-8

from aliyunsdkcore import client
from aliyunsdkvpc.request.v20160428 import CreateVpcRequest
from aliyunsdkcore.profile import region_provider
#region_provider.modify_point('slb', '<regionId>', 'slb.<regionId>.aliyuncs.com')

clt = client.AcsClient('<AccessKey ID>','<AccessKey Secret>','Region ID')

# Set parameters.
request = CreateVpcRequest.CreateVpcRequest()
request.set_accept_format('json')
# Initiate the request.
response = clt.do_action(request)

print response
```

2.14.2.2.2. Usage

2.14.2.2.2.1. Install the SDK for Python

This topic describes how to install and call the VPC SDK for Python.

The SDK for Python supports Python V2.6.x, 2.7.x, 3.x, and later. You can use the following installation methods:

- Use pip (recommended)

  Run the following commands to install the SDK for Python through pip:

  ```
  pip install aliyun-python-sdk-core # Install the SDK core library.
  pip install aliyun-python-sdk-vpc # Install the VPC management library.
  ```

  > **Note** If you are using Python V3.x, use the `pip install aliyun-python-sdk-core-v3` command instead of the `pip install aliyun-python-sdk-core` command.

- Use GitHub

  Run the following commands to install the SDK for Python through GitHub:

  ```
  git clone https://github.com/aliyun/aliyun-openapi-python-sdk.git
  # Install the SDK core library.
  cd aliyun-python-sdk-core
  python setup.py install
  # Install the VPC SDK.
  cd aliyun-python-sdk-vpc
  python setup.py install
  ```

- Use the source code
  i. Download the SDK package and decompress it.
  ii. You can use one of the following methods to install the SDK package:
  - Modify the sys.path variable, and add the directory that you want to search for. It is the directory of the SDK package after it is decompressed. For example:

    ```
    >>> import sys
    >>> sys.path.append('/Users/michael/ my_py_scripts')
    ```

    > **Note** This modification only takes effect during the running process.

  - Configure the PYTHONPATH environment variable, and add the directory that you want to decompress the SDK package to. The content of this environment variable is automatically added to the module search directory.

    You can configure the PYTHONPATH environment variable similar to how you configure the Path environment variable.

- Place the decompressed SDK package in the project. You can then use the SDK for Python in the project.

2.14.2.2.2.2. Configure identity verification credentials

When using SDKs to access Apsara Stack resources, you must provide an authorized Apsara Stack tenant account to verify your identity.

The Python SDK supports the use of AccessKey pairs for identity verification. For more information about how to obtain an AccessKey, see Obtain an AccessKey pair.

To use AccessKey pairs as credentials, you must configure your credentials when initializing the client.

> **Notice** Ensure that code containing your AccessKey is kept confidential and is not exposed (such as being uploaded to a public GitHub project). Otherwise, the information security of your Apsara Stack tenant account may become compromised.

```
clt = client.AcsClient(secret_id, secret_key, region_id)
```

2.14.2.2.2.3. Call a service

This topic describes how to use the VPC SDK for Python to initiate a request.

Procedure

1. Import the SDK of the service that you want to call.

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkvpc.request.v20160428 import CreateVpcRequest
from aliyunsdkvpc.request.v20160428 import DescribeVpcAttributeRequest
```

2. Create an AcsClient instance.

```
client = AcsClient(
   "<your-access-key-id>",
   "<your-access-key-secret>",
   "<your-region-id>" );
```

3. Create a Request object.

```
request = CreateVpcRequest.CreateVpcRequest()
response = client.do_action_with_exception(request)
vpc_id = json.loads(response)['VpcId']
print "VPC ID is", vpc_id
request = DescribeVpcAttributeRequest.DescribeVpcAttributeRequest()
request.set_VpcId(vpc_id)
```

4. Call the service and handle the response.

```
response = client.do_action_with_exception(request)
Print response
```

2.14.2.2.2.4. Set HTTPS requests

The SDK for Python allows you to send API requests through HTTP and HTTPS.

You can specify a protocol (HTTP or HTTPS) for a request, or set a global protocol for all requests.

> **Note** The default protocol of a service takes precedence over the global protocol.

Add OpenSSL support

OpenSSL support is required to send HTTPS requests by using Python. To send HTTPS requests through the SDK for Python, you must add OpenSSL support in Python.

Run `python -c "import ssl"` to check whether your Python environment supports OpenSSL. If the error message `ImportError: No module named ssl` does not appear, OpenSSL is already supported.

If OpenSSL is not supported, run the following command to install it:

```
pip install pyopenssl
```

Set the protocol to HTTP or HTTPS for a request

The following code provides an example of how to set HTTPS as the protocol type for a request.

```
request = CreateVpcRequest.CreateVpcRequest()
request.set_protocol_type("https")
# Valid values: "https" or "http".
```

Set a default protocol for all requests globally

The following code provides an example of how to set a default global protocol.

```
import aliyunsdkcore.request
aliyunsdkcore.request.set_default_protocol_type("https")
# Create a request and call client.do_action_with_exception() to send the request.
```

2.14.2.2.2.5. Handle exceptions

If an error occurs on the server side or SDK side when you use the Python SDK, the Python SDK returns the corresponding exception message. An exception message contains the detailed error information, namely the error code and the error message.

Generally, you are not required to handle the errors returned by the Python SDK. You are only required to handle the errors on the server side according to the error message.

- `ServerException` is the error message on the server side.
- `ClientException` is the error message on the SDK side.

For example, if the following error occurs, modify the ID of AccessKey according to the detailed error message.

```
aliyunsdkcore.acs\_exception.exceptions.ServerException: HTTP Status: 404 Error:InvalidAccessKeyId.NotFound Specified access key is not found.
```

To handle the errors returned by the Python SDK, see the following code example for reference:

```
try:
    response = client.do_action_with_exception(request)
except ServerException as e:
    # Add your own error handling logic here.
    # For example, print the detailed error message.
    print e.get_http_status()
    print e.get_error_code()
    print e.get_error_msg()
```

2.14.2.2.2.6. Common errors

This topic describes the common errors when you use the SDK and troubleshoot the problems based on the corresponding causes and solutions.

Error code	Error message	Cause	Solution

`SDK.InvalidRegionId`	`Can not find endpoint to access.`	The SDK cannot automatically obtain the endpoint of the called service in the specified region.	Check whether the provided region ID and endpoint are correct. Use the following code to set the endpoint:
			`from aliyunsdkcore.profile import region_provider`
			`region_provider.modify_point('product_name', 'region_id', 'endpoint')`

Error code	Error message	Cause	Solution
SDK.TimeoutError	—	The request times out and all retry attempts fail.	In scenarios such as low network quality, we recommend that you increase the timeout period or the maximum number of retries.
SDK.ServerError:InvalidProtocol.NeedSsl	Your request is denied as lack of ssl protect.Recommend:https://error-center.aliyun.com/status/search?Keyword=InvalidProtocol.NeedSsl&source=PopGw	The API only accepts HTTPS requests and does not accept HTTP requests.	Before you send a request, add the following code: `request.set_protocol_type('https')`

2.14.2.3. Call the SDK for PHP

2.14.2.3.1. Quick start

The Apsara Stack PHP SDK allows you to access VPC without performing complex programming operations. This topic describes how to obtain and use the Apsara Stack PHP SDK.

Environment preparation

- Before using the PHP SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey in Apsara Stack Management Console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.
- The Apsara Stack PHP SDK applies to PHP V5.3, 5.4 5.5, 5.6, 7.0, and 7.1. (You can run the **php-v** command to obtain the current PHP version number.)

Install the PHP SDK

To install the PHP SDK, perform the following operations:

1. Download the PHP SDK source code from the Apsara Stack official website.
2. Add the PHP SDK reference to your code.

   For example, if the PHP SDK is downloaded to `/path/to/aliyun-openapi-php-sdk`, use the following command:

   ```
   require_once '/path/to/aliyun-openapi-php-sdk/aliyun-php-sdk-core/Config.php';
   ```

Use the PHP SDK

The following code shows you how to use the Apsara Stack PHP SDK:

1. Create a DefaultAcsClient instance and initialize it.

   When you create and initialize a DefaultAcsClient instance, you must provide the values of Region ID, AccessKey ID, and AccessKey Secret.

2. Create an API request and set its parameters.
3. Initiate the request and handle the response or exceptions.

```
<? php

use Vpc\Request\V20140515\DescribeRegionsRequest;

# Create a DefaultAcsClient instance and initialize it.
$clientProfile = DefaultProfile::getProfile(
   "<your-region-id>",              # Your region ID.
   "<your-access-key-id>",          #  Your AccessKey ID.
   "<your-access-key-secret>"       # Your AccessKey Secret.
);
$client = new DefaultAcsClient($clientProfile);

# Create an API request and set its parameters.
$request = new DescribeRegionsRequest();
$request->setPageSize(10);

# Initiate the request and process the response or exceptions.
try {
   $response = $client->getAcsResponse($request);
   print_r($response);
} catch(ServerException $e) {
   print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
} catch(ClientException $e) {
   print "Error: " . $e->getErrorCode() . " Message: " . $e->getMessage() . "\n";
}
? >
```

2.14.2.4. Call the SDK for Go

2.14.2.4.1. Quick start

The Apsara Stack Go SDK allows you to access VPC without performing complex programming operations. This topic describes how to obtain and use the Apsara Stack Go SDK.

Environment preparation

- Before using the Go SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey in Apsara Stack Management Console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.

Install the Go SDK

1. Download the Go SDK source code from the Apsara Stack official website.
2. Decompress the source code to the directory specified by *GO_PATH*.

Use the Go SDK

The following code provides an example of how to use the Apsara Stack Go SDK:

1. Create a client instance.
2. Create an API request and set its parameters.
3. Initiate the request and handle the response or exceptions.

```
package main

import (
    "github.com/aliyun/alibaba-cloud-sdk-go/services/vpc"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "fmt"
)

func main() {
    // Create a VPC client instance.
    vpcClient, err := vpc.NewClientWithAccessKey(
        "<your-region-id>", // Your region ID.
        "<your-access-key-id>", // Your AccessKey ID.
        "<your-access-key-secret>") // Your AccessKey Secret.
    if err ! = Nell {
        // Handle exceptions.
        panic(err)
    }
     // Create an API request and set its parameters.
    request := vpc.CreateDescribeRegionsRequest()
    // Set request.PageSize to 10.
    request.PageSize = requests.NewInteger(10)
    // Initiate the request and handle exceptions.
    response, err := vpcClient.DescribeRegions(request)
    if err ! = Nell {
        // Handle exceptions.
        panic(err)
    }
    fmt.Println(response)
}
```

2.14.2.4.2. Usage

2.14.2.4.2.1. Install the VPC SDK for Go

This topic describes how to install the VPC SDK for Go.

Context

The VPC SDK for Go supports Go V1.7 and later. You can use the following method to install the VPC SDK for Go:

Procedure

1. Download the SDK for Go source code from Apsara Stack official website.
2. Decompress it to the directory where *GO_PATH* of the current user resides.

2.14.2.4.2.2. Configure identity verification credentials

When you use the VPC SDK to access Apsara Stack resources, you must provide an authorized account for identity verification.

The Go SDK supports the use of AccessKey pairs for identity verification. For more information about how to obtain an AccessKey, see Obtain an AccessKey pair.

To use AccessKey pairs as credentials, you must configure your credentials when initializing the client.

> **Notice** Ensure that code containing your AccessKey is kept confidential and does not leak (such as being exposed to a public GitHub project). Otherwise, the information security of your Apsara Stack account may become compromised.

```
// Create a VPC client instance.
vpcClient, err := vpc.NewClientWithAccessKey(
    "<your-region-id>", // Your zone ID.
    "<your-access-key-id>", // Your AccessKey ID.
    "<your-access-key-secret>") // Your AccessKey Secret.
```

If you want to use a custom *Config* or a credential other than an AccessKey, you must first create a `Credential` object and save it. You must then submit the `Credential` object when initializing the client.

```
// Customize Config.
config := NewConfig()
// Create a Credential object.
credential := &credentials.BaseCredential{
   AccessKeyId:    "<your-access-key-id>",
   AccessKeySecret: "<your-access-key-secret>",
}
// Initialize the client.
client, err := NewClientWithOptions("cn-hangzhou", config, credential)
```

2.14.2.4.2.3. Call a service

This topic describes how to use the VPC SDK for Go to initiate a request.

Procedure

1. Import the VPC SDK for Go.

```
import github.com/aliyun/alibaba-cloud-sdk-go/services/vpc
```

2. Create a VPC client. The client includes all APIs of the VPC.

```
vpcClient := vpc.NewClientWithAccessKey(
   "<your-region-id>",
   "<your-access-key-id>",
   "<your-access-key-secret>")
```

3. Use `xxx.CreateXXXRequest` to create a request.

   The naming convention for the method is `${service}. Create${apiName}Request`. In the code,

   - ${service} is the service name (lower case), such as *vpc*.
   - ${apiName} is the API name, such as *DescribeRegions*.

```
request := vpc.CreateDescribeRegionsRequest()
request.InstanceId = ""
```

4. Initiate the request.

```
response, err := vpcClientDescribeRegions(request)
```

5. Handle the response.

   All the returned fields are deserialized into the response. You can call `response.getXXX()` to obtain the response fields.

```
instanceStatus := response.Status
```

   If an error `(err ! = nil)` occurs, or you want to obtain the original HTTP response, you can use the following methods to obtain the original data:

```
// Obtain the original HTTP response. The response type is *http.Response.
httpResponse := response.GetOriginHttpResponse()

// Obtain the status code of the original HTTP response. The response type is integer.
statusCode := response.GetHttpStatus()

// Obtain the header of the original HTTP response. The response type is map[string][]string.
headers := response.GetHttpHeaders()

// Obtain the content of the original HTTP response. The response type is []byte.
contentBytes := response.GetHttpContentBytes()

// Obtain the content of the original HTTP response and transcode it to a string based on UTF-8. Th
e response type is string.
contentString := response.GetHttpContentString()
```

2.14.2.4.2.4. Handle exceptions

If an error occurs on the server side or SDK side, the Alibaba Cloud Go SDK returns the corresponding exception message, namely the `ClientError` and `ServerError` in the `sdk.errors` package. These errors are based on the standard Go error API. Therefore, you can handle errors returned by the Alibaba Cloud Go SDK in the same way as handling standard Go errors.

ClientError

When an error occurs in an SDK for an invocation that cannot be handled automatically, the SDK returns a `ClientError` .

The following code shows how to determine and obtain the error message in `ClientError` :

```
response, err := vpcClient.DescribeInstances(request)
if clientError, ok := err.(*errors.ClientError); ok{
    // Obtain the error code.
    clientError.ErrorCode()
    // Obtain the error description.
    clientError.Message()
    // Obtain the original error (may be nil).
    clientError.OriginError()
}
```

ServerError

When the SDK receives an error response from the server side, the SDK encapsulates the response into a `ServerError` and returns it to the server.

> **Note** In this case, you can still obtain the original HTTP response from the error response.

The following code shows how to determine and obtain the error message in ServerError and the response:

```
response, err := vpcClient.DescribeInstances(request)
if serverError, ok := err.(*errors.ServerError); ok{
   // Obtain the error code.
   serverError.ErrorCode()
   // Obtain the error description.
   serverError.Message()
   // Obtain the original HTTP response.
   response.GetOriginHttpResponse()
}
```

2.14.2.4.2.5. Customize configurations

This topic describes the custom configurations that Go SDK supports.

Configuration method

The Apsara Stack SDK for Go allows you to use the following method to customize configurations:

```
config := NewConfig().
      WithEnableAsync(true).
      WithGoRoutinePoolSize(5).
      WithMaxTaskQueueSize(1000)
client, err := slb.NewClientWithOptions("<region-id>", config, credential)
```

> **Note** The `config` module of the Apsara Stack SDK for Go cannot be called in the following manner:
>
> ```
> config := &Config{EnableAsync: true,}
> ```

Supported custom configurations

The following table shows the supported custom configurations currently.

Configuration	Default value	Description
AutoRetry	true	Whether to enable the automatic retry

Configuration	Default value	Description
MaxRetryTime	3	The maximum number of retries With the automatic retry enabled, the maximum time consumption for a single call is Timeout (MaxRetryTime + 1).
Timeout	10time.Second	Timeout value. Full-link timeout value, containing establishing connection, redirecting, and reading response If the value is *0*, no timeout occurs.
HttpTransport	nil	Enable the configuration of the underlying `net/http.client` You can configure the original `http.client` of Go with this configuration, such as persistent connection.
EnableAsync	false	Whether to enable the asynchronous feature
MaxTaskQueueSize	1000	The length of the asynchronous queue, which takes effect only when `EnableAsync=true` If the queue is full, new calls are congested.
GoRoutinePoolSize	5	The maximum number of concurrent connections, which takes effect only when `EnableAsync=true`

2.14.2.4.2.6. Asynchronous method invocation

With the concurrent characteristic of the Go language, we recommend that you control the concurrent requests of SDK on the application layer. For your convenience, the Alibaba Cloud Go SDK provides the concurrent calling method that can be directly used. The related concurrency control is achieved within SDK.

Enable asynchronous method invocation for an SDK client

In the following example, the `Credential` object is used as the user credential.

```
// The maximum number of concurrent connections.
poolSize := 10

// The maximum number of cacheable requests.
maxTaskQueueSize := 10000

// Enable asynchronous method invocation when you create an SDK client.
config := sdk.NewConfig().
   WithEnableAsync(true).
   WithGoRoutinePoolSize(poolSize).          // Optional. Default value: 5.
   WithMaxTaskQueueSize(maxTaskQueueSize) // Optional. Default value: 1,000.

// Use the custom configuration to initialize the client.
vpcClient, err := vpc.NewClientWithOptions("<your-region-id>", config, credential)

// Or enable asynchronous method invocation after you have initialized the client.
client.EnableAsync(poolSize, maxTaskQueueSize)
```

Initiate asynchronous calls

The Alibaba Cloud Go SDK supports two methods of initiating asynchronous calls as follows:

- Use channel as the returned value.

```
// this will not block
responseChannel, errChannel := client.FooWithChan(request)
// this will block
response := <-responseChannel
err = <-errChanne
```

- Use callback to control the response.

```
// this will not block
blocker := client.FooWithCallback(request, func(response *FooResponse, err error) {
       // handle the response and err
    }
  )
// The blocker is (chan int) and is used to control the synchronization. If the returned value is 1, the a
ction succeeds. If the returned value is 0, the action fails.
// If <-blocker returns 0 and the action fails, the error message is transmitted to callback by means of
err.
// this will block
result := <-blocker
```

2.14.2.4.2.7. Use CommonRequest

If the product API that you want to call does not have the corresponding SDK, you can use the generic calling method (CommonRequest) to call the product APIs. By using the CommonRequest calling method, you can call any APIs.

Example: Call a RESTful API

The following code provides an example of how to use CommonRequest to call GetClusterList:

```
package main

import (
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk"
    "fmt"
)

func main() {
    client, err := sdk.NewClientWithAccessKey("{your_region_id", "{your_access_key_id}", "{your_access_ke
y_id}")
    if err ! = nil {
        panic(err)
    }

    request := requests.NewCommonRequest()
    request.Domain = "cs.aliyuncs.com"
    request.Version = "2015-12-15"
    // Because this is a RESTful API, the PathPattern field must be specified.
    request.PathPattern = "/clusters"
    response, err := client.ProcessCommonRequest(request)
    if err ! = nil {
        panic(err)
    }
    fmt.Print(response.GetHttpContentString())
}
```

2.14.2.4.2.8. Common errors

This topic describes how to troubleshoot common errors you may encounter during the use of SDKs.

Error code	Error message	Cause	Solution
SDK.CanNotResolveEndpoint	Can not resolve endpoint, please check the user guide	The SDK cannot obtain the region endpoint of the called service.	Check whether the provided region ID and endpoint are correct. After you have obtained the endpoint, you can run the following code to set the endpoint: `request.Domain = "<endpoint>"`
SDK.JsonUnmarshalError	Failed to unmarshal response, but you can get the data via response.GetHttpStatusCode() and response.GetHttpContentString()	The SDK response fails to be deserialized. In most cases, the cause is that the structure of the response received by the SDK does not conform to the API metadata. For example, the fields do not match or the format is incorrect.	For more information, see Response parsing.
SDK.TimeoutError	*The request timed out 4 times(3 for retry), perhaps we should have the threshold raised a little?*	The request has timed out and all retry attempts have failed.	• In scenarios such as cross-region invocations or poor network quality, we recommend that you increase the timeout period or the maximum number of retries. • If the problem persists even though network quality is guaranteed, we recommend that you submit a ticket.
SDK.AsyncFunctionNotEnabled	Async function is not enabled in client, please invoke 'client.EnableAsync()' function	An asynchronous API is called when the asynchronous request switch is not turned on.	Enable the asynchronous feature. For more information, see Asynchronous method invocation.

Response parsing

Ignore SDK deserialization failures and obtain the response attributes by extracting the original HTTP response.

Note The SDK for Go has a dependency on JMESPath. Therefore, when the response content is in the JSON format, you can use JMESPath to parse the response.

```
response, err := client.CreateInstance(request)
    if err ! = Nell {
        // Handle exceptions.
        if clientErr, isClientErr := err.(*errors.ClientError); isClientErr {
            if clientErr.ErrorCode() == errors.JsonUnmarshalErrorCode {
                // You can obtain the data in the original response by using the following encapsulation metho
d.
                // The HTTP status code in the response. Type: integer.
                statusCode := response.GetHttpStatus()
                // The HTTP header in the response. Type: map[string][]string.
                responseHeader := response.GetHttpHeaders()
                // The response body content. Type: []byte.
                responseBytes := response.GetHttpContentBytes()
                // The response body content. Type: string, equivalent to string(response.GetHttpContentByte
s()).
                responseContent := response.GetHttpContentString()
                // You can also directly obtain the original response. Type: net/http.Response.
                httpResponse := response.GetOriginHttpResponse()
            }
        }
    }
```

2.14.2.5. Call the SDK for .NET

2.14.2.5.1. Quick start

The Apsara Stack .NET SDK allows you to access VPC without performing complex programming operations. This topic describes how to obtain and call the Apsara Stack .NET SDK.

Environment preparation

- Before using the .NET SDK, you must have an authorized account and an AccessKey pair that comprises an AccessKey ID and an AccessKey Secret. For more information about how to view and obtain your AccessKey in Apsara Stack Management Console, see Obtain an AccessKey pair.
- Obtain the service endpoint. For more information, see Obtain an endpoint.
- The Apsara Stack .NET SDK applies to .NET Framework 4.0 and later.

Install the Apsara Stack .NET SDK

To call the SDK of a service, you must install the SDK core library and the SDK of the service. For example, to call the VPC SDK, you must obtain and install both the VPC SDK and its core library. You can use one of the following methods to install the .NET SDK:

- Add DLL reference
  i. Download the compressed package containing a DLL file from .NET SDK release list, and decompress it to obtain the DLL file.
  ii. Right-click your project in Solution Explorer of Visual Studio and choose **Reference** from the shortcut menu.
  iii. In the pop-up menu, click **Add Reference**.
  iv. In the dialog box that appears, click **Browse**. Then select the downloaded DLL file and click **Confirm**.
- Add project reference
  i. Visit the Apsara Stack official website to download the .NET SDK source code.
  ii. Find the *aliyun-net-openapi-XXX* subfolder in the downloaded folder, and then locate the \ **.csproj* file. It is the .NET project file. For example, in the `aliyun-net-openapi-vpc` sub-folder, there is a file named `aliyun-net-sdk-vpc.csproj` .
  iii. In Visual Studio, right-click your solution.
  iv. Choose **Add** > **Existing Projects** .
  v. In the dialog box that appears, select the .NET project file (such as `aliyun-net-sdk-vpc.csproj`) from the downloaded source code, and click **Open**.
  vi. Right-click your project and choose **Reference** > **Add reference** from the shortcut menu.

Call the .NET SDK

The following code provides an example of how to call the .NET SDK:

1. Create a DefaultAcsClient instance and initialize it.
2. Create an API request and set its parameters.
3. Initiate the request and process the response or exceptions.

```
using Aliyun.Acs.Core;
using Aliyun.Acs.Core.Profile;
using Aliyun.Acs.Core.Exceptions;
using Aliyun.Acs.Vpc.Model.V20140526;

class TestProgram
{
   static void Main(string[] args)
   {
      // Create a client to initiate a request.
      IClientProfile profile = DefaultProfile.GetProfile(
         "<your-region-id>",
         "<your-access-key-id>",
         "<your-access-key-secret>");
      DefaultAcsClient client = new DefaultAcsClient(profile);
      try
      {
         // Create a request.
         DescribeRegionsRequest request = new DescribeRegionsRequest();
         request.PageSize = 10;
         // Initiate the request and obtain the response.
         DescribeRegionsResponse response = client.GetAcsResponse(request);
         System.Console.WriteLine(response.TotalCount);
      }
      catch (ServerException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
      catch (ClientException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
   }
}
```

2.14.2.5.2. Usage

2.14.2.5.2.1. Install the SDK for .NET

This topic describes how to install the VPC SDK for .NET.

You can use one of the following methods to install the SDK for .NET:

- Add DLL reference
  i. Download the compressed package that contains the relevant DLL file from .NET SDK release list, and decompress it to obtain the DLL file.
  ii. Right-click your project in Solution Explorer of Visual Studio and choose **Reference** from the shortcut menu.
  iii. In the pop-up menu, click **Add Reference**.
  iv. In the dialog box that appears, click **Browse**. Then select the downloaded DLL file and click **Confirm**.
- Add project reference
  i. Visit Apsara Stack official website to download the source code of the SDK for .NET.
  ii. Find the *aliyun-net-openapi-XXX* subfolder in the downloaded folder, and then locate the \ *.*csproj* file. It is the .NET project file. For example, in the `aliyun-net-openapi-vpc` sub-folder, there is a file named `aliyun-net-sdk-vpc.csproj` .
  iii. In Visual Studio, right-click your solution.
  iv. Choose **Add** > **Existing Projects**.
  v. In the dialog box that appears, select the .NET project file (such as `aliyun-net-sdk-vpc.csproj`) from the downloaded source code, and click **Open**.
  vi. Right-click your project and choose **Reference** > **Add reference** from the shortcut menu.

2.14.2.5.2.2. Configure identity verification credentials

When using the Alibaba Cloud .NET SDK to access Alibaba Cloud Apsara Stack services, you must provide an Alibaba Cloud account for authentication.

The .NET SDK supports the use of AccessKey pairs for identity verification. For more information about how to obtain an AccessKey, see Obtain an AccessKey pair.

To use AccessKey pairs as credentials, you must configure your credentials when initializing the client.

> **Notice** Ensure that code containing your AccessKey is kept confidential and is not exposed (such as being uploaded to a public GitHub project). Otherwise, the information security of your Apsara Stack tenant account may become compromised.

```
IClientProfile clientProfile = DefaultProfile.GetProfile(
  "<your-region-id>", // The region ID.
  "<your-access-key-id>", //  The AccessKey ID of the RAM account.
  "<your-access-key-secret>"); // The AccessKey Secret of the RAM account.
```

2.14.2.5.2.3. Call a service

This topic describes how to use the Apsara Stack VPC SDK for .NET to initiate a request.

1. Create a default client instance.

```
DefaultAcsClient client = new DefaultAcsClient(clientProfile);
```

2. Create a request.

   The naming convention for requests is `${apiName}Request`. ${apiName} is the API name, such as *DescribeRegions*.

   When multiple SDKs are used, different requests may have the same name. Differentiate the requests based on the PageSize value.

```
DescribeRegionsRequest request = new DescribeRegionsRequest();
request.PageSize = 10;
```

3. Call a service and process the response.

```
DescribeRegionsResponse response = client.GetAcsResponse(request);
```

   All the returned fields are deserialized into the response. You can call `response.getXXX()` to obtain the response fields.

```
System.Console.WriteLine(response.TotalCount);
```

2.14.2.5.2.4. Handle exceptions

If an error occurs on the server side or SDK side when you use Alibaba Cloud .NET SDK, the .NET SDK returns the corresponding exception message. An exception message contains the detailed error information, namely the error code and the error message.

Typically, you do not need to handle the exceptions that the SDK for .NET returns. You need only to handle exceptions related to the server.

- `ServerException` indicates the error message generated on the server side.
- `ClientException` indicates the error message for SDK exceptions.

For example, if the following exception occurs, you can modify the AccessKey ID based on the error message.

```
InvalidAccessKeyId.NotFound : Specified access key is not found.
```

If you need to handle SDK exceptions, you can use the following example as a reference:

```
try
{
    DescribeRegionsResponse response = client.GetAcsResponse(request);
    // Handle the response.
    // ...
}
catch (ServerException e)
{
    // You can add your own exception handling logic here.
    // In this example, an error message is displayed when an exception occurs.
    Console.WriteLine("ErrorCode=" + e.ErrorCode);
    Console.WriteLine("ErrorMessage=" + e.ErrorMessage);
    // If the problem persists, you can submit a ticket with the request ID included to the Alibaba Cloud de
velopment team.
    Console.WriteLine("ErrorCode=" + e.RequestId);
}
catch (ClientException e)
{
    // You can add your own exception handling logic here.
    // In this example, an error message is displayed when an exception occurs.
    Console.WriteLine("ErrorCode=" + e.ErrorCode);
    Console.WriteLine("ErrorMessage=" + e.ErrorMessage);
}
```

2.14.2.5.2.5. Call an API through CommonRequest

If the product API that you want to call does not have the corresponding SDK, you can use the generic calling method (CommonRequest) to call the product APIs. By using the CommonRequest calling method, you can call any APIs.

Characteristics of CommonRequest calling

The CommonRequest calling method has the following characteristics:

- Light weight: You only need the core package to initiate the call, without downloading or installing the SDK of each product.
- Easy and convenient: You can call the latest API without updating the SDK.
- Fast iteration

Use CommonRequest

To initiate a CommonRequest request, you must obtain the values for the following parameters. You can obtain the values of these parameters from the API documentation.

- Domain: the service endpoint.

- Version: the version of the API, in the format of YYYY-MM-DD.

  You can obtain the API version from the common parameters in the API documentation.
- API information: the name of the API to be called.

  You must obtain the Action parameter, and run `request.ApiName = "<Action>"` to specify the API name.

  For example, to initiate a CommonRequest request for RunInstances, you need to specify the API name by using `request.ApiName = "RunInstances"` .

Example: Call a RESTful API

The following code provides an example of how to use CommonRequest to call GetClusterList:

```
using Aliyun.Acs.Core;
using Aliyun.Acs.Core.Exceptions;
using Aliyun.Acs.Core.Profile;

class Sample
{
   static void Main(string[] args)
   {
      // Create a client instance to initiate a request.
      IClientProfile profile = DefaultProfile.GetProfile(
         "<your-region-id>",
         "<your-access-key-id>",
         "<your-access-key-secret>");
      DefaultAcsClient client = new DefaultAcsClient(profile);

      try
      {
         // Create a request.
         CommonRequest request = new CommonRequest();
         request.Domain = "cs.aliyuncs.com";
         request.Version = "2015-12-15";

         // Because this is a RESTful API, the UriPattern field must be specified.
         request.UriPattern = "/clusters";

         // Initiate a request and obtain the response.
         CommonResponse response = client.GetCommonResponse(request);
         System.Console.WriteLine(response.Data);
      }
      catch (ServerException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
      catch (ClientException ex)
      {
         System.Console.WriteLine(ex.ToString());
      }
   }
}
```

2.14.2.5.2.6. Common errors

This topic describes the common errors when you use the .NET SDK. Troubleshoot the problems based on the corresponding causes and solutions.

Error code	Cause	Solution
SDK.InvalidRegionId	SDK cannot automatically obtain the endpoint of the called product in the specified region.	Check if your endpoint is correct.
InvalidAccessKeyId.NotFound	The configured AccessKey ID is invalid.	Check if your AccessKey ID is correct.
SDK.ConnectionReset	The endpoint cannot be connected when you initiate a request.	Check if your network is available.
SDK.InvalidProfile	The DefaultProfile parameter that you provided when initializing DefaultAcsClient is invalid.	Make sure that the provided DefaultProfile parameter object is properly initialized and configured with corresponding parameters.
SDK.SessionTokenExpired	The DefaultProfile parameter that you provided when initializing DefaultAcsClient is invalid.	Make sure that the provided SessionToken parameter is in the validity period, which is generally one hour.
SignatureDoesNotMatch	The provided SessionToken is invalid or has expired.	Make sure that the provided DefaultProfile parameter object is properly initialized and configured with corresponding parameters.
SDK.InvalidProfile	The AccessKey Secret does not match the AccessKey ID.	Make sure that the provided AccessKey Secret is valid.

2.14.2.6. Obtain an endpoint

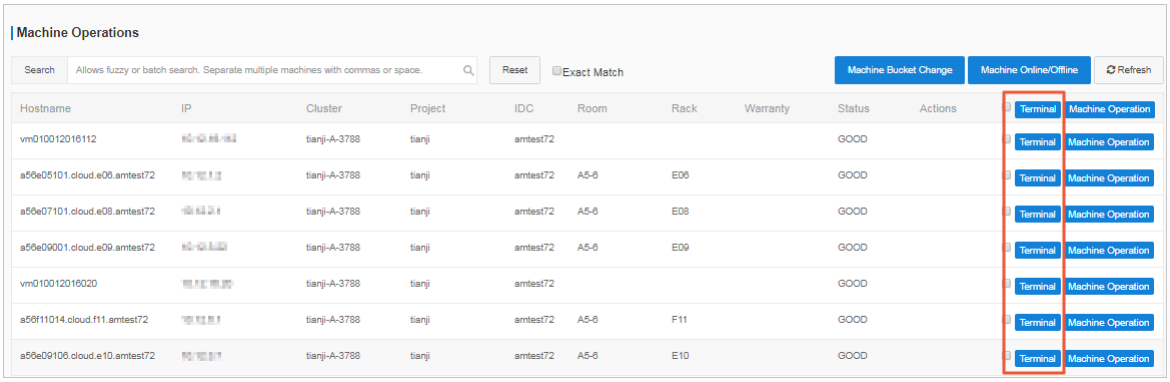
You can obtain the endpoint of a VPC service in the Apsara Stack Operations console.

Procedure

1. Log on to Apsara Stack Operations. For how to log on to Apsara Stack Operations, see **Operations of basic platforms > Apsara Stack Operations > Log on to Apsara Stack Operations** in *Operations Guide* .
2. Click **Products** in the left-side navigation pane.
3. Choose **Apsara Infrastructure Management Framework** in the product list to go to the Apsara

Infrastructure Management Framework page.

4. Choose **Operations > Machine Operations**. The **Machine Operations** page appears.
5. Select a machine and then click **Terminal** to log on to the machine.



6. Run the following command to obtain the JSON data:

```
curl -l "http://127.0.0.1:7070/api/v3/column/c.sr.service_registration,c.sr.id?c.sr.service_registration
"
```

7. Obtain the endpoint of a VPC based on the ID (vpc-yaochi) and the key value (vpc.openapi.endpoint) of the VPC service.

2.14.2.7. Obtain an AccessKey pair

You can obtain an AccessKey pair in the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center > Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this

department.

> Note The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**.

   The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.15. Log Service

2.15.1. API reference

2.15.1.1. Overview

Log Service is a platform-based service specific to logs. Log Service supports real-time collection, storage, and delivery of various types of logs.

Log Service allows you to perform log operations through the Apsara Stack console. In addition, it allows you to use the Log Service API to write and query logs as well as manage your projects and Logstores. API operations supported by Log Service lists the currently available API operations.

API operations supported by Log Service

Object	Operation
Log	Basic concepts such as log and log group
Config	List, Create, Delete, Get, Update
-	GetAppliedMachineGroups
MachineGroup	List, Create, Delete, Get, Update
-	Apply, Remove
-	GetAppliedConfigs
Logstore	List, Create, Delete, Get, Update
-	GetLogs, GetHistograms
Shard	List, Split, Merge
-	PostLogStoreLogs
-	GetCursor

Object	Operation
-	PullLogs

You can call API operations to:

- Collect logs based on the Logtail configuration and machine group information.
- Create a Logstore and write logs to and query logs from the Logstore.

> Note
> - The Log Service API is a RESTful API.
> - Security verification is required for all the API requests. For more information about the API request signing mechanism and process, see Request signatures.

2.15.1.2. Obtain an AccessKey pair

You can obtain your AccessKey pair from the Apsara Stack console.

Obtain an AccessKey pair of a department

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click the icon, and then choose **User Center** > **Department Management**.
3. Select a department and click **Create AccessKey** to obtain an AccessKey pair of this department.

> Note The AccessKey pair is automatically allocated to a level-1 department. The sub-departments use the same AccessKey pair as their level-1 department.

Obtain an AccessKey pair of a personal account

Follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the Web page, click your avatar and select **Personal Information**.

   The system displays your AccessKey ID.
3. Click **Show** under **AccessKey Secret** to view the AccessKey Secret.

2.15.1.3. Common request headers

Log Service APIs are RESTful APIs based on the HTTP protocol, which support a set of common request headers that can be used in all API requests (unless otherwise stated, each Log Service API request must provide these common request headers). The detailed definitions of these headers are described in Header definition.

Header definition

Header name	Type	Description
Accept	String	The type of the value that the client expects the server to return. Currently, two types are supported: application/json and application/x-protobuf. This field is optional and is valid only for GET requests. The specific value is subject to the definition of each API.
Accept-Encoding	String	The compression algorithm that the client expects Log Service to return. Currently, LZ4 and DEFLATE are supported. It can be null. This field is optional and valid only for GET requests. The specific value is subject to the definition of each API.
Authorization	String	The signature content. For more information, see the Request signature.
Content-Length	Numerical value	The length of the HTTP request body defined in RFC 2616. If the request has no body, it is unnecessary to provide this request header.
Content-MD5	String	The string generated after the request body undergoes MD5 calculation, and the calculation result is in uppercase. If the request has no body, this request header is not required.
Content-Type	String	The type of the HTTP request body defined in RFC 2616. Currently, Log Service API requests support only application/x-protobuf. If the request has no body, it is unnecessary to provide this request header. The specific value is subject to the definition of each API.
Date	String	The time when the request is sent. Currently, parameters only support the RFC 822 format, and the GMT standard time is used. The formatted string is as follows: %a, %d %b %Y %H:%M:%S GMT (for example: Mon, 3 Jan 2010 08:33:47 GMT).
Host	String	The complete host name of the HTTP request, protocol headers such as `http://` are not included. For example, `big-game.regionid.example.com`.
x-log-apiversion	String	The API version. The current version is 0.6.0.
x-log-bodyrawsize	Numerical value	The initial size of the request body. When the request has no body, the value is 0. When the body is a compressed data, the value is the size of the initial data before compression. The value range for this field is 0-3x1024x1024. This field is optional and only required when the body is compressed.
x-log-compresstype	String	The compression type of the API request body. Currently, LZ4 and DEFLATE are supported (RFC 1951. For more information about the zlib format, see RFC 1950). If the body is not compressed, this request header is not required.

Header name	Type	Description
x-log-date	String	The time when the request is sent. The time format is the same as that of the Date header. This request header is optional. If a request contains this common request header, this value replaces the value of the standard Date header for server request authentication. Whether an x-log-date header is present or not, the standard HTTP Date header must be provided.
x-log-signaturemethod	String	The signature computing method. Currently, only `hmac-sha1` is supported.

Note

- The maximum difference between the time expressed in the Date header of a request and the time the server receives the request is 15 minutes. If the request contains the x-log-date header, the time difference is calculated based on the value of the x-log-date header.
- If the compression algorithm is specified in x-log-compresstype of the request, the raw data must be compressed and then put into the HTTP body. The Content-Length and Content-MD5 header are also calculated based on the HTTP body.
- When HTTP requests are sent from certain platforms, they cannot specify a Date header (the sending time is automatically specified in the platform's internal database). Therefore, the correct Date value cannot be used to calculate the request signature. In this case, specify the x-log-date header and use the header value to calculate the request signature. After receiving an API request, the Log Service server first determines whether the request contains an x-log-date header. If an x-log-date header exists, the server uses the header value for signature authentication. Otherwise, the server uses the HTTP standard header Date for signature authentication.

2.15.1.4. Common response headers

Log Service APIs are RESTful APIs based on the HTTP protocol. All Log Service API responses provide a set of common response headers, whose detailed definitions are described in Definitions of common response headers.

Definitions of common response headers

Header name	Type	Description
Content-Length	Numerical value	The length of the HTTP response content defined in RFC 2616.
Content-MD5	String	The MD5 value of the HTTP response content defined in RFC 2616, It is an uppercase string produced after the MD5 calculation of the request body.

Header name	Type	Description
Content-Type	String	The type of the HTTP response content defined in RFC 2616. Currently, Log Service supports two response types: application/json and application/x-protobuf.
Date	String	The time when the request is returned. Currently, parameters only support the RFC 822 format, and the GMT standard time is used. The formatted string is as follows: %a, %d %b %Y %H:%M:%S GMT (for example: Mon, 3 Jan 2010 08:33:47 GMT).
x-log-requestid	String	The unique ID generated in Log Service that marks this request. This response header is irrelevant to actual applications. It is mainly used to track and investigate problems. For the API request troubleshooting purpose, you can provide the Log Service team with this ID.

2.15.1.5. Request signature

All the HTTP requests of Log Service APIs are subjected to security authentication. This ensures the security of log data. Security authentication is based on an AccessKey pair and is completed by using the symmetric encryption algorithm.

This process is as follows:

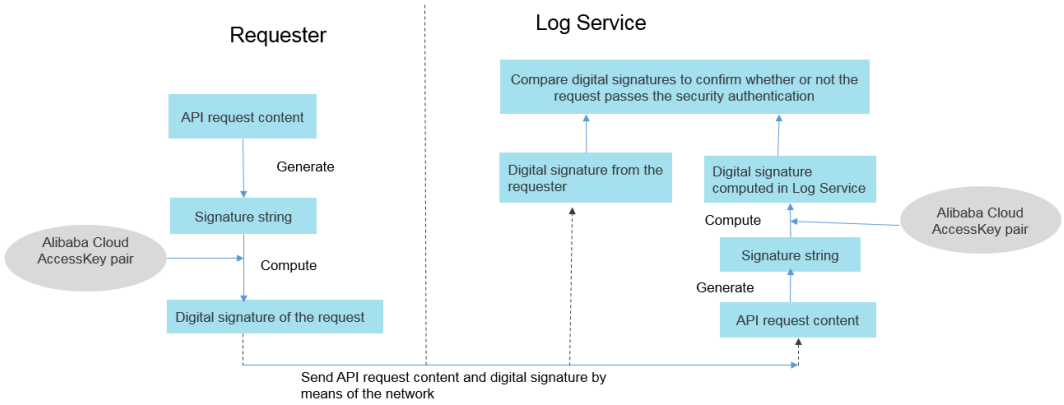
1. The requester generates a signature string based on the API request content that includes the HTTP header and body.
2. The requester uses an AccessKey pair that consists of an AccessKey ID and AccessKey Secret to sign the signature string generated in step 1. A digital signature is generated for this API request.
3. The requester sends both the API request content and digital signature to the server.
4. After receiving the request, the server repeats step 1 and step 2.

   > **Note** The server retrieves the AccessKey pair from the back end to calculate the signature string and generate the expected digital signature for this request.

5. The server compares the expected digital signature with the digital signature sent from the requester. If both signatures are the same, the request passes security authentication. Otherwise, the request is immediately rejected.

Security authentication process illustrates the preceding process.

Security authentication process



The preceding security authentication process can also be used for the following purposes:

- Identify which user sends the API request. A user must specify the AccessKey pair that is used to generate the digital signature before sending the request. The server can then use this AccessKey pair to verify the identity of the user and implement access control.
- Check whether the user request is tampered during transmission over the network. The server recalculates the signature string based on the received request content. Therefore, if the content is tampered during transmission, the digital signature sent from the requester does not match with the digital signature obtained from the server.

API request signature

To pass security authentication for an API request, you must use the client to sign the API request to generate a correct digital signature. You must also use the HTTP Authorization request header to transfer the digital signature of the request over the network. The format of the Authorization header is as follows:

```
Authorization:LOG <AccessKeyId>:<Signature>
```

As shown in the preceding format, the value of the Authorization header contains the AccessKey ID. The corresponding AccessKey Secret is used to create a signature value. The following steps describe how to generate the signature value.

1. Prepare an AccessKey pair

   You must use an AccessKey pair that consists of an AccessKey ID and AccessKey Secret to generate a digital signature for an API request.

2. Generate a signature string for the request

   The signature string of a Log Service API is generated based on the method, header, and body of the HTTP request. The generation method is as follows:

   ```
   SignString = VERB + "\n"
            + CONTENT-MD5 + "\n"
            + CONTENT-TYPE + "\n"
            + DATE + "\n"
            + CanonicalizedLOGHeaders + "\n"
            + CanonicalizedResource
   ```

In the preceding formula, `\n` indicates the newline escape character and a plus sign (`+`) indicates the string concatenation operator. Signature string definitions describes the definitions of the other parts.

Signature string definitions

Parameter	Description	Examples
VERB	The method name of the HTTP request.	PUT, GET, and POST
CONTENT-MD5	The MD5 value of the HTTP request body, which must be an uppercase string.	875264590688CA6171F6228AF5BBB3D2
CONTENT-TYPE	The type of the HTTP request body.	application/x-protobuf
DATE	The standard timestamp header of the HTTP request, which follows the RFC 1123 format and uses GMT.	Mon, 3 Jan 2010 08:33:47 GMT
CanonicalizedLOGHeaders	The string constructed by custom headers prefixed with `x-log` and `x-acs` in the HTTP request. The construction method is described as follows.	x-log-apiversion:0.6.0\nx-log-bodyrawsize:50\nx-log-signaturemethod:hmac-sha1
CanonicalizedResource	The string constructed by the HTTP request resources. The construction method is described as follows.	/logstores/app_log

For HTTP requests without the request body, both the CONTENT-MD5 and CONTENT-TYPE fields are empty. The generation method of the signature string is as follows:

```
SignString = VERB + "\n"
        + "\n"
        + "\n"
        + DATE + "\n"
        + CanonicalizedLOGHeaders + "\n"
        + CanonicalizedResource
```

As described in Common request headers, a custom request header named `x-log-date` is used for Log Service APIs. If you specify a custom request header when sending a request, the header value will replace the value of the HTTP standard request header Date to calculate the signature string.

The CanonicalizedLOGHeaders construction method is as follows:

i. Convert the names of all HTTP request headers that are prefixed with `x-log` and `x-acs` to lowercase letters.

ii. Sort all Log Service custom request headers obtained in the preceding step in lexicographical order.

iii. Delete any spaces on either side of a separator between the request header and content.

iv. Separate all headers and contents with separators (`\n`) to form the final CanonicalizedHeaders.

The CanonicalizedResource construction method is as follows:

i. Set CanonicalizedResource to an empty string ("").

ii. Specify the Log Service resources to be accessed. For example, */logstores/logstorename*. This field can be left blank if the `logstorename` does not exist.

iii. If the request contains a query string (`QUERY_STRING`), add a question mark `(?)` and the query string to the end of the CanonicalizedResource string.

The `QUERY_STRING` is a string generated after URL request parameters are sorted in lexicographical order. Use equal signs (`=`) between parameter names and parameter values to produce a string. Sort the name-value pairs in lexicographical order. Then, use ampersands (`&`) to connect the pairs to construct a string. The formula is as follows:

```
QUERY_STRING = "KEY1=VALUE1" + "&" + "KEY2=VALUE2"
```

3. Generate a digital signature for the request

Log Service APIs support only one digital signature algorithm, which is also the default signature algorithm `hmac-sha1` . The signature formula is as follows:

```
Signature = base64(hmac-sha1(UTF8-Encoding-Of(SignString), AccessKeySecret))
```

Use the HMAC-SHA1 method defined in RFC 2104 as the signature method. The AccessKey Secret in the preceding formula must correspond to the AccessKey ID that is used in the Authorization header. Otherwise, the request cannot pass authentication by the server.

After a signature string is calculated, use this value to construct a security authentication header for the Log Service API request in Authorization header format. Then, insert the header into the HTTP request before sending the request.

Examples of the request signature process

The following two examples demonstrate how to sign the Log Service API request. Assume that the AccessKey pair you use to sign the Log Service API request is as follows:

```
AccessKeyId = "<yourAccessKeyId>"
AccessKeySecret = "<yourAccessKeySecret>"
```

- You must send the following GET request to list all the Logstores in the ali-test-project project. The HTTP request is as follows:

```
GET /logstores HTTP 1.1
Mon, 09 Nov 2015 06:11:16 GMT
Host: ali-test-project.regionid.example.com
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

The following signature string is generated for the Log Service API request:

```
GET\n\n\nMon, 09 Nov 2015 06:11:16 GMT\nx-log-apiversion:0.6.0\nx-log-signaturemethod:hmac-sha1
\n/logstores? logstoreName=&offset=0&size=1000
```

This request is a GET request, which does not have the HTTP request body. Therefore, the CONTENT-TYPE and CONTENT-MD5 fields are empty. After the previously specified AccessKey Secret is used to calculate the signature string, the digital signature is generated as follows:

```
jEYOTCJs2e88o+y5F4/S5IsnBJQ=
```

The digitally signed HTTP request content is sent as follows:

```
GET /logstores HTTP 1.1
Mon, 09 Nov 2015 06:11:16 GMT
Host: ali-test-project.regionid.example.com
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
Authorization: LOG <yourAccessKeyId>:<yourSignature>
```

- You must write the following log into the Logstore named test-logstore in the ali-test-project project.

```
topic=""
time=1447048976
source="10.10.10.1"
"TestKey": "TestContent"
```

Therefore, the following HTTP request must be constructed based on Log Service API definition:

```
POST /logstores/test-logstore HTTP/1.1
Date: Mon, 09 Nov 2015 06:03:03 GMT
Host: test-project.regionid.example.com
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
Content-MD5: 1DD45FA4A70A9300CC9FE7305AF2C494
Content-Length: 52
x-log-apiversion:0.6.0
x-log-bodyrawsize:50
x-log-compresstype:lz4
x-log-signaturemethod:hmac-sha1
<Log contents are serialized to byte streams in protocol buffers format>
```

In this HTTP request, the written log content is serialized in protocol buffers format (for more information about this format, see Protocol buffers format) and then used as the request body. Therefore, the Content-Type header value of this request is application/x-protobuf. Similarly, the Content-MD5 header value is the MD5 value of the request body. Based on the preceding signature string construction method, the signature string corresponding to this request is as follows:

```
POST\n1DD45FA4A70A9300CC9FE7305AF2C494\napplication/x-protobuf\nMon, 09 Nov 2015 06:03:03 G
MT\nx-log-apiversion:0.6.0\nx-log-bodyrawsize:50\nx-log-compresstype:lz4\nx-log-signaturemethod
:hmac-sha1\n/logstores/test-logstore
```

In the similar way, the AccessKey Secret in the preceding example is used to calculate the signature string. The final signature is as follows:

```
XWLGYHGg2F2hcfxWxMLiNkGki6g=
```

The digitally signed HTTP request content is sent as follows:

```
POST /logstores/test-logstore HTTP/1.1
Date: Mon, 09 Nov 2015 06:03:03 GMT
Host: test-project.regionid.example.com
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
Content-MD5: 1DD45FA4A70A9300CC9FE7305AF2C494
Content-Length: 52
x-log-apiversion:0.6.0
x-log-bodyrawsize:50
x-log-compresstype:lz4
x-log-signaturemethod:hmac-sha1
Authorization: LOG <yourAccessKeyId>:<yourSignature>
<Log contents are serialized to byte streams in protocol buffers format>
```

2.15.1.6. Common error codes

When an API request error occurs, Log Service returns an error message, including the HTTP status code and the specific error details in the response body. The error details in the response body are in the following formats:

```
{
"errorCode" : <ErrorCode>,
"errorMessage" : <ErrorMessage>
}
```

Among all the error messages that may be returned by Log Service, some of them are applicable to the majority of the APIs, while the others are unique to certain APIs. Common error codes are described in the following table and appear in the responses of multiple APIs. The special error codes of an API are described in the reference to that particular API.

Common error codes

HTTP status code	Error code	Error message	Description
411	MissingContentLength	Content-Length does not exist in HTTP header when it is necessary.	The error message returned when the required Content-Length request header is not provided.
415	InvalidContentType	Content-Type {type} is unsupported.	The error message returned when the specified Content-Type is not supported.
400	MissingContentType	Content-Type does not exist in HTTP header when body is not empty.	The error message returned when the Content-Type header is not specified when the HTTP request body is not empty.
400	MissingBodyRawSize	x-log-bodyrawsize does not exist in header when it is necessary.	The error message returned when the required x-log-bodyrawsize request header is not provided in the compression scenario.
400	InvalidBodyRawSize	x-log-bodyrawsize is invalid.	The error message returned when the x-log-bodyrawsize value is invalid.
400	InvalidCompressType	x-log-compresstype {type} is unsupported.	The error message returned when the compression type specified in x-log-compresstype is not supported.

HTTP status code	Error code	Error message	Description
400	MissingHost	Host does not exist in HTTP header.	The error message returned when the HTTP standard request header Host is not provided.
400	MissingDate	Date does not exist in HTTP header.	The error message returned when the HTTP standard request header Date is not provided.
400	InvalidDateFormat	Date {date} must follow RFC822.	The error message returned when the Date request header value does not conform to the RFC822 standard.
400	MissingAPIVersion	x-log-apiversion does not exist in HTTP header.	The error message returned when the HTTP request header x-log-apiversion is not provided.
400	InvalidAPIVersion	x-log-apiversion {version} is unsupported.	The error message returned when the value of the HTTP request header x-log-apiversion is not supported.
400	MissAccessKeyId	x-log-accesskeyid does not exist in header.	The error message returned when no AccessKey ID is provided in the Authorization header.
401	Unauthorized	The AccessKeyId is unauthorized.	The error message returned when the provided AccessKey ID value is unauthorized.
400	MissingSignatureMethod	x-log-signaturemethod does not exist in HTTP header.	The error message returned when x-log-signaturemethod does not exist in HTTP header.
400	InvalidSignatureMethod	signature method {method} is unsupported.	The error message returned when the signature method specified by the x-log-signaturemethod header is not supported.
400	RequestTimeTooSkewed	Request time exceeds server time more than 15 minutes.	The error message returned when the request sent time is more than 15 minutes before or after the current server time.
404	ProjectNotExist	Project {name} does not exist.	The error message returned when the Log Service project does not exist.

HTTP status code	Error code	Error message	Description
401	SignatureNotMatch	Signature {signature} is not matched.	The error message returned when the digital signature of the request does not match with that computed in Log Service.
403	WriteQuotaExceed	Write quota is exceeded.	The error message returned when the log write quota is exceeded.
403	ReadQuotaExceed	Read quota is exceeded.	The error message returned when the log read quota is exceeded.
500	InternalServerError	Internal server error message.	The error message returned when the an internal server error occurred.
503	ServerBusy	The server is busy, please try again later.	The error message returned when the server is disconnected. Please try again later.

The {...} in the error message indicates the specific error information. For example, {name} in the ProjectNotExist error message is replaced by a specific project name.

2.15.1.7. Logstore operations

2.15.1.7.1. CreateLogstore

You can call this operation to create a Logstore for a project.

Examples:

```
POST /logstores
```

Request syntax

```
POST /logstores HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
{
   "logstoreName" : <logStoreName>,
   "ttl": <ttl>,
   "shardCount": <shardCount>
}
```

Request parameters

Request parameters describes the request parameters.

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore. The name must be unique within a project.
ttl	Integer	Yes	The data retention time. Unit: days.
shardCount	Integer	Yes	The number of shards in the Logstore.

Request header

No special request header is required. For more information about the common request headers of Log Service API, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to CreateLogstore, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to CreateLogstore

HTTP status code	Error code	Error message
400	LogstoreAlreadyExist	logstore {logstoreName} already exists
500	InternalServerError	Specified Server Error Message
400	LogstoreInfoInvalid	logstore info is invalid
400	ProjectQuotaExceed	Project Quota Exceed

Detailed description

Logstores cannot be created for a project if the quota is exhausted.

Examples

Sample requests:

```
POST /logstores HTTP/1.1
Header :
{
x-log-apiversion=0.6.0,
Authorization=LOG <yourAccessKeyId>:<yourSignature>,
Host=ali-test-project.regionid.example.com,
Date=Wed, 11 Nov 2015 07:35:00 GMT,
Content-Length=55,
x-log-signaturemethod=hmac-sha1,
Content-MD5=7EF43D0B8F4A807B95E775048C911C72,
User-Agent=sls-java-sdk-v-0.6.0,
Content-Type=application/json
}
Body :
{
   "logstoreName": "test-logstore",
   "ttl": 1,
   "shardCount": 2
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header:
{
Date=Wed, 11 Nov 2015 07:35:00 GMT,
Content-Length=0,
x-log-requestid=5642EFA499248C827B012B39,
Connection=close,
Server=nginx/1.6.1
}
```

2.15.1.7.2. DeleteLogstore

You can call this operation to delete a Logstore, including all shards and indexes of the Logstore.

Request syntax

```
DELETE /logstores/{logstoreName} HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

DeleteLogstore request Parameters describes the request parameters.

DeleteLogstore request Parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore. The name must be unique within a project.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to DeleteLogstore, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to DeleteLogstore

HTTP status code	Error code	Error message
404	LogStoreNotExist	logstore {logstoreName} does not exist
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
DELETE /logstores/test_logstore HTTP/1.1
Header :
{
x-log-apiversion=0.6.0,
Authorization=LOG <yourAccessKeyId>:<yourSignature>,
Host=ali-test-project.regionid.example.com,
Date=Wed, 11 Nov 2015 08:09:38 GMT,
Content-Length=0,
x-log-signaturemethod=hmac-sha1,
User-Agent=sls-java-sdk-v-0.6.0,
Content-Type=application/json
}
```

Sample responses:

```
HTTP/1.1 200 OK
Body:
{
Date=Wed, 11 Nov 2015 08:09:39 GMT,
Content-Length=0,
x-log-requestid=5642F7C399248C817B013A07,
Connection=close,
Server=nginx/1.6.1
}
```

2.15.1.7.3. UpdateLogstore

You can call this operation to update the attributes of a Logstore. You can only update Time To Live (TTL) and shard attributes.

Request syntax

```
PUT /logstores/{logstoreName} HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
{
   "logstoreName": <logstoreName>,
   "ttl": <ttl>,
   "shardCount": <shardCount>
}
```

Request parameters

UpdateLogstore request parameters describes the request parameters.

UpdateLogstore request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore. The name must be unique within a project.
ttl	Integer	Yes	The lifecycle of the log data. Valid values: 1 to 365. Unit: days.
shardCount	Integer	Yes	The number of shards. Valid values: 1 to 10.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to UpdateLogstore, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to UpdateLogstore

HTTP status code	Error code	Error message
404	ProjectNotExist	Project {ProjectName} does not exist
404	LogStoreNotExist	logstore {logstoreName} does not exist
400	LogStoreAlreadyExist	logstore {logstoreName} already exists
500	InternalServerError	Specified Server Error Message
400	ParameterInvalid	invalid shard count, you can only increase the count

Detailed description

The number of shards can be increased but cannot be decreased.

Examples

Sample requests:

```
PUT /logstores/test-logstore HTTP/1.1
Header:
{
x-log-apiversion=0.6.0,
Authorization=LOG <yourAccessKeyId>:<yourSignature>,
Host=ali-test-project.regionid.example.com,
Date=Wed, 11 Nov 2015 08:28:19 GMT,
Content-Length=55,
x-log-signaturemethod=hmac-sha1,
Content-MD5=757C60FC41CC7D3F60B88E0D916D051E,
User-Agent=sls-java-sdk-v-0.6.0,
Content-Type=application/json
}
Body :
{
   "logstoreName": "test-logstore",
   "ttl": 1,
   "shardCount": 2
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header:
{
Date=Wed, 11 Nov 2015 08:28:20 GMT,
Content-Length=0,
x-log-requestid=5642FC2399248C8F7B0145FD,
Connection=close,
Server=nginx/1.6.1
}
```

2.15.1.7.4. GetLogstore

You can call this operation to view the attributes of a Logstore.

Request syntax

```
GET /logstores/{logstoreName} HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

GetLogstore request parameters describes the request parameters.

GetLogstore request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore. The name must be unique within a project.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

```
{
   "logstoreName" : <logstoreName>,
   "ttl": <ttl>,
   "shardCount": <shardCount>,
   "createTime": <createTime>,
   "lastModifyTime": <lastModifyTime>
}
```

Error codes

As described in Error codes specific to GetLogstore, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to GetLogstore

HTTP status code	Error code	Error message
404	ProjectNotExist	Project {ProjectName} does not exist
404	LogstoreNotExist	logstore {logstoreName} does not exist
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
GET /logstores/test-logstore HTTP/1.1
Header :
{
x-log-apiversion=0.6.0,
Authorization=LOG <yourAccessKeyId>:<yourSignature>,
Host=ali-test-project.regionid.example.com,
Date=Wed, 11 Nov 2015 07:53:29 GMT,
Content-Length=0,
x-log-signaturemethod=hmac-sha1,
User-Agent=sls-java-sdk-v-0.6.0,
Content-Type=application/json
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header :
{
Date=Wed, 11 Nov 2015 07:53:30 GMT,
Content-Length=107,
x-log-requestid=5642F3FA99248C817B01352D,
Connection=close,
Content-Type=application/json,
Server=nginx/1.6.1
}
Body :
{
   "logstoreName" : test-logstore,
   "ttl": 1,
   "shardCount": 2,
   "createTime": 1447833064,
   "lastModifyTime": 1447833064
}
```

2.15.1.7.5. ListLogstore

You can call this operation to list the names of all the Logstores in a specified project.

Request syntax

```
GET /logstores HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

ListLogstore request parameters describes the request parameters.

ListLogstore request parameters

Parameter	Type	Required	Description
offset(optional)	Integer	No	The starting position of returned records. Default value: 1.

Parameter	Type	Required	Description
size(optional)	Integer	No	The maximum number of entries to return on each page. Default and maximum value: 500.
logstoreName	String	No	The name of the Logstore to be filtered. Partial matching is supported.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

When the request is successful, the response body contains the list of names of all the Logstores in a specified project. Response parameters describes the response parameters.

Response parameters

Parameter	Type	Description
count	Integer	The number of returned Logstores.
total	Integer	The total number of Logstores.
logstores	String array	The list of names of returned Logstores.

As described in Error codes specific to ListLogstore, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to ListLogstore

HTTP status code	Error code	Error message
404	ProjectNotExist	Project {ProjectName} does not exist
500	InternalServerError	Specified Server Error Message
400	ParameterInvalid	Invalid parameter size, (0.6.0]
400	InvalidLogStoreQuery	logstore Query is invalid

Examples

Sample requests:

```
GET /logstores HTTP/1.1
Header:
{
x-log-apiversion=0.6.0,
Authorization=LOG <yourAccessKeyId>:<yourSignature>,
Host=ali-test-project.regionid.example.com,
Date=Wed, 11 Nov 2015 08:09:39 GMT,
Content-Length=0,
x-log-signaturemethod=hmac-sha1,
User-Agent=sls-java-sdk-v-0.6.0,
Content-Type=application/json
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header:
{
Date=Wed, 11 Nov 2015 08:09:39 GMT,
Content-Length=52,
x-log-requestid=5642F7C399248C8D7B01342F,
Connection=close,
Content-Type=application/json,
Server=nginx/1.6.1
}
Body:
{
"count":1,
"logstores":["test-logstore"],
"total":1
}
```

2.15.1.7.6. ListShards

You can call this operation to list all the available shards in a Logstore.

Request syntax

```
GET /logstores/<logstorename>/shards HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

ListShards request parameters describes the request parameters.

ListShards request parameters

Parameter	Type	Required	Description
logstoreName	String	No	The name of the Logstore.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

Content-Type: application/json

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The array that consists of shards.

```
[
    {
      "shardID":0
      "status": "readwrite",
      "inclusiveBeginKey": "00000000000000000000000000000000",
        "exclusiveEndKey": "80000000000000000000000000000000",
        "createTime":1453949705
    },
    {
      ...
    },
    {
      ...
    }
]
```

Detailed description

None

Special error codes

As described in Error codes specific to ListShards, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to ListShards

HTTP status code	Error code	Error message
404	LogStoreNotExist	logstore {logstoreName} does not exist
500	InternalServerError	Specified Server Error Message
400	LogStoreWithoutShard	logstore has no shard

The {name} variable in the error message is replaced with a Logstore name.

Examples

Sample requests:

```
GET /logstores/sls-test-logstore/shards
Header :
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Thu, 12 Nov 2015 03:40:31 GMT",
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
Header:
{
   "content-length": "57",
   "server": "nginx/1.6.1",
   "connection": "close",
   "date": "Thu, 12 Nov 2015 03:40:31 GMT",
   "content-type": "application/json",
   "x-log-requestid": "56440A2F99248C050600C74C"
}
Body :
[
   {
      “shardID” : 1,
      “status” :  “readwrite",
      “inclusiveBeginKey” : "00000000000000000000000000000000",
      “exclusiveEndKey” : "80000000000000000000000000000000",
      “createTime” :1453949705
   },
   {
      “shardID” : 2,
      “status” :  “readwrite",
      “inclusiveBeginKey” : "80000000000000000000000000000000",
      “exclusiveEndKey” : "ffffffffffffffffffffffffffffffff",
      “createTime” :1453949705
   },
   {
      “shardID” : 0,
      “status” :  “readonly",
      “inclusiveBeginKey” : "00000000000000000000000000000000",
      “exclusiveEndKey” : "ffffffffffffffffffffffffffffffff",
      “createTime” :1453949705
   }
]
```

2.15.1.7.7. SplitShard

You can call this operation to split a specified shard in the read/write state.

Request syntax

```
POST /logstores/<logstorename>/shards/<shardid>? action=split&key=<splitkey> HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

SplitShard request parameters describes the request parameters.

SplitShard request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore to which the shard to be split belongs.
shardid	Integer	Yes	The ID of the shard to be split.
splitkey	String	Yes	The location where the shard is split.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

Content-Type: application/json

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The following array consists of three shards. The first one is the original shard to be split. The other two are the new shards generated after the split.

```
[
    {
      "shardID":33
       “status” : “readonly",
       “inclusiveBeginKey” : "ee000000000000000000000000000000",
         “exclusiveEndKey” : "ffffffffffffffffffffffffffffffff",
         “createTime” :1453949705
    },
    {
      "shardID":163
       “status” : “readwrite",
       “inclusiveBeginKey” : "ee000000000000000000000000000000",
         “exclusiveEndKey” : "ef000000000000000000000000000000",
         “createTime” :1453949705
    },
    {
      "shardID":164
       “status” : “readwrite",
       “inclusiveBeginKey” : "ef000000000000000000000000000000",
         “exclusiveEndKey” : "ffffffffffffffffffffffffffffffff",
         “createTime” :1453949705
    }
]
```

Detailed description

None

Special error codes

As described in Error codes specific to SplitShard, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to SplitShard

HTTP status code	Error code	Error message
404	LogStoreNotExist	logstore {logstoreName} does not exist
400	ParameterInvalid	invalid shard id
400	ParameterInvalid	invalid mid hash
500	InternalServerError	Specified Server Error Message

HTTP status code	Error code	Error message
400	LogStoreWithoutShard	logstore has no shard

The {name} variable in the error message will be replaced with a Logstore name.

Examples

Sample requests:

```
POST /logstores/logstorename/shards/33? action=split&key=ef00000000000000000000000000000
Header :
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Thu, 12 Nov 2015 03:40:31 GMT",
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
Header:
{
   "content-length": "57",
   "server": "nginx/1.6.1",
   "connection": "close",
   "date": "Thu, 12 Nov 2015 03:40:31 GMT",
   "content-type": "application/json",
   "x-log-requestid": "56440A2F99248C050600C74C"
}
Body :
[
     {
        "shardID":33
         “status” : “readonly",
         “inclusiveBeginKey” : "ee000000000000000000000000000000",
           “exclusiveEndKey” : "ffffffffffffffffffffffffffffffff",
           “createTime” :1453949705
     },
     {
        "shardID":163
         “status” : “readwrite",
         “inclusiveBeginKey” : "ee000000000000000000000000000000",
           “exclusiveEndKey” : "ef000000000000000000000000000000",
           “createTime” :1453949705
     },
     {
        "shardID":164
         “status” : “readwrite",
         “inclusiveBeginKey” : "ef000000000000000000000000000000",
           “exclusiveEndKey” : "ffffffffffffffffffffffffffffffff",
           “createTime” :1453949705
     }
]
```

2.15.1.7.8. MergeShards

You can call this operation to merge two adjacent shards that are in the read/write state. If the ID of a shard is specified, the server will automatically find the adjacent shard at the right of the specified shard.

Request syntax

```
POST /logstores/<logstorename>/shards/<shardid>? action=merge HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

MergeShards request parameters describes the request parameters.

MergeShards request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore.
shardid	Integer	Yes	The ID of the shard.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

Content-Type: application/json

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The following array consists of three shards. The first one is the merged shard. The other two are those before the merging.

```
[
  {
    'shardID': 167,
    'status': 'readwrite',
    'inclusiveBeginKey': 'e00000000000000000000000000000000',
    'createTime': 1453953105,
    'exclusiveEndKey': 'ffffffffffffffffffffffffffffffff'
  },
  {
    'shardID': 30,
    'status': 'readonly',
    'inclusiveBeginKey': 'e00000000000000000000000000000000',
    'createTime': 0,
    'exclusiveEndKey':
    'e70000000000000000000000000000000'
  },
  {
    'shardID': 166,
    'status': 'readonly',
    'inclusiveBeginKey': 'e70000000000000000000000000000000',
    'createTime': 1453953073,
    'exclusiveEndKey': 'ffffffffffffffffffffffffffffffff'
  }
]
```

Detailed description

None

Special error codes

As described in Error codes specific to MergeShards, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to MergeShards

HTTP status code	Error code	Error message
404	LogStoreNotExist	logstore {logstoreName} does not exist
400	ParameterInvalid	invalid shard id
400	ParameterInvalid	cannot merge the last shard
500	InternalServerError	Specified Server Error Message

HTTP status code	Error code	Error message
400	LogStoreWithoutShard	logstore has no shard

The {name} variable in the error message will be replaced with a Logstore name.

Examples

Sample requests:

```
POST /logstores/logstorename/shards/30? action=merge
Header :
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Thu, 12 Nov 2015 03:40:31 GMT",
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
Header:
{
   "content-length": "57",
   "server": "nginx/1.6.1",
   "connection": "close",
   "date": "Thu, 12 Nov 2015 03:40:31 GMT",
   "content-type": "application/json",
   "x-log-requestid": "56440A2F99248C050600C74C"
}
Body :
[
   {
      'shardID': 167,
      'status': 'readwrite',
      'inclusiveBeginKey': 'e00000000000000000000000000000000',
      'createTime': 1453953105,
      'exclusiveEndKey': 'ffffffffffffffffffffffffffffffff'
   },
   {
      'shardID': 30,
      'status': 'readonly',
      'inclusiveBeginKey': 'e00000000000000000000000000000000',
      'createTime': 0,
      'exclusiveEndKey':
      'e70000000000000000000000000000000'
   },
   {
      'shardID': 166,
      'status': 'readonly',
      'inclusiveBeginKey': 'e70000000000000000000000000000000',
      'createTime': 1453953073,
      'exclusiveEndKey': 'fffffffffffffffffffffffffffffffff'
   }
]
```

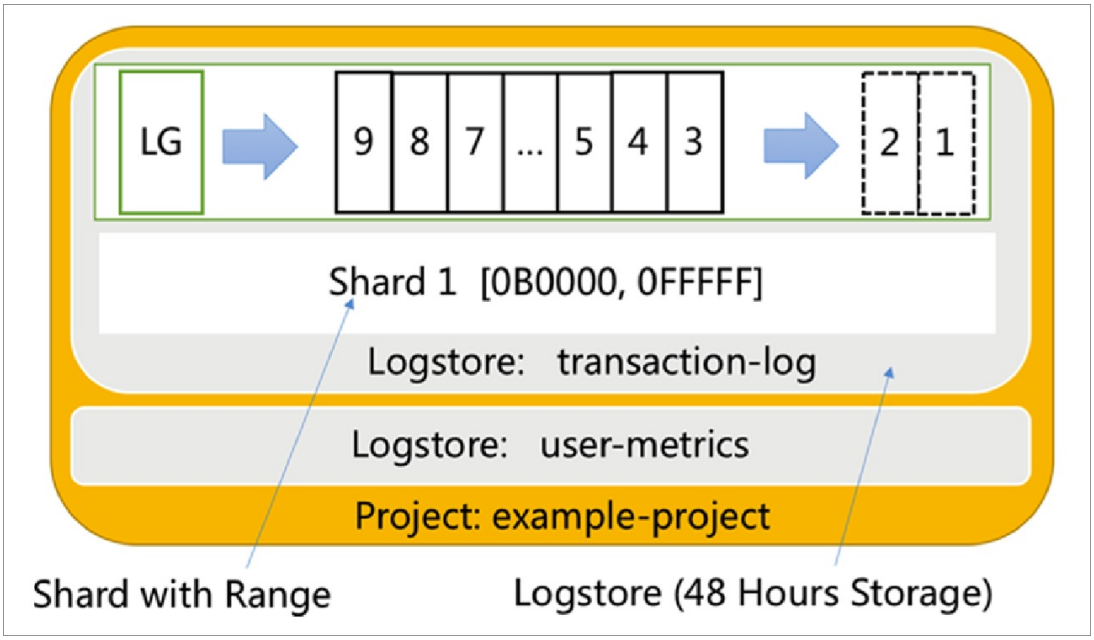
2.15.1.7.9. GetCursor

You can call this operation to get a cursor based on the time. Relationships among a project, a Logstore, a shard, and a cursor shows the relationships among a project, a Logstore, a shard, and a cursor.

- A project can have multiple Logstores.

- Each Logstore can have multiple shards.
- A cursor can be used to locate a specified log.

Relationships among a project, a Logstore, a shard, and a cursor



Request syntax

```
GET /logstores/ay42/shards/2? type=cursor&from=1402341900 HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
```

Request parameters

GetCursor request parameters describes the request parameters.

GetCursor request parameters

Parameter	Type	Required	Description
shard	String	Yes	-
type	String	Yes	The cursor.
from	String	Yes	The point in time. Valid values: begin, end, and a time point expressed in UNIX format and measured in seconds.

Logstore lifecycle:

The lifecycle of a Logstore is specified by the lifeCycle parameter. For example, the current time is 2015-11-11 09:00:00 and the lifeCycle parameter is set to 24. The time range for the consumable data in each shard is [2015-11-10 09:00:00,2015-11-11 09:00:00). The time is the server time.

By using the from parameter, you can locate the logs within the lifecycle in the shard. Assume that the Logstore lifecycle is [begin_time,end_time) and the from parameter is set to from_time.

from_time <= begin_time or from_time == "begin": returns to the cursor position corresponding to the be gin_time.
from_time< = end_time or from_time = "end": returns to the cursor position where the next log entry is written at the current point in time. No log data is available at the current cursor position.
from_time > begin_time and from_time < end_time: returns to the cursor position for the first packet wh ose receipt time on the server is greater than or equal to from_time.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

```
{
  "cursor": "MTQ0NzI5OTYwNjg5NjYzMjM1Ng=="
}
```

Detailed description

None

Error codes

As described in Error codes specific to GetCursor, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to GetCursor

HTTP status code	Error code	Error message
404	LogStoreNotExist	Logstore {Name} does not exist
400	ParameterInvalid	Parameter From is not valid
400	ShardNotExist	Shard {ShardID} does not exist
500	InternalServerError	Specified Server Error Message
400	LogStoreWithoutShard	the logstore has no shard

Examples

Sample requests:

```
GET /logstores/sls-test-logstore/shards/0? type=cursor&from=begin
Header:
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Thu, 12 Nov 2015 03:56:57 GMT",
   "x-log-apiversion": "0.6.0",
   "Content-Type": "application/json",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
Header:
{
   "content-length": "41",
   "server": "nginx/1.6.1",
   "connection": "close",
   "date": "Thu, 12 Nov 2015 03:56:57 GMT",
   "content-type": "application/json",
   "x-log-requestid": "56440E0999248C070600C6AA"
}
Body:
{
   "cursor": "MTQ0NzI5OTYwNjg5NjYzMjM1Ng=="
}
```

2.15.1.7.10. PullLogs

You can call this operation to read logs based on the cursor and the number of returned log groups. You must specify a shard before reading logs. If Storm is used to read log data, elective and collaborative consumption can be performed through LoghubClientLib. Only LogGroupList data in PB format can be read.

Request syntax

```
GET /logstores/ay42/shards/0? type=logs&cursor=MTQ0NzMyOTQwMTEwMjEzMDkwNA==&count=100 HTTP/1.1
Accept: application/x-protobuf
Accept-Encoding: lz4
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
type	String	Yes	The logs.
cursor	String	Yes	Specifies where to start reading log data, which is equivalent to the start point.
count	Integer	Yes	The number of returned log groups. Valid values: 1 to 1000.

Request header

- Accept: application/x-protobuf
- Accept-Encoding: LZ4, deflate or "" .

For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

- x-log-cursor: the cursor for the next batch of log data to be read.
- x-log-count: the number of returned logs.

For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

Data from serialized logs in PB format, which may be compressed.

Detailed description

None

Special error codes

As described in Error codes specific to PullLogs, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to PullLogs

HTTP status code	Error code	Error message
404	LogStoreNotExist	Logstore {Name} does not exist
400	ParameterInvalid	Parameter Cursor is not valid
400	ParameterInvalid	ParameterCount should be in [0-1000]
400	ShardNotExist	Shard {ShardID} does not exist
400	InvalidCursor	this cursor is invalid
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
Read log data from Shard 0.
GET /logstores/sls-test-logstore/shards/0? cursor=MTQ0NzMyOTQwMTEwMjEzMDkwNA==&count=1000&
type=log
Header:
{
   "Authorization"="LOG <yourAccessKeyId>:<yourSignature>",
   "x-log-bodyrawsize"=0,
   "User-Agent" : "sls-java-sdk-v-0.6.0",
   "x-log-apiversion" : "0.6.0",
   "Host" : "ali-test-project.regionid.example.com",
   "x-log-signaturemethod" : "hmac-sha1",
   "Accept-Encoding" : "lz4",
   "Content-Length": 0,
   "Date" : "Thu, 12 Nov 2015 12:03:17 GMT",
   "Content-Type" : "application/x-protobuf",
   "accept" : "application/x-protobuf"
}
```

Sample responses:

```
Header:
{
   "x-log-count" : "1000",
   "x-log-requestid" : "56447FB20351626D7C000874",
   "Server" : "nginx/1.6.1",
   "x-log-bodyrawsize" : "34121",
   "Connection" : "close",
   "Content-Length" : "4231",
   "x-log-cursor" : "MTQ0NzMyOTQwMTEwMjEzMDkwNA==",
   "Date" : "Thu, 12 Nov 2015 12:01:54 GMT",
   "x-log-compresstype" : "lz4",
   "Content-Type" : "application/x-protobuf"
}
Body:
The <LogGroupList data in PB format> after the compression.
```

Page flip

To flip the page (get the next token) without returning data, you can send HTTP HEAD requests.

2.15.1.7.11. PostLogStoreLogs

You can call this operation to write log data to a specified Logstore. Only LogGroup data in protocol buffers (PB) format can be written to a specified Logstore. You can use the following two methods to write log data:

- Load balancing mode: Log data is automatically written to all the writable shards in the Logstore. This mode is applicable to the scenario where you do not need to consider the order in which you consume the log data that is written to multiple shards.
- KeyHash mode: A key is required when log data is written. Log Service automatically selects a shard whose range includes the key. Then, the log data is written to the shard. For example, hash a producer (such as an instance) to a specified shard based on the name of the producer to make sure that the data writing and consumption in this shard are strictly ordered. This ensures that a key appears only on one shard at a given point in time when shards are merged or split.

Request syntax

Load balancing mode

```
POST /logstores/<logstorename>/shards/lb HTTP/1.1
Authorization: <AuthorizationString>
Content-Type: application/x-protobuf
Content-Length: <Content Length>
Content-MD5: <Content MD5>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-bodyrawsize: <BodyRawSize>
x-log-compresstype: lz4
x-log-signaturemethod: hmac-sha1
<Compressed log data in PB format>
```

KeyHash mode

x-log-hashkey is added to the request header to determine the shard whose range includes the key. This parameter is optional. If it is left blank, Log Service automatically switches to the load balancing mode.

```
POST /logstores/<logstorename>/shards/lb HTTP/1.1
Authorization: <AuthorizationString>
Content-Type: application/x-protobuf
Content-Length: <Content Length>
Content-MD5: <Content MD5>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-bodyrawsize: <BodyRawSize>
x-log-compresstype: lz4
x-log-hashkey : 14d2f850ad6ea48e46e4547edbbb27e0
x-log-signaturemethod: hmac-sha1
<Compressed log data in PB format>
```

Request parameters

PostLogStoreLogs request parameters describes the request parameters.

PostLogStoreLogs request parameters

Parameter	Type	Required	Description
logstorename	String	Yes	The name of the Logstore to write logs to.

Request header

In the KeyHash mode, you must add the x-log-hashkey header. For more information, see the preceding example. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

No response parameter is returned after the successful request.

Detailed description

- When you call this operation to write logs, the maximum number of logs in a log group is 4,096, or the maximum size for logs in a log group is 3 MB. The size of the values in each log cannot be larger than 1 MB. If either of the two limits is reached, the request will fail, and no log data will be written.
- Log Service checks the format of the written log data. The request will fail, and no log data will be written if any log does not conform to this format.

Error codes

As described in Error codes specific to PostLogStoreLogs, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to PostLogStoreLogs

HTTP status code	Error code	Error message	Description
400	PostBodyInvalid	Protobuffer content cannot be parsed.	The error message returned because the protocol buffers content cannot be parsed.
400	InvalidTimestamp	Invalid timestamps are in logs.	The error message returned because invalid timestamps appear in logs.
400	InvalidEncoding	Non-UTF8 characters are in logs.	The error message returned because logs contain non-UTF-8 characters.
400	InvalidKey	Invalid keys are in logs.	The error message returned because invalid keys appear in logs.
400	PostBodyTooLarge	Logs must be less than 3M and 4096 lines.	The error message returned because the number of logs exceeds 4,096 or the size of logs is greater than 3 MB.
400	PostBodyUncompressError	Body is uncompressed fail.	The error message returned because log extraction fails.

HTTP status code	Error code	Error message	Description
499	PostBodyInvalid	The post data time is out of range.	The error message returned because the log time is not within the valid range [-7 days, +15 minutes].
404	LogStoreNotExist	logstore {Name}does not exist.	The error message returned because the Logstore does not exist.

The {name} variable in the error message will be replaced with a Logstore name.

Examples

Sample requests:

```
POST /logstores/sls-test-logstore
{
   "Content-Length": 118,
   "Content-Type":"application/x-protobuf",
   "x-log-bodyrawsize":1356,
   "Host": "ali-test-project.regionid.example.com",
   "Content-MD5":"6554BD042149C844761C2C094A8FECCE",
   "Date":"Thu, 12 Nov 2015 06:54:26 GMT",
   "x-log-apiversion": "0.6.0",
   "x-log-compresstype":"lz4"
   "x-log-signaturemethod": "hmac-sha1",
   "Authorization":"LOG <yourAccessKeyId>:<yourSignature>"
}
<Binary log data in PB format compressed with LZ4>
```

Sample responses:

```
Header
{
   "date": "Thu, 12 Nov 2015 06:53:03 GMT",
   "connection": "close",
   "x-log-requestid": "5644160399248C060600D216",
   "content-length": "0",
   "server": "nginx/1.6.1"
}
```

2.15.1.7.12. GetLogs

You can call this operation to query log data in a Logstore under a specified project. You can also query the logs that meet the specific conditions by specifying the relevant parameters.

When a log is written to the Logstore, the latency of querying this log by using Log Service query APIs (GetHistograms and GetLogs) varies with the log type. Based on the log timestamp, Log Service classifies logs into the following two types:

- Real-time data: The time point in a log is the current time point on the server (-180s, 900s]. For example, if the log time is UTC 2014-09-25 12:03:00 and the time when the server receives the log is UTC 2014-09-25 12:05:00, the log is processed as the real-time data, which usually appears in normal scenarios.
- Historical data: The time point in a log is the current time point on the server (-7 x 86400s, -180s]. For example, if the log time is UTC 2014-09-25 12:00:00 and the time when the server receives the log is UTC 2014-09-25 12:05:00, the log is processed as the historical data, which usually appears in the supplementary data scenario.

The maximum latency between a real-time data write and a query is three seconds.

Request syntax

```
GET /logstores/<logstorename>? type=histogram&topic=<logtopic>&from=<starttime>&to=<endtime>&
query=<querystring>&line=<linenum>&offset=<startindex>&reverse=<ture|false> HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-bodyrawsize: 0
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

The request parameters are described in GetLogs request parameters.

GetLogs request parameters

Name	Type	Required	Description
logstorename	String	Yes	The name of the Logstore to which the log to be queried belongs.
type	String	Yes	The type of Logstore data to be queried. This parameter must be log in GetLogs API.
from	Integer	Yes	The query start time (the number of seconds since 1970-1-1 00:00:00 UTC).
to	Integer	Yes	The query end time (the number of seconds since 1970-1-1 00:00:00 UTC).

Name	Type	Required	Description
topic	String	No	The topic of the log to be queried.
query	String	No	The query expression. For the detailed syntax of query statements, see the **Query syntax** section of the *User Guide* .
line	Integer	No	The maximum number of logs returned from the request. Valid values: 0 to 100. Default value: 100.
offset	Integer	No	The returned log start point of the request. Valid values: 0 and a positive integer. Default value: 0.
reverse	Boolean	No	Indicates whether logs are returned in reverse order according to the log timestamp. true indicates reverse order and false indicates sequence order. The default value is false.

Request header

The GetLogs API does not have any special request headers. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

The GetLogs API does not have any special response headers. For more information about the common response headers of Log Service APIs, see Common response headers.

The response header contains a special element that indicates whether the returned results of the request are complete. The specific formats of response elements are described in GetLogs response elements.

GetLogs response elements

Name	Type	Description
progress	String	The status of the query results. The two optional values Incomplete and Complete indicate whether the results are complete or not.
count	Integer	The total number of logs in the current query results.

Response elements

After the successful request, the response body contains the logs that meet the query conditions. The response results of this API may be incomplete when the log volume to be queried is large (measured in TBs). The response body of the GetLogs API is an array, and each element in this array is a log. The structure of each element in the array is described in Element structure.

Element structure

Name	Type	Description
__time__	Integer	The log timestamp (the number of seconds since 1970-1-1 00:00:00 UTC).
__source__	String	The log source, which is specified when logs are written.
[content]	Key-value pair	The original content of the log, which is organized in key-value pairs.

Detailed description

- The time interval defined by the request parameters from and to in this API follows the left-closed and right-opened principle, that is, the time interval includes the start time, but not the end time. If the from and to values are the same, the time interval is invalid and the function returns an error directly.
- Each call to this API must return results within a specified time, and each query can only scan a specified number of logs. The results returned from this request are incomplete if the log volume to be processed for this request is large (whether the results are complete is indicated by using x-log-progress in the response header). At the same time, the server caches the results of the query within 15 minutes. When a portion of the query request results are cache hits, the server continues to scan the log data that are not cache hits for this request. To reduce the workload of merging multiple query results, the server cache hit query results and the new hits of the current query are merged and returned to you. Therefore, Log Service allows you to call the API multiple times with the same parameter to obtain the final complete results. Log Service API cannot predict how many times the API must be called before obtaining the complete results because the volume of the logs to be queried fluctuates dramatically. Therefore, you must check the x-log-progress status in the returned results of each request to determine whether or not to continue the query. Each call to this API consumes the same number of query CUs again.

Special error codes

As described in Error codes specific to GetLogs, in addition to the Common error codes of Log Service APIs, the API may also return the following special error codes.

Error codes specific to GetLogs

HTTP status code	Error code	Error message	Description

HTTP status code	Error code	Error message	Description
404	LogStoreNotExist	logstore {Name} does not exist	The error message returned when the Logstore does not exist.
400	InvalidTimeRange	request time range is invalid	The error message returned when the time interval of the request is invalid.
400	InvalidQueryString	query string is invalid	The error message returned when the query string of the request is invalid.
400	InvalidOffset	offset is invalid	The error message returned when the offset of the request is invalid.
400	InvalidLine	line is invalid	The error message returned when the line of the request is invalid.
400	InvalidReverse	Reverse value is invalid	The error message returned when the Reverse parameter value is invalid.
400	IndexConfigNotExist	logstore without index config	The error message returned when the Logstore does not enable the index.

Note The {name} variable in the preceding error message will be replaced with a specific Logstore name.

Examples

Using a project named big-game as an example, query the logs with the groupA topic in the app_log Logstore of the project. The time interval for this query is 2014-09-01 00:00:00-2014-09-01 22:00:00. The keyword for this query is error. The query starts from the beginning of the time interval, and a maximum of 20 logs are returned.

Sample requests:

```
GET /logstores/app_log type=log&topic=groupA&from=1409529600&to=1409608800&query=error&line=20
&offset=0 HTTP/1.1
Authorization: <AuthorizationString>
Date: Wed, 3 Sept. 2014 08:33:46 GMT
Host: big-game.regionid.example.com
x-log-bodyrawsize: 0
x-log-apiversion: 0.4.0
x-log-signaturemethod: hmac-sha1
```

Sample responses:

```
HTTP/1.1 200 OK
Content-MD5: 36F9F7F0339BEAF571581AF1B0AAAFB5
Content-Type: application/json
Content-Length: 269
Date: Wed, 3 Sept. 2014 08:33:47 GMT
x-log-requestid: efag01234-12341-15432f
x-log-progress : Complete
x-log-count : 10000
x-log-processed-rows: 10000
x-log-elapsed-millisecond:5
{
  "progress": "Complete",
  "count": 2,
  "logs": [
    {
      "__time__": 1409529660,
      "__source__": "10.237.0.17",
      "Key1": "error",
      "Key2": "Value2"
    },
    {
      "__time__": 1409529680,
      "__source__": "10.237.0.18",
      "Key3": "error",
      "Key4": "Value4"
    }
  ]
}
```

In this sample response the x-log-progress status is Complete, which indicates the log query is completed and the returned results are complete. For this request, two logs meet the query condition and are displayed as the values of logs. If the x-log-progress status is Incomplete in the response result, you must repeat the request to obtain the complete results.

2.15.1.7.13. GetHistograms

You can call this operation to query the log distribution in a Logstore of a specific project. By specifying the relevant parameters, it can also query the distribution of the logs that meet the specified criteria.

When a log is written to the Logstore, the latency of querying this log by using Log Service query APIs (GetHistograms and GetLogs) varies according to the log type. Based on the log timestamp, Log Service classifies logs into the following two types:

- Real-time data: For this type, the point of time in a log is the current time point on the server (-180 seconds, 900 seconds]. For example, if the log time is UTC 2014-09-25 12:03:00 and the time when the server receives the log is UTC 2014-09-25 12:05:00, the log is processed as the real-time data, which usually appears in normal scenarios.
- Historical data: The time point in a log is the current time point on the server (-7 x 86400s, -180s]. For example, if the log time is UTC 2014-09-25 12:00:00 and the time when the server receives the log is UTC 2014-09-25 12:05:00, the log is processed as the historical data, which usually appears in the data supplementation scenario.

The latency between a real-time data write and a query is three seconds.

Request syntax

```
GET /logstores/<logstorename>? type=histogram&topic=<logtopic>&from=<starttime>&to=<endtime>&
query=<querystring> HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-bodyrawsize: 0
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

The request parameters are described in GetHistograms request parameters.

GetHistograms request parameters

Name	Type	Required	Description
logstorename	String	Yes	The name of the Logstore to which the log to be queried belongs.
type	String	Yes	The type of Logstore data to be queried. The value of this parameter must be histogram in the GetHistograms API.
from	Integer	Yes	The query start time (the number of seconds elapsed since 1970-1-1 00:00:00 UTC).
to	Integer	Yes	The query end time (the number of seconds elapsed since 1970-1-1 00:00:00 UTC).
topic	String	No	The topic of the log to be queried.

Name	Type	Required	Description
query	String	No	The query statement. For more information about the syntax of query statements, see the *Query syntax* .

Request header

The GetHistograms API does not have any special request headers. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

The GetHistograms API does not have any special response headers. For more information about the common response headers of Log Service APIs, see Common response headers.

Response elements

When a GetHistograms request is successful, the response body contains the distribution of the numbers of log hits returned by the query along the time axis. The response results evenly divide the time range into several (1-60) sub-intervals and return the number of logs that meet the query conditions in each sub-interval. Because Log Service must return results within a limited period to ensure real-time functionality, each query can only scan the specified number of logs. The response results of this API may be incomplete when the log volume to be queried is large. Therefore, the response element contains a specialized member that indicates whether or not the request's return results are complete. The specific response element format is described in GetHistograms response elements.

GetHistograms response elements

Name	Type	Description
progress	String	The status of the query results. The two optional values Incomplete and Complete indicate whether or not the results are complete.
count	Integer	The total number of logs in the current query results.
histograms	Array	The distribution of the current query results in the sub-intervals. For more information about the structure, see the following table.

The structure of each element in the histograms array is described in Histograms array element structure.

Histograms array element structure

Name	Type	Description
from	Integer	The start time for the sub-interval (the number of seconds since 1970-1-1 00:00:00 UTC).
to	Integer	The end time for the sub-interval (the number of seconds since 1970-1-1 00:00:00 UTC).
count	Integer	The number of logs that meet the query conditions for this sub-interval in the current query results.
progress	String	indicates whether the current query results in this sub-interval are complete. Optional values: Incomplete and Complete.

Detailed description

- All the time intervals in this API, whether the time intervals defined by the request parameters from and to, or sub-intervals in the returned results, follow the left-closed and right-opened principle, that is, the time interval includes the start time, but not the end time. If the from and to values are the same, the time interval is invalid and the function directly returns an error.
- The sub-interval division method in the response of this API is consistent and unchanging. If the queried time range remains unchanged, the sub-interval division in the response is also unchanged.
- Each call to this API must return results within a specified time, and each query can only scan a specified number of logs. The results returned from this request are incomplete if the volume of the logs to be processed for this request is large (whether or not the results are complete is indicated by using the progress in the returned results). At the same time, Log Service caches the query results within 15 minutes. When part of the query request results matches those in the cache, the server continues to scan the log data that is not hit in the cache for this request. To reduce the workload of merging multiple query results, the query results of server cache hits and the new hits of the current query are merged and returned. Therefore, Log Service allows you to repeatedly call the API with the same parameters to eventually obtain the complete results. Log Service API cannot predict how many times the API must be called before obtaining the complete results because the volume of the logs to be queried fluctuates dramatically. Therefore, you must check the progress member status in the returned results of each request to determine whether to proceed. Each call to this API consumes the same number of query CUs.

Special error codes

As described in Error codes specific to GetHistograms, in addition to the Common error codes of Log Service APIs, the API may also return the following special error codes.

Error codes specific to GetHistograms

HTTP status code	Error code	Error message	Description
404	LogStoreNotExist	logstore {Name} not exist	The error message returned when the Logstore does not exist.
400	InvalidTimeRange	request time range is invalid	The error message returned when the time interval of the request is invalid.
400	InvalidQueryString	query String is invalid	The error message returned when the query string of the request is invalid.

The {name} variable in the preceding error message will be replaced with a specific Logstore name.

Examples

Using a project named big-game as an example, query the distribution of the logs with the topic groupA in the app_log Logstore of the big-game project. The time interval for this query is 2014-09-01 00:00:00-2014-09-01 22:00:00. The keyword for this query is error.

Sample requests:

```
GET /logstores/app_log? type=histogram&topic=groupA&from=1409529600&to=1409608800&query=error
HTTP/1.1
Authorization: <AuthorizationString>
Date: Wed, 3 Sept. 2014 08:33:46 GMT
Host: big-game.regionid.example.com
x-log-bodyrawsize: 0
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Sample responses:

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-MD5: E6AD9C21204868C2DE84EE3808AAA8C8
Content-Type: application/json
Date: Wed, 3 Sept. 2014 08:33:47 GMT
Content-Length: 232
x-log-requestid: efag01234-12341-15432f
{
  "progress": "Incomplete",
  "count": 3,
  "histograms": [
    {
      "from": 1409529600,
      "to": 1409569200,
      "count": 2,
      "progress": "Complete"
    },
    {
      "from": 1409569200,
      "to": 1409608800,
      "count": 1,
      "progress": "Incomplete"
    }
  ]
}
```

In this sample response, the server divides the entire histogram into two equal time intervals: [2014-09-01 00:00:00, 2014-09-01 11:00:00) and [2014-09-01 11:00:00, 2014-09-01 22:00:00). Because the amount of data is too large, the first query returns incomplete data. In the response, the number of hit logs is 3, but the results are incomplete. Only the results that fall into the time interval [2014-09-01 00:00:00 2014-09-01 11:00:00) are complete, with 2 hits. The results for the other interval are incomplete, but there is already 1 hit. In this situation, to obtain the complete results, you must repeatedly call the preceding sample request until the progress value in the response changes to Complete.

Sample responses:

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-MD5: E6AD9C21204868C2DE84EE3808AAA8C8
Content-Type: application/json
Date: Wed, 3 Sept. 2014 08:33:48 GMT
Content-Length: 232
x-log-requestid: afag01322-1e241-25432e
{
  "progress": "Incomplete",
  "count": 4,
  "histograms": [
    {
      "from": 1409529600,
      "to": 1409569200,
      "count": 2,
      "progress": "Complete"
    },
    {
      "from": 1409569200,
      "to": 1409608800,
      "count": 2,
      "progress": "complete"
    }
  ]
}
```

2.15.1.7.14. CreateIndex

You can call this operation to create an index for a specified Logstore.

Examples:

```
POST /logstores/{logstoreName}/index
```

Request syntax

```
POST /logstores/<logstoreName>/index HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: <x-log-bodyrawsize>
    User-Agent: <User-Agent>
    x-log-apiversion: <APIVersion>
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/json
    Content-MD5: <Content-MD5>
    Content-Length: <Content-Length>
    {
    "line": <full text index>,
    "keys": <key-value index>,
    "ttl": <ttl>
    }
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore for which an index is created.
ttl	Integer	No	The lifecycle of the index to be created. Valid values: 7, 30, and 90. Unit: days.
keys	Object	No	The index configuration that is specified as a key-value pair. Key indicates the field name, and value indicates the field index configuration.
line	Object	No	The configuration of the full-text index.

You must specify the keys parameter or the line parameter or both. The configuration of the full-text index includes the following attributes.

Parameter	Type	Required	Description

Parameter	Type	Required	Description
caseSensitive	Bool	No	Specifies whether the field is case-sensitive.
chn	Bool	No	Specifies whether the field contains Chinese characters.
token	Array	Yes	The list of delimiters.
include_keys	Array	No	The list of included fields. This parameter and the exclude_keys parameter cannot be specified at the same time.
exclude_keys	Array	No	The list of excluded fields. This parameter and the include_keys parameter cannot be specified at the same time.

The configuration of the field index includes the following attributes.

Parameter	Type	Required	Description
type	String	Yes	The type of the field.
alias	String	No	The alias of the field.
chn	Bool	No	Specifies whether the field contains Chinese characters. This parameter exists only when the type parameter is set to text.
token	Array	No.	The list of delimiters. This parameter takes effect only when the type parameter is set to text.
caseSensitive	Bool	No	Specifies whether the field is case-sensitive. This parameter takes effect only when the type parameter is set to text.

Parameter	Type	Required	Description
doc_value	Bool	No	Specifies whether to enable statistical analysis on the field.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
400	IndexInfoInvalid	required field token is lacking or of error format
400	IndexAlreadyExist	log store index is already created
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
500	InternalServerError	Specified Server Error Message

Note {Project} and {logstoreName} in the error messages are replaced by a project name and a Logstore name, respectively.

Examples

Sample requests:

```
POST /logstores/my-logstore/index HTTP/1.1
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
```

```
x-log-signaturemethod: hmac-sha1
Date: Mon, 07 May 2018 09:43:16 GMT
Content-Type: application/json
Content-MD5: 22876515FC311F857AD6C7902F6A0148
Content-Length: 316
Connection: Keep-Alive
{
"line": {
"token": [
",",
" ",
"'",
"\"",
";",
"=",
"(",
")",
"[",
"]",
"{",
"}",
"?",
"@",
"&",
"<",
">",
"/",
":",
"\n",
"\t",
"\r"
]
},
"keys": {
"agent": {
"doc_value": true,
"caseSensitive": true,
"alias": "agent_alias",
"type": "text",
"token": [
",",
" ",
```

```
"",
"\"",
";",
"=",
"(",
")",
"[",
"]",
"{",
"}",
"?",
"@",
"&",
"<",
">",
"/",
":",
"\n",
"\t",
"\r"
]
}
},
"ttl": 90
}
```

2.15.1.7.15. DeleteIndex

You can call this operation to delete the index of a specified Logstore.

Examples:

```
DELETE /logstores/{logstoreName}/index
```

Request syntax

```
DELETE /logstores/<logstoreName>/index HTTP/1.1

Authorization: <AuthorizationString>
x-log-bodyrawsize: 0
User-Agent: <UserAgent>
x-log-apiversion: 0.6.0
Host: <Project Endpoint>
x-log-signaturemethod: hmac-sha1
Date: <GMT Date>
Content-Type: application/x-protobuf
Connection: Keep-Alive
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore to be deleted.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
400	ParameterInvalid	log store index not created
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
DELETE /logstores/my-logstore/index HTTP/1.1

Authorization: LOG <yourAccessKeyId>:<yourSignature>
x-log-bodyrawsize: 0
User-Agent: sls-java-sdk-v-0.6.1
x-log-apiversion: 0.6.0
Host: my-project.cn-shanghai.log.aliyuncs.com
x-log-signaturemethod: hmac-sha1
Date: Sun, 06 May 2018 13:22:57 GMT
Content-Type: application/x-protobuf
Connection: Keep-Alive
```

Sample responses:

```
HTTP/1.1 200

Server: nginx/1.12.1
Content-Length: 0
Connection: close
Access-Control-Allow-Origin: *
Date: Sun, 06 May 2018 13:22:57 GMT
x-log-requestid: 5AEF01B1A458E41C2F8326A8
```

2.15.1.7.16. GetIndex

You can call this operation to query the index of a specified Logstore.

Examples:

```
GET /logstores/{logstoreName}/index
```

Request syntax

```
GET /logstores/<logstoreName>/index HTTP/1.1
Authorization: <AuthorizationString>
x-log-bodyrawsize: 0
User-Agent: <UserAgent>
x-log-apiversion: 0.6.0
Host: <Project Endpoint>
x-log-signaturemethod: hmac-sha1
Date: <GMT Date>
Content-Type: application/x-protobuf
Connection: Keep-Alive
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

When the request is successful, the response body includes the indexes of the specified project and Logstore. The format is described in the following table.

Parameter	Type	Description
index_mode	String	The type of the index.
keys	Dict	The index configuration that is specified as a key-value pair. Key indicates the field name, and value indicates the field index configuration.
line	Object	The configuration of the full-text index.
storage	String	The storage type. pg is supported.
ttl	Integer	The lifecycle of the index. Valid values: 7, 30, and 90. Unit: days.

Parameter	Type	Description
lastModifyTime	Integer	The last time when the index was updated. The time is displayed in the Unix timestamp format.

The configuration of the full-text index includes the following attributes.

Parameter	Type	Description
caseSensitive	Bool	Indicates whether the field is case-sensitive.
chn	Bool	Indicates whether the field contains Chinese characters.
token	Array	The list of delimiters.
include_keys	Array	The list of included fields.
exclude_keys	Array	The list of excluded fields.

The corresponding index configuration of each field includes the following attributes.

Parameter	Type	Description
type	String	The type of the field.
alias	String	The alias of the field.
chn	Bool	Indicates whether the field contains Chinese characters. This parameter takes effect only when the type parameter is set to text.
token	Array	The list of delimiters. This parameter takes effect only when the type parameter is set to text.
caseSensitive	Bool	Indicates whether the field is case-sensitive. This parameter takes effect only when the type parameter is set to text.
doc_value	Bool	Indicates whether to enable statistical analysis on the field.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
400	IndexConfigNotExist	index config doesn't exist
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
GET /logstores/logstore-4/index HTTP/1.1
Authorization: LOG <yourAccessKeyId>:<yourSignature>
x-log-bodyrawsize: 0
User-Agent: sls-java-sdk-v-0.6.1
x-log-apiversion: 0.6.0
Host: my-project.cn-shanghai.log.aliyuncs.com
x-log-signaturemethod: hmac-sha1
Date: Sun, 06 May 2018 13:08:42 GMT
Content-Type: application/x-protobuf
Connection: Keep-Alive
```

Sample responses:

```
HTTP/1.1 200
Server: nginx/1.12.1
Content-Type: application/json
Content-Length: 712
Connection: close
Access-Control-Allow-Origin: *
Date: Sun, 06 May 2018 13:08:42 GMT
x-log-requestid: 5AEEFE5A8B8AEB5E6C82B395
{
 "index_mode": "v2",
 "keys": {
  "agent": {
   "alias": "",
   "caseSensitive": false,
   "chn": false,
   "doc_value": true,
   "token": [
```

```
      ",",
      " ",
      "'",
      "\"",
      ";",
      "=",
      "(",
      ")",
      "[",
      "]",
      "{",
      "}",
      "?",
      "@",
      "&",
      "<",
      ">",
      "/",
      ":",
      "\n",
      "\t",
      "\r"
    ],
    "type": "text"
  },
  "bytes": {
    "alias": "",
    "doc_value": true,
    "type": "long"
  },
  "remote_ip": {
    "alias": "",
    "caseSensitive": false,
    "chn": false,
    "doc_value": true,
    "token": [
      ",",
      " ",
      "'",
      "\"",
      ";",
      "=",
```

```
      "(",
      ")",
      "[",
      "]",
      "{",
      "}",
      "?",
      "@",
      "&",
      "<",
      ">",
      "/",
      ":",
      "\n",
      "\t",
      "\r"
    ],
    "type": "text"
  },
  "response": {
    "alias": "",
    "doc_value": true,
    "type": "long"
  }
},
"line": {
  "caseSensitive": false,
  "chn": false,
  "token": [
    ",",
    " ",
    "'",
    "\"",
    ";",
    "=",
    "(",
    ")",
    "[",
    "]",
    "{",
    "}",
```

```
    "?",
    "@",
    "&",
    "<",
    ">",
    "/",
    ":",
    "\n",
    "\t",
    "\r"
   ]
  },
  "storage": "pg",
  "ttl": 30,
  "lastModifyTime": 1524155379
}
```

2.15.1.7.17. UpdateIndex

You can call this operation to update the index of a specified Logstore.

Examples:

```
PUT /logstores/{logstoreName}/index
```

Request syntax

```
PUT /logstores/<logstoreName>/index HTTP/1.1
Authorization: <AuthorizationString>
x-log-bodyrawsize: 0
User-Agent: <UserAgent>
x-log-apiversion: 0.6.0
Host: <Project Endpoint>
x-log-signaturemethod: hmac-sha1
Date: <GMT Date>
Content-Type: application/json
Content-MD5: <Content-MD5>
Content-Length: <ContentLength>
{
  "line": <full text index>,
  "keys": <key-value index>,
  "ttl": <ttl>
}
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore.
ttl	Integer	No	The lifecycle of the index to be updated. Value values: 7, 30, and 90. Unit: days.
keys	Object	No	The index configuration that is specified as a key-value pair. Key indicates the field name, and value indicates the field index configuration.
line	Object	No	The configuration of the full-text index.

You must specify the keys parameter or the line parameter or both. The configuration of the full-text index includes the following attributes.

Parameter	Type	Required	Description
token	Array	Yes	The list of delimiters.

Parameter	Type	Required	Description
caseSensitive	Bool	No	Specifies whether the field is case-sensitive.
chn	Bool	No	Specifies whether the field contains Chinese characters.
include_keys	Array	No	The list of included fields. This parameter and the exclude_keys parameter cannot be specified at the same time.
exclude_keys	Array	No	The list of the excluded fields. This parameter and the include_keys parameter cannot be specified at the same time.

The configuration of the field index includes the following attributes.

Parameter	Type	Required	Description
type	String	Yes	The type of the field.
alias	String	No	The alias of the field.
chn	Bool	No	Specifies whether the field contains Chinese characters. This parameter takes effect only when the type parameter is set to text.
token	Array	No	The list of delimiters. This parameter takes effect only when the type parameter is set to text.
caseSensitive	Bool	No	Specifies whether the field is case-sensitive. This parameter takes effect only when the type parameter is set to text.

Parameter	Type	Required	Description
doc_value	Bool	No	Specifies whether to enable statistical analysis on the field.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
400	ParameterInvalid	log store index is not created
400	ParameterInvalid	key config must has type
400	IndexInfoInvalid	required field token is lacking or of error format
400	IndexInfoInvalid	required fields line/keys are lacking or of error format
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
500	InternalServerError	Specified Server Error Message

Examples

- Sample requests

```
PUT /logstores/logstore-4/index HTTP/1.1
Header:
Authorization: LOG <yourAccessKeyId>:<yourSignature>
x-log-bodyrawsize: 0
User-Agent: sls-java-sdk-v-0.6.1
x-log-apiversion: 0.6.0
Host: my-project.cn-shanghai.log.aliyuncs.com
```

```
x-log-signaturemethod: hmac-sha1
Date: Mon, 07 May 2018 09:47:20 GMT
Content-Type: application/json
Content-MD5: 1860B805A6AA5288B97B32CF3B519112
Content-Length: 316
Connection: Keep-Alive
Body:
{
 "line": {
  "token": [
   ",",
   " ",
   "",
   "\"",
   ";",
   "=",
   "(",
   ")",
   "[",
   "]",
   "{",
   "}",
   "?",
   "@",
   "&",
   "<",
   ">",
   "/",
   ":",
   "\n",
   "\t",
   "\r"
  ]
 },
 "keys": {
  "agent": {
   "doc_value": true,
   "caseSensitive": true,
   "alias": "agent_alias",
   "type": "text",
   "token": [
```

```
      ",",
      " ",
      "'",
      "\"",
      ";",
      "=",
      "(",
      ")",
      "[",
      "]",
      "{",
      "}",
      "?",
      "@",
      "&",
      "<",
      ">",
      "/",
      ":",
      "\n",
      "\t",
      "\r"
    ]
   }
  },
  "ttl": 90
}
```

- Sample responses

```
HTTP/1.1 200
Server: nginx/1.12.1
Content-Length: 0
Connection: close
Access-Control-Allow-Origin: *
Date: Mon, 07 May 2018 09:47:21 GMT
x-log-requestid: 5AF020A98CBAA2EF52AB66C9
```

2.15.1.8. Logtail machine group operations

2.15.1.8.1. CreateMachineGroup

You can call this operation to create a machine group to which the configurations on Logtail are distributed and applied.

Examples:

```
POST /machinegroups
```

Request syntax

```
POST /machinegroups HTTP/1.1
Authorization: <AuthorizationString>
Content-Type:application/json
Content-Length:<Content Length>
Content-MD5<:<Content MD5>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
{
   "groupName" : "testgroup",
   "groupType" : "",
   "groupAttribute" : {
      "externalName" : "testgroup",
      "groupTopic": "testgrouptopic"
   },
   "machineIdentifyType" : "ip",
   "machineList" : [
      "test-ip1",
      "test-ip2"
   ]
}
```

Request parameters

Request body parameters describes the request body parameters.

Request body parameters

Parameter	Type	Required	Description
groupName	String	Yes	The name of the machine group. The name must be unique within a project.
groupType	String	No	The type of the machine group. Default value: null.

Parameter	Type	Required	Description
machineIdentifyType	String	Yes	The type of a machine identifier, which can be either IP address or user-defined identifier.
groupAttribute	Object	Yes	The attribute of the machine group. Default value: null.
machineList	Array	Yes	The list of machine identifiers. Valid values: IP addresses or user-defined identifiers.

groupAttribute details describes groupAttribute details.

groupAttribute details

Parameter	Type	Required	Description
groupTopic	String	No	The topic of the machine group. Default value: null.
externalName	String	No	The ID of the external management system (Armory) on which the machine group depends on. Default value: null.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to CreateMachineGroup, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to CreateMachineGroup

HTTP status code	Error code	Error message
400	GroupAlreadyExist	group {GroupName} already exists

HTTP status code	Error code	Error message
400	InvalidParameter	invalid group resource json
500	InternalServerError	Internal server error

Detailed description

None

Examples

Sample requests:

```
POST /machinegroups HTTP/1.1
Header :
{
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Tue, 10 Nov 2015 17:57:33 GMT",
   "Content-Length": "187",
   "x-log-signaturemethod": "hmac-sha1",
   "Content-MD5": "82033D507DEAAD72067BB58DFDCB590D",
   "User-Agent": "sls-java-sdk-v-0.6.0",
   "Content-Type": "application/json",
   "x-log-bodyrawsize": "0"
}
Body :
{
   "groupName": "test-machine-group",
   "groupType": "",
   "machineIdentifyType": "ip",
   "groupAttribute":    {
      "groupTopic": "testtopic",
      "externalName": "testgroup"
   },
   "machineList":    [
      "127.0.0.1",
      "127.0.0.2"
   ]
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header :
{
   "Date": "Tue, 10 Nov 2015 17:57:33 GMT",
   "Content-Length": "0",
   "x-log-requestid": "5642300D99248CB76D005D36",
   "Connection": "close",
   "Server": "nginx/1.6.1"
}
```

2.15.1.8.2. DeleteMachineGroup

You can call this operation to delete a machine group. The configurations on Logtail that are applied to the machine group will be deleted along with the machine group.

Examples:

```
DELETE /machinegroups/{groupName}
```

Request syntax

```
DELETE /machinegroups/{groupName} HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
groupName	String	Yes	The name of the machine group.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to DeleteMachineGroup, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to DeleteMachineGroup

HTTP status code	Error code	Error message
404	GroupNotExist	group {GroupName} does not exist
500	InternalServerError	internal server error

Detailed description

None

Examples

Sample requests:

```
DELETE /machinegroups/test-machine-group-4 HTTP/1.1
Header :
{
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Tue, 10 Nov 2015 19:13:28 GMT",
   "Content-Length": "0",
   "x-log-signaturemethod": "hmac-sha1",
   "User-Agent": "sls-java-sdk-v-0.6.0",
   "Content-Type": "application/x-protobuf",
   "x-log-bodyrawsize": "0"
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header :
{
   "Date": "Tue, 10 Nov 2015 19:13:28 GMT",
   "Content-Length": "0",
   "x-log-requestid": "564241D899248C827B000CFE",
   "Connection": "close",
   "Server": "nginx/1.6.1"
}
```

2.15.1.8.3. UpdateMachineGroup

You can call this operation to update the information of a machine group. If the configurations on Logtail are applied to a machine group, they are automatically added or removed when machines are added to or removed from the machine group.

Examples:

```
PUT /machinegroups/{groupName}
```

Request syntax

```
PUT /machinegroups/{groupName} HTTP/1.1
Authorization: <AuthorizationString>
Content-Type:application/json
Content-Length:<Content Length>
Content-MD5<:<Content MD5>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
{
   "groupName": "test-machine-group",
   "groupType" : "",
   "groupAttribute" : {
      "externalName" : "testgroup",
      "groupTopic": "testgrouptopic"
   },
   "machineIdentifyType" : "ip",
   "machineList" : [
      "test-ip1",
      "test-ip2"
   ]
}
```

Request parameters

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
groupName	String	Yes	The name of the machine group.

Request body parameters describes the request body parameters.

Request body parameters

Parameter	Type	Required	Description
groupName	String	Yes	The name of the machine group. The name must be unique within a project.
groupType	String	No	The type of the machine group. Default value: null.

Parameter	Type	Required	Description
machineIdentifyType	String	Yes	The type of a machine identifier, which can be either IP address or user-defined identifier.
groupAttribute	Object	Yes	The attribute of the machine group. Default value: null.
machineList	Array	Yes	The list of machine identifiers. Valid values: IP addresses or user-defined identifiers.

groupAttribute details describes groupAttribute details.

groupAttribute details

Parameter	Type	Required	Description
groupTopic	String	No	The topic of the machine group. Default value: null.
externalName	String	No	The ID of the external management system (Armory) on which the machine group depends. Default value: null.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to UpdateMachineGroup, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to UpdateMachineGroup

HTTP status code	Error code	Error message
404	GroupNotExist	group {GroupName} does not exist

HTTP status code	Error code	Error message
400	InvalidParameter	invalid group resource json
500	InternalServerError	internal server error

Detailed description

None

Examples

Sample requests:

```
PUT /machinegroups/test-machine-group HTTP/1.1
Header :
{
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Tue, 10 Nov 2015 18:41:43 GMT",
   "Content-Length": "194",
   "x-log-signaturemethod": "hmac-sha1",
   "Content-MD5": "2CEBAEBE53C078891527CB70A855BAF4",
   "User-Agent": "sls-java-sdk-v-0.6.0",
   "Content-Type": "application/json",
   "x-log-bodyrawsize": "0"
}
Body :
{
   "groupName": "test-machine-group",
   "groupType": "",
   "machineIdentifyType": "userdefined",
   "groupAttribute":    {
      "groupTopic": "testtopic2",
      "externalName": "testgroup2"
   },
   "machineList":    [
      "uu_id_1",
      "uu_id_2"
   ]
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header :
{
   "Date": "Tue, 10 Nov 2015 18:41:43 GMT",
   "Content-Length": "0",
   "x-log-requestid": "56423A6799248CA57B00035C",
   "Connection": "close",
   "Server": "nginx/1.6.1"
}
```

2.15.1.8.4. ListMachineGroup

Examples:

```
GET /machinegroups? offset=1&size=100
```

Request syntax

```
GET /machinegroups? offset=1&size=100 HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
offset	Integer	No	The starting position of returned records. Default value: 0.
size	Integer	No	The maximum number of entries to return on each page. Default and maximum value: 500.
groupName	String	No	The name of the machine group to be filtered. Partial matching is supported.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

When the request is successful, the response body contains the list of names of all machine groups in the specified project. ListMachineGroup response parameters describes ListMachineGroup response parameters.

ListMachineGroup response parameters

Parameter	Type	Description
count	Integer	The number of returned machine groups.
total	Integer	The total number of returned machine groups.
machinegroups	JSON array	The list of names of returned machine groups.

```
{
  "machinegroups":  [
    "test-machine-group",
    "test-machine-group-2"
  ],
  "count": 2,
  "total": 2
}
```

Error codes

As described in Error codes specific to ListMachineGroup, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to ListMachineGroup

HTTP status code	Error code	Error message
500	InternalServerError	internal server error

Detailed description

None

Examples

Sample requests:

```
GET /machinegroups? groupName=test-machine-group&offset=0&size=3 HTTP/1.1
Header :
{
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Tue, 10 Nov 2015 18:34:44 GMT",
   "Content-Length": "0",
   "x-log-signaturemethod": "hmac-sha1",
   "User-Agent": "sls-java-sdk-v-0.6.0",
   "Content-Type": "application/x-protobuf",
   "x-log-bodyrawsize": "0"
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header :
{
   "Date": "Tue, 10 Nov 2015 18:34:44 GMT",
   "Content-Length": "83",
   "x-log-requestid": "564238C499248C8F7B0001DE",
   "Connection": "close",
   "Content-Type": "application/json",
   "Server": "nginx/1.6.1"
}
Body :
{
   "machinegroups":    [
      "test-machine-group",
      "test-machine-group-2"
   ],
   "count": 2,
   "total": 2
}
```

2.15.1.8.5. GetMachineGroup

You can call this operation to view the details of a machine group.

Examples:

```
GET /machinegroups/{groupName}
```

Request syntax

```
GET /machinegroups/{groupName} HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
groupName	String	Yes	The name of the machine group.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

GetMachineGroup response parameters describes the response parameters.

GetMachineGroup response parameters

Parameter	Type	Description
groupName	String	The name of the machine group. The name must be unique within a project.
groupType	String	The type of the machine group. Valid values: null and Armory. Default value: null.
machineIdentifyType	String	The type of a machine identifier, which can be either IP address or user-defined identifier.

Parameter	Type	Description
groupAttribute	JSON object	The attribute of the machine group. Default value: null.
machineList	JSON array	The list of machine identifiers. Valid values: IP addresses or user-defined identifiers.
createTime	Integer	The time when the machine group was created.
lastModifyTime	Integer	The last time when the machine group was updated.

groupAttribute details describes groupAttribute details.

groupAttribute details

Parameter	Type	Required	Description
groupTopic	String	No	The topic of the machine group, which is typically not specified.
externalName	String	No	The ID of the external management system (Armory) on which the machine group depends.

```
{
  "groupName": "test-machine-group",
  "groupType": "",
  "groupAttribute":    {
    "externalName": "testgroup",
    "groupTopic": "testtopic"
  },
  "machineIdentifyType": "ip",
  "machineList":    [
    "127.0.0.1",
    "127.0.0.2"
  ],
  "createTime": 1447178253,
  "lastModifyTime": 1447178253
}
```

Error codes

As described in Error codes specific to GetMachineGroup, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to GetMachineGroup

HTTP status code	Error code	Error message
404	GroupNotExist	group {GroupName} does not exist
500	InternalServerError	internal server error

Detailed description

None

Examples

Sample requests:

```
GET /machinegroups/test-machine-group HTTP/1.1
Header :
{
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Tue, 10 Nov 2015 18:15:24 GMT",
   "Content-Length": "0",
   "x-log-signaturemethod": "hmac-sha1",
   "User-Agent": "sls-java-sdk-v-0.6.0",
   "Content-Type": "application/x-protobuf",
   "x-log-bodyrawsize": "0"
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header :
{
   "Date": "Tue, 10 Nov 2015 18:15:23 GMT",
   "Content-Length": "239",
   "x-log-requestid": "5642343B99248CB36D0060B8",
   "Connection": "close",
   "Content-Type": "application/json",
   "Server": "nginx/1.6.1"
}
Body :
{
   "groupName": "test-machine-group",
   "groupType": "",
   "groupAttribute":    {
      "externalName": "testgroup",
      "groupTopic": "testtopic"
   },
   "machineIdentifyType": "ip",
   "machineList":    [
      "127.0.0.1",
      "127.0.0.2"
   ],
   "createTime": 1447178253,
   "lastModifyTime": 1447178253
}
```

2.15.1.8.6. ApplyConfigToMachineGroup

You can call this operation to apply a configuration to a machine group.

Examples:

```
PUT /machinegroups/{GroupName}/configs/{ConfigName}
```

Request parameters

ApplyConfigToMachineGroup request parameters describes the request parameters.

ApplyConfigToMachineGroup request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
GroupName	String	Yes	The name of the machine group.
ConfigName	String	Yes	The name of the log configuration to be applied to the machine group.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to ApplyConfigToMachineGroup, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to ApplyConfigToMachineGroup

HTTP status code	Error code	Error message
404	GroupNotExist	group {GroupName} does not exist
404	ConfigNotExist	config {ConfigName} does not exist
500	InternalServerError	internal server error

Examples

Sample requests:

```
PUT /machinegroups/sample-group/configs/logtail-config-sample
Header :
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Mon, 09 Nov 2015 09:44:43 GMT",
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
{
   "date": "Mon, 09 Nov 2015 09:44:43 GMT",
   "connection": "close",
   "x-log-requestid": "56406B0B99248CAA230BA094",
   "content-length": "0",
   "server": "nginx/1.6.1"
}
```

2.15.1.8.7. RemoveConfigFromMachineGroup

You can call this operation to remove a configuration from a machine group.

Examples:

```
DELETE /machinegroups/{GroupName}/configs/{ConfigName}
```

Request parameters

RemoveConfigFromMachineGroup request parameters describes the request parameters.

RemoveConfigFromMachineGroup request parameters

Parameter	Type	Required	Description
GroupName	String	Yes	The name of the machine group.
ConfigName	String	Yes	The name of the log configuration.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to RemoveConfigFromMachineGroup, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to RemoveConfigFromMachineGroup

HTTP status code	Error code	Error message
404	GroupNotExist	group {GroupName} does not exist
404	ConfigNotExist	config {ConfigName} does not exist
500	InternalServerError	internal server error

Examples

Sample requests:

```
DELETE /machinegroups/sample-group/configs/logtail-config-sample
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Mon, 09 Nov 2015 09:48:48 GMT",
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
{
    "date": "Mon, 09 Nov 2015 09:48:48 GMT",
    "connection": "close",
    "x-log-requestid": "56406C0099248CAA230BE135",
    "content-length": "0",
    "server": "nginx/1.6.1"
}
```

2.15.1.8.8. ListMachines

You can call this operation to query the status of your machines that are in a machine group and connected to the server.

Examples:

```
GET /machinegroups/{groupName}/machines? offset=1&size=10
```

Request syntax

```
GET /machinegroups/{groupName}/machines HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
groupName	String	Yes	The name of the machine group.
offset	Integer	No	The starting position of returned records. Default value: 0.
size	Integer	No	The maximum number of entries to return on each page. Default and maximum value: 500.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

ListMachines response parameters describes the response parameters.

ListMachines response parameters

Parameter	Type	Description
count	Integer	The number of returned machines.
total	Integer	The total number of machines.
machines	JSON array	The list of names of returned machines.

Machine details describes the machine details.

Machine details

Parameter	Type	Description
ip	String	The IP address of the machine.
machine-uniqueid	String	The DMI UUID of the machine.
userdefined-id	String	The user-defined identifier of the machine.

```
{
   "count":10,
   "total":100,
   "machines":
   [{
      "ip" : "testip1",
      "machine-uniqueid" : "testuuid1",
      "userdefined-id" : "testuserdefinedid1",
      "lastHeartbeatTime" : 1447182247
   },
   {
      "ip" : "testip1",
      "machine-uniqueid" : "testuuid2",
      "userdefined-id" : "testuserdefinedid2",
      "lastHeartbeatTime" : 1447182247
   },
   {
      "ip" : "testip2",
      "machine-uniqueid" : "testuuid",
      "userdefined-id" : "testuserdefinedid"
      "lastHeartbeatTime" : 1447182247
   }]
}
```


Error codes

As described in Error codes specific to ListMachines, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to ListMachines

HTTP status code	Error code	Error message
404	GroupNotExist	group {GroupName} does not exist
500	InternalServerError	internal server error

Detailed description

This operation only obtains the list of server-connected machines that work properly.

Examples

Sample requests:

```
GET /machinegroups/test-machine-group-5/machines? offset=0&size=3 HTTP/1.1
Header :
{
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Tue, 10 Nov 2015 19:04:57 GMT",
   "Content-Length": "0",
   "x-log-signaturemethod": "hmac-sha1",
   "User-Agent": "sls-java-sdk-v-0.6.0",
   "Content-Type": "application/x-protobuf",
   "x-log-bodyrawsize": "0"
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header :
{
   "Date": "Tue, 10 Nov 2015 19:04:58 GMT",
   "Content-Length": "324",
   "x-log-requestid": "56423FD999248C827B000A57",
   "Connection": "close",
   "Content-Type": "application/json",
   "Server": "nginx/1.6.1"
}
Body :
{
   "machines":    [
      {
         "ip": "10.101.166.116",
         "machine-uniqueid": "",
         "userdefined-id": "",
         "lastHeartbeatTime": 1447182247
      },
      {
         "ip": "10.101.165.193",
         "machine-uniqueid": "",
         "userdefined-id": "",
         "lastHeartbeatTime": 1447182246
      },
      {
         "ip": "10.101.166.91",
         "machine-uniqueid": "",
         "userdefined-id": "",
         "lastHeartbeatTime": 1447182248
      }
   ],
   "count": 3,
   "total": 8
}
```

2.15.1.8.9. GetAppliedConfigs

You can call this operation to retrieve the name of the configuration that is applied to a machine group.

Examples:

```
GET /machinegroups/{groupName}/configs
```

Request syntax

```
GET /machinegroups/{groupName}/configs HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
groupName	String	Yes	The name of the machine group.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

When the request is successful, the response body includes the list of all machines in the specified machine group. Machine list describes the list of machines.

Machine list

Parameter	Type	Description
count	Integer	The number of returned configurations.
configs	String array	The list of names of returned configurations.

```
{
   "count":2,
   "configs":
   ["config1","config2"]
}
```

Error codes

As described in Error codes specific to GetAppliedConfigs, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to GetAppliedConfigs

HTTP status code	Error code	Error message
404	GroupNotExist	group {GroupName} does not exist
500	InternalServerError	internal server error

Detailed description

None

Examples

Sample requests:

```
GET /machinegroups/test-machine-group/configs HTTP/1.1
Header :
{
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Tue, 10 Nov 2015 19:45:48 GMT",
   "Content-Length": "0",
   "x-log-signaturemethod": "hmac-sha1",
   "User-Agent": "sls-java-sdk-v-0.6.0",
   "Content-Type": "application/x-protobuf",
   "x-log-bodyrawsize": "0"
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header :
{
   "Date": "Tue, 10 Nov 2015 19:45:48 GMT",
   "Content-Length": "53",
   "x-log-requestid": "5642496C99248C8C7B00173F",
   "Connection": "close",
   "Content-Type": "application/json",
   "Server": "nginx/1.6.1"
}
Body :
{
   "configs":    [
      "two",
      "three",
      "test_logstore"
   ],
   "count": 3
}
```

2.15.1.9. Logtail configuration operations

2.15.1.9.1. CreateConfig

You can call this operation to create log configurations in a project.

Examples:

```
POST /configs
```

Request syntax

```
POST /configs HTTP/1.1
Authorization: <AuthorizationString>
Content-Type:application/json
Content-Length:<Content Length>
Content-MD5<:<Content MD5>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
{
   "configName": "testcategory1",
   "inputType": "file",
   "inputDetail": {
      "logType": "common_reg_log",
      "logPath": "/var/log/httpd/",
      "filePattern": "access*.log",
      "localStorage": true,
      "timeFormat": "%Y/%m/%d %H:%M:%S",
      "logBeginRegex": ".*",
      "regex": "(\w+)(\s+)",
      "key" :["key1", "key2"],
      "filterKey":["key1"],
      "filterRegex":["regex1"],
      "fileEncoding":"utf8",
      "topicFormat": "none"
   },
   "outputType": "LogService",
   "outputDetail":
   {
      "logstoreName": "perfcounter"
   }
}
```

Request parameters

CreateConfig request parameters describes the request parameters.

CreateConfig request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
configName	String	Yes	The name of the log configuration. The name must be unique within a project.
inputType	String	Yes	The input type. Only the file type is supported.
inputDetail	JSON	Yes	See inputDetail details.
outputType	String	Yes	The output type. Only LogService is supported.
outputDetail	JSON	Yes	See outputDetail details.
logSample	String	No	The log sample of the Logtail configuration. The log size cannot exceed 1,000 bytes.

inputDetail details describes inputDetail types.

inputDetail details

Parameter	Type	Required	Description
logType	String	Yes	The type of the log. Only the common_reg_log type is supported.
logPath	String	Yes	The parent directory where the log is located. For example, `/var/logs/`.
filePattern	String	Yes	The type of the log file. For example, `access*.log`.
localStorage	Boolean	Yes	Specifies whether to enable local cache. Logs up to 1 GB can be locally cached when the link to Log Service is disconnected.
timeFormat	String	Yes	The format of the log time. For example, `%Y/%m/%d %H:%M:%S`.
logBeginRegex	String	Yes	The characteristics (regular expression) of the first line of a log entry. This parameter is used to match a log entry that consists of multiple lines.

Parameter	Type	Required	Description
regex	String	Yes	The regular expression for extracting logs.
key	Array	Yes	The key that is generated after logs are extracted.
filterKey	Array	Yes	The key used to filter logs. A log is considered valid only when the key value matches the regular expression specified in the corresponding filterRegex column.
filterRegex	Array	Yes	The regular expression corresponding to each filterKey. The length of filterRegex must be the same as that of filterKey.
topicFormat	String	No	The topic generation method. The following four methods are supported: • A part of the log file path is used as the topic. For example, `/var/log/(.*).log`. • none indicates that the topic is empty. • default indicates that the log file path is used as the topic (for internal users only). • group_topic indicates that the topic attribute of the machine group to which this configuration is applied is used as the topic.
preserve	Boolean	No	Valid values: true and false. true indicates that the monitoring of the directory never times out, while false indicates that the timeout for directory monitoring is 30 minutes. The default value is true.

Parameter	Type	Required	Description
preserveDepth	Integer	No	Specifies the depth of the monitored directories if preserve is set to false. The maximum depth is 3.
fileEncoding	String	No	The encoding format of the log file. UTF-8 and GBK are supported.

outputDetail details describes outputDetail types.

outputDetail details

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the corresponding Logstore.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to CreateConfig, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to CreateConfig

HTTP status code	Error code	Error message
400	ConfigAlreadyExist	config {Configname} already exists
400	InvalidParameter	invalid config resource json
500	InternalServerError	internal server error

Detailed description

The configuration fails to be created if an error occurs during the creation. For example, the configuration already exists, the format is incorrect, the required parameters are not specified, or the quota is exhausted.

Examples

Sample requests:

```
POST /configs HTTP/1.1
Header :
{
   'Content-Length': 737,
   'Host': 'ali-test-project.regionid.example.com',
   'x-log-bodyrawsize': 737,
   'Content-MD5': 'FBA01ECF7255BE143379BC70C56BBF68',
   'x-log-signaturemethod': 'hmac-sha1',
   'Date': 'Mon, 09 Nov 2015 07:45:30 GMT',
   'x-log-apiversion': '0.6.0',
   'User-Agent': 'log-python-sdk-v-0.6.0',
   'Content-Type': 'application/json',
   'Authorization': 'LOG <yourAccessKeyId>:<yourSignature>'
}
Body:
{
   "configName": "sample-logtail-config",
   "inputType": "file",
   "inputDetail": {
      "logType": "common_reg_log",
      "logPath": "/var/log/httpd/",
      "filePattern": "access*.log",
      "localStorage": true,
      "timeFormat": "%d/%b/%Y:%H:%M:%S",
      "logBeginRegex": "\\d+\\.\\d+\\.\\d+\\.\\d+ - .*",
      "regex": "([\\d\\.] +) \\S+ \\S+ \\[(\\S+) \\S+\\] \"(\\w+) ([^\"]*)\" ([\\d\\.]+) (\\d+) (\\d+) (\\d+|-) \
"([^\"]*)\" \"([^\"]*)\".*",
      "key": ["ip", "time", "method", "url", "request_time", "request_length", "status", "length", "ref_url", "br
owser"],
      "filterKey": [],
      "filterRegex": [],
      "topicFormat": "none",
      "fileEncoding": "utf8"
   },
   "outputType": "LogService",
   "outputDetail":
   {
      "logstoreName": "sls-test-logstore"
   }
}
```

Sample responses:

```
HTTP/1.1 200 OK
Header
{
   'date': 'Mon, 09 Nov 2015 07:45:30 GMT',
   'connection': 'close',
   'x-log-requestid': '56404F1A99248CA26C002180',
   'content-length': '0',
   'server': 'nginx/1.6.1'
}
```

2.15.1.9.2. ListConfig

You can call this operation to list all configurations of a project on multiple pages.

Examples:

```
GET /configs? offset=1&size=100
```

Request syntax

```
GET /configs? offset=0&size=100 HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
offset(optional)	Integer	No	The starting position of returned records. Default value: 0.
size(optional)	Integer	No	The maximum number of entries to return on each page. Default and maximum value: 500.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The response body contains a list of all configurations in the project. Response parameters describes the response parameters.

Response parameters

Parameter	Type	Description
count	Integer	The number of returned configurations.
total	Integer	The total number of configurations in Log Service.
configs	String array	The name list of returned configurations.

Error codes

As described in Error codes specific to ListConfig, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to ListConfig

HTTP status code	Error code	Error message
404	ConfigNotExist	config {Configname} does not exist
500	InternalServerError	internal server error

Detailed description

None

Examples

Sample requests:

```
GET /configs? offset=0&size=10 HTTP/1.1
Header :
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Mon, 09 Nov 2015 09:19:13 GMT",
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
Header :
{
   "content-length": "103",
   "server": "nginx/1.6.1",
   "connection": "close",
   "date": "Mon, 09 Nov 2015 09:19:13 GMT",
   "content-type": "application/json",
   "x-log-requestid": "5640651199248CAA2300C2BA"
}
Body:
{
   "count": 3,
   "configs":
   [
      "logtail-config-sample",
      "logtail-config-sample-2",
      "logtail-config-sample-3"
   ],
   "total": 3
}
```

2.15.1.9.3. GetAppliedMachineGroups

You can call this operation to list the machine groups to which the configuration is applied.

Examples:

```
GET /configs/{configName}/machinegroups
```

Request syntax

```
GET /configs/{configName}/machinegroups HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
ConfigName	String	Yes	The name of the configuration.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

When the request is successful, the response body includes the list of all machines in the specified machine group. Response parameters describes the response parameters.

Response parameters

Parameter	Type	Description
count	Integer	The number of returned machine groups.
machinegroups	String array	The list of names of returned machine groups.

```
{
   "count":2,
   "machinegroups":
   ["group1","group2"]
}
```

Error codes

As described in Error codes specific to GetAppliedMachineGroups, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to GetAppliedMachineGroups

HTTP status code	Error code	Error message
404	GroupNotExist	group {GroupName} does not exist
500	InternalServerError	internal server error

Detailed description

None

Examples

Sample requests:

```
GET /configs/logtail-config-sample/machinegroups
Header:
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Mon, 09 Nov 2015 09:51:38 GMT",
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
Header :
{
   "content-length": "44",
   "server": "nginx/1.6.1",
   "connection": "close",
   "date": "Mon, 09 Nov 2015 09:51:38 GMT",
   "content-type": "application/json",
   "x-log-requestid": "56406CAA99248CAA230BE828"
}
Body:
{
   "count": 1,
   "machinegroups":
   [
      "sample-group"
   ]
}
```

2.15.1.9.4. GetConfig

You can call this operation to query the details of a configuration.

Examples:

```
GET /configs/{configName}
```

Request syntax

```
GET /configs/<configName> HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

GetConfig request parameters describes the request parameters.

GetConfig request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
ConfigName	String	Yes	The name of the log configuration.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

GetConfig response parameters describes the response parameters.

GetConfig response parameters

Parameter	Type	Description
configName	String	The name of the log configuration. The name must be unique within a project.
inputType	String	The input type. Only the file type is supported.
inputDetail	JSON	The output type. The following table describes inputDetail.
outputType	String	The output type. Only LogService is supported.
outputDetail	JSON	The following table describes outputDetail.
createTime	Int	The time when the configuration was created.
lastModifyTime	Int	The time when the resource was updated on the server.

inputDetail details describes inputDetail parameters.

inputDetail details

Parameter	Type	Description
logType	String	The type of the log. Only the common_reg_log type is supported.

Parameter	Type	Description
logPath	String	The parent directory where the log is located. For example, `/var/logs/`.
filePattern	String	The pattern of the log file. For example, `access*.log`.
localStorage	Boolean	Indicates whether to enable local cache. Logs up to 1 GB can be locally cached when the link to Log Service is disconnected.
timeFormat	String	The format of the log time. For example, `%Y/%m/%d %H:%M:%S`.
logBeginRegex	String	The characteristics (regular expression) of the first line of a log entry. This parameter is used to match a log entry that consists of multiple lines.
regex	String	The regular expression for extracting logs.
key	Array	The key generated after logs are extracted.
filterKey	Array	The key used to filter logs. A log is considered valid only when the key value matches the regular expression specified in the corresponding filterRegex column.
filterRegex	Array	The regular expression corresponding to each filterKey. The length of filterRegex must be the same as that of filterKey.
topicFormat	String	Indicates that a part of the log file path is used as the topic. For example, `/var/log/(.*).log`. The default value is none, which indicates that the topic is empty.

Parameter	Type	Description
preserve	Boolean	Valid values: true and false. true indicates that the monitoring of the directory never times out, while false indicates that the timeout for directory monitoring is 30 minutes. The default value is true.
preserveDepth	Integer	Specifies the depth of the monitored directories if preserve is set to false. The maximum depth is 3.
fileEncoding	String	The encoding format of the log file. UTF-8 and GBK are supported.

outputDetail details describes the outputDetail parameters.

outputDetail details

Parameter	Type	Required	Description
endpoint	String	No	The endpoint of the region where the project is located. The value of this parameter does not include the project name as the prefix. If this parameter is not specified, the default value is EndPoint.
logstoreName	String	Yes	The name of the Logstore.

Error codes

As described in Error codes specific to GetConfig, in addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to GetConfig

HTTP status code	Error code	Error message
404	ConfigNotExist	Config {Configname} does not exist
500	InternalServerError	Specified Server Error Message

Detailed description

N/A

Examples

Sample requests:

```
GET /configs/logtail-config-sample
Header :
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Mon, 09 Nov 2015 08:29:15 GMT",
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
Header :
{
   "content-length": "730",
   "server": "nginx/1.6.1",
   "connection": "close",
   "date": "Mon, 09 Nov 2015 08:29:15 GMT",
   "content-type": "application/json",
   "x-log-requestid": "5640595B99248CAA23004A59"
}
Body :
{
   "configName": "logtail-config-sample",
   "outputDetail": {
      "endpoint": "http://regionid.example.com",
      "logstoreName": "sls-test-logstore"
   },
   "outputType": "LogService",
   "inputType": "file",
   "inputDetail": {
      "regex": "([\\d\\.] +) \\S+ \\S+ \\[(\\S+) \\S+\\] \"(\\w+) ([^\"]*)\" ([\\d\\.]+) (\\d+) (\\d+) (\\d+|-) \
"([^\"]*)\" \"([^\"]*)\".*",
      "filterKey": [],
      "logPath": "/var/log/httpd/",
      "logBeginRegex": "\\d+\\.\\d+\\.\\d+\\.\\d+ - .*",
      "logType": "common_reg_log",
```

```
        "topicFormat": "none",
        "localStorage": true,
        "key": [
            "ip",
            "time",
            "method",
            "url",
            "request_time",
            "request_length",
            "status",
            "length",
            "ref_url",
            "browser"
        ],
        "filePattern": "access*.log",
        "timeFormat": "%d/%b/%Y:%H:%M:%S",
        "filterRegex": []
    },
    "createTime": 1447040456,
    "lastModifyTime": 1447050456
}
```

2.15.1.9.5. DeleteConfig

You can call this operation to delete a specified configuration. If the configuration is applied to a machine group, the Logtail configuration is also deleted from the machine group.

Examples:

```
DELETE /configs/{configName}
```

Request syntax

```
DELETE /configs/<configName> HTTP/1.1
Authorization: <AuthorizationString>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
```

Request parameters

URL parameters describes the URL parameters.

URL parameters

Parameter	Type	Required	Description
ConfigName	String	Yes	The name of the log configuration.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to DeleteConfig, in addition to the Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to DeleteConfig

HTTP status code	Error code	Error message
404	ConfigNotExist	config {Configname} not exist
400	InvalidParameter	invalid config resource json
500	InternalServerError	internal server error

Examples

Sample requests:

```
DELETE /configs/logtail-config-sample
Header :
{
   "Content-Length": 0,
   "x-log-signaturemethod": "hmac-sha1",
   "x-log-bodyrawsize": 0,
   "User-Agent": "log-python-sdk-v-0.6.0",
   "Host": "ali-test-project.regionid.example.com",
   "Date": "Mon, 09 Nov 2015 09:28:21 GMT",
   "x-log-apiversion": "0.6.0",
   "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
```

Sample responses:

```
Header :
{
   "date": "Mon, 09 Nov 2015 09:28:21 GMT",
   "connection": "close",
   "x-log-requestid": "5640673599248CAA230836C6",
   "content-length": "0",
   "server": "nginx/1.6.1"
}
```

2.15.1.9.6. UpdateConfig

You can call this operation to update a configuration. If the updated configuration is applied to a machine group, the machines in this machine group are also updated.

Examples:

```
PUT /configs/{configName}
```

Request syntax

```
PUT /configs/<configName> HTTP/1.1
Authorization: <AuthorizationString>
Content-Type:application/json
Content-Length:<Content Length>
Content-MD5<:<Content MD5>
Date: <GMT Date>
Host: <Project Endpoint>
x-log-apiversion: 0.6.0
x-log-signaturemethod: hmac-sha1
{
   "configName": "testcategory1",
   "inputType": "file",
   "inputDetail": {
      "logType": "common_reg_log",
      "logPath": "/var/log/httpd/",
      "filePattern": "access.log",
      "localStorage": true,
      "timeFormat": "%Y/%m/%d %H:%M:%S",
      "logBeginReg": ".*",
      "regex": "(\w+)(\s+)",
      "key" :["key1", "key2"],
      "filterKey":["key1"],
      "filterRegex":["regex1"],
      "topicFormat": "none"
   },
   "outputType": "LogService",
   "outputDetail":
   {
      "logstoreName": "perfcounter"
   }
}
```

Request parameters

UpdateConfig request parameters describes the request parameters.

UpdateConfig request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
configName	String	Yes	The name of the log configuration to be updated. The name must be unique within a project.
inputType	String	Yes	The input type. Only the file type is supported.
inputDetail	JSON	Yes	The following table describes inputDetail.
outputType	String	Yes	The output type. Only LogService is supported.
outputDetail	JSON	Yes	The following table describes outputDetail.

inputDetail details describes the inputDetail parameters.

inputDetail details

Parameter	Type	Required	Description
logType	String	Yes	The type of the log. Only the common_reg_log type is supported.
logPath	String	Yes	The parent directory where the log is located. For example, `/var/logs/`.
filePattern	String	Yes	The pattern of the log file. For example, `access*.log`.
localStorage	Boolean	Yes	Specifies whether to enable local cache. Logs up to 1 GB can be locally cached when the link to Log Service is disconnected.
timeFormat	String	Yes	The format of the log time. For example, `%Y/%m/%d %H:%M:%S`.
logBeginRegex	String	Yes	The characteristics (regular expression) of the first line of a log entry. This parameter is used to match a log entry that consists of multiple lines.

Parameter	Type	Required	Description
regex	String	Yes	The regular expression for extracting logs.
key	Array	Yes	The key that is generated after logs are extracted.
filterKey	Array	Yes	The key used to filter logs. A log is considered valid only when the key value matches the regular expression specified in the corresponding filterRegex column.
filterRegex	Array	Yes	The regular expression corresponding to each filterKey. The length of filterRegex must be the same as that of filterKey.
topicFormat	String	No	A part of the log file path is used as the topic. For example, `/var/log/(. *).log`. The default value is none, which indicates that the topic is empty.
preserve	Boolean	No	Valid values: true and false. true indicates that the monitoring of the directory never times out, while false indicates that the timeout for directory monitoring is 30 minutes. The default value is true.
preserveDepth	Integer	No	Specifies the depth of the monitored directories if preserve is set to false. The maximum depth is 3.
fileEncoding	String	No	The encoding format of the log file. UTF-8 and GBK are supported. The default value is UTF-8.

outputDetail details describes outputDetail parameters.

outputDetail details

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

As described in Error codes specific to UpdateConfig, in addition to the Common error codes of Log Service APIs, this operation may also return the following special error codes.

Error codes specific to UpdateConfig

HTTP status code	Error code	Error message
404	ConfigNotExist	config {Configname} does not exist
400	InvalidParameter	invalid config resource json
400	BadRequest	config resource configname not match request
500	InternalServerError	internal server error

Detailed description

The configuration fails to be created if an error occurs during the creation period. For example, the format is incorrect, the required parameters are missing, or the quota is exhausted.

Examples

Sample requests:

```
PUT /configs/logtail-config-sample
Header :
{
   "Content-Length": 737,
   "Host": "ali-test-project.regionid.example.com",
   "x-log-bodyrawsize": 737,
   "Content-MD5": "431263EB105D584A5555762A81E869C0",
   "x-log-signaturemethod": "hmac-sha1",
   "Date": "Mon, 09 Nov 2015 09:14:32 GMT",
   "x-log-apiversion": "0.6.0",
   "User-Agent": "log-python-sdk-v-0.6.0",
```

```
    "Content-Type": "application/json",
    "Authorization": "LOG <yourAccessKeyId>:<yourSignature>"
}
Body :
{
    "outputDetail": {
        "logstoreName": "sls-test-logstore"
    },
    "inputType": "file",
    "inputDetail": {
        "regex": "([\\d\\.] +) \\S+ \\S+ \\[(\\S+) \\S+\\] \"(\\w+) ([^\"]*)\" ([\\d\\.]+) (\\d+) (\\d+) (\\d+|-) \
"([^\"]*)\" \"([^\"]*)\".*",
        "filterKey": [],
        "logPath": "/var/log/nginx/",
        "logBeginRegex": "\\d+\\.\\d+\\.\\d+\\.\\d+ - .*",
        "logType": "common_reg_log",
        "topicFormat": "none",
        "localStorage": true,
        "key": [
            "ip",
            "time",
            "method",
            "url",
            "request_time",
            "request_length",
            "status",
            "length",
            "ref_url",
            "browser"
        ],
        "filePattern": "access*.log",
        "timeFormat": "%d/%b/%Y:%H:%M:%S",
        "filterRegex": []
    },
    "outputType": "LogService",
    "configName": "logtail-config-sample"
}
```

Sample responses:

```
{
   "date": "Mon, 09 Nov 2015 09:14:32 GMT",
   "connection": "close",
   "x-log-requestid": "564063F899248CAA2300B778",
   "content-length": "0",
   "server": "nginx/1.6.1"
}
```

2.15.1.10. Consumer group operations

2.15.1.10.1. CreateConsumerGroup

You can call this operation to create a consumer group for a specified Logstore.

Examples:

```
POST /logstores/{logstoreName}/consumergroups
```

Request syntax

```
POST /logstores/<logstoreName>/consumergroups HTTP/1.1
        Authorization: <AuthorizationString>
        x-log-bodyrawsize: 0
        User-Agent: <UserAgent>
        x-log-apiversion: 0.6.0
        Host: <Project Endpoint>
        x-log-signaturemethod: hmac-sha1
        Date: <GMT Date>
        Content-Type: application/json
        Content-MD5: F58544E4D022CC28A93D0B7CC208A5AA
        Content-Length: <ContentLength>
        {
        "consumerGroup": <consumerGroup>,
        "timeout": <timeout>,
        "order": <order>
        }
```

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore for which the consumer group is created.
consumerGroup	String	Yes	The name of the consumer group to be created. The name must be unique within a project.
timeout	Integer	Yes	The heartbeat timeout. If no heartbeat packet is received during this period, the consumer group will be deleted.
order	Bool	Yes	Specifies whether to consume log data in order.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
400	ConsumerGroupAlreadyExist	consumer group already exist
400	JsonInfoInvalid	consumerGroup or timeout is of error format
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
POST /logstores/my-logstore/consumergroups HTTP/1.1
    Header:
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Fri, 04 May 2018 08:02:22 GMT
    Content-Type: application/json
    Content-MD5: F58544E4D022CC28A93D0B7CC208A5AA
    Content-Length: 65
    Connection: Keep-Alive
    Body:
    {
    "consumerGroup": "consumer-group-1",
    "timeout": 300,
    "order": true
    }
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx/1.12.1
    Content-Length: 0
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Fri, 04 May 2018 08:15:11 GMT
    x-log-requestid: 5AEC168FA796F4195BF404CB
```

2.15.1.10.2. DeleteConsumerGroup

You can call this operation to delete a specified consumer group.

Examples:

```
DELETE /logstores/{logstoreName}/consumergroups/{consumerGroupName}
```

Request syntax

```
DELETE /logstores/<logstoreName>/consumergroups/<consumerGroupName> HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/x-protobuf
    Content-MD5: F58544E4D022CC28A93D0B7CC208A5AA
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore to which the consumer group belongs.
consumerGroup	String	Yes	The name of the consumer group to be deleted.

Request header

No special request header is required. For more information about common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
500	InternalServerError	Specified Server Error Message

Detailed description

If you attempt to delete a consumer group that does not exist, the system will return a success message.

Examples

Sample requests:

```
DELETE /logstores/logstore-test/consumergroups/consumer-group-1 HTTP/1.1
    Header:
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Fri, 04 May 2018 08:02:22 GMT
    Content-Type: application/json
    Content-MD5: F58544E4D022CC28A93D0B7CC208A5AA
    Content-Length: 65
    Connection: Keep-Alive
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx/1.12.1
    Content-Length: 0
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Fri, 04 May 2018 08:15:11 GMT
    x-log-requestid: 5AEC168FA796F4195BF404CB
```

2.15.1.10.3. GetCheckPoint

You can call this operation to query the checkpoints of one or all shards that are consumed by a specified consumer group.

Examples:

```
GET /logstores/{logstoreName}/consumergroups/{consumerGroupName}? shard={shardId}
```

Request syntax

```
GET /logstores/<logstoreName>/consumergroups/<consumerGroup>? shard=<shardId> HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/json
    Connection: Keep-Alive
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore to which the consumer group belongs.
consumerGroup	String	Yes	The name of the consumer group.
shardId	Integer	No	The ID of the shard. If the shard ID is not specified, checkpoints of all shards are returned.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

If the request is successful, the response body contains the checkpoint of the shard that is consumed by the specified consumer group. The response parameters are described as follows.

Parameter	Type	Description
shard	Integer	The ID of the shard.
checkpoint	String	The value of the checkpoint.
updateTime	Integer	The last time when the checkpoint was updated.

Parameter	Type	Description
consumer	String	The consumer of the shard.

Error codes

In addition to Common response headers of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
404	ConsumerGroupNotExist	consumer group not exist
500	InternalServerError	Specified Server Error Message

Detailed description

If the specified shard does not exist, an empty list is returned. If the shard ID is not specified, checkpoints of all shards are returned.

Examples

Sample requests:

```
GET /logstores/my-logstore/consumergroups/consumer_group_test? shard=0
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Fri, 04 May 2018 09:26:53 GMT
    Content-Type: application/x-protobuf
    Connection: Keep-Alive
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx/1.12.1
    Content-Type: application/json
    Content-Length: 111
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Fri, 04 May 2018 09:26:53 GMT
    x-log-requestid: 5AEC275D1FFC036AB254B20C
    [
    {
    "shard": 0,
    "checkpoint": "MTUyNDE1NTM3OTM3MzkwODQ5Ng==",
    "updateTime": 1524224984800922,
    "consumer": "consumer_1"
    }
    ]
```

2.15.1.10.4. HeartBeat

You can call this operation to send a heartbeat packet to the server for a specified consumer.

Examples:

```
POST /logstores/{logstoreName}/consumergroups/{consumerGroupName}? type=heartbeat&consumer={consumer}
```

Request syntax

```
POST /logstores/<logstoreName>/consumergroups/<consumerGroup>? type=heartbeat&consumer=<consumer> HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/json
    Content-MD5: F58544E4D022CC28A93D0B7CC208A5AA
    Content-Length: <ContentLength>
    <shard ID list>
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore. The name must be unique within a project.
consumerGroup	String	Yes	The name of the consumer group. The name must be unique within a project.
consumer	String	Yes	The consumer of shards.
{Shard ID List}	Array	Yes	The ID list of shards that are being consumed.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

If the request is successful, the HTTP status code 200 and the ID list of all shards consumed by the consumer are returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
400	NotExistConsumerWithBody	non-exist consumer with non-empty body of heartbeat message
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
404	ConsumerGroupNotExist	consumer group not exist
500	InternalServerError	Specified Server Error Message

Detailed description

The heartbeat packet is sent only when the connection between the consumer and the server is established.

Examples

Sample requests:

```
POST /logstores/my-logstore/consumergroups/consumer_group_test? type=heartbeat&consumer=cons
umer_1 HTTP/1.1
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Sun, 06 May 2018 09:44:10 GMT
    Content-Type: application/json
    Content-MD5: 8D5162CA104FA7E79FE80FD92BB657FB
    Content-Length: 3
    Connection: Keep-Alive
    [0]
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx/1.12.1
    Content-Type: application/json
    Content-Length: 5
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Sun, 06 May 2018 09:44:11 GMT
    x-log-requestid: 5AEECE6B1FFC0366B2553FB5
    [0,1]
```

2.15.1.10.5. ListConsumerGroup

You can call this operation to query all consumer groups of a specified Logstore.

Examples:

```
GET /logstores/{logstoreName}/consumergroups
```

Request syntax

```
GET /logstores/<logstoreName>/consumergroups HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/x-protobuf
    Connection: Keep-Alive
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore to which consumer groups belong.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

If the request is successful, the response body contains the list of all consumer groups in the specified project and Logstore. The response parameters are described as follows.

Parameter	Type	Description
consumerGroup	String	The name of the consumer group.
timeout	Integer	The heartbeat timeout. If no heartbeat packet is received during this period, the consumer group will be deleted.
order	Bool	Indicates whether to consume log data in order.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
GET /logstores/my-logstore/consumergroups HTTP/1.1
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Fri, 04 May 2018 08:47:30 GMT
    Content-Type: application/x-protobuf
    Connection: Keep-Alive
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx/1.12.1
    Content-Type: application/json
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Fri, 04 May 2018 08:47:31 GMT
    x-log-requestid: 5AEC1E23048191954B42EAB9
    [
    {
    "name": "test-consumer-group",
    "timeout": 30,
    "order": true
    }
    ]
```

2.15.1.10.6. UpdateCheckPoint

You can call this operation to update the checkpoint of a shard for a consumer group in a specified project and Logstore.

Examples:

```
POST /logstores/{logstoreName}/consumergroups/{consumerGroupName}? forceSuccess={forceSuccess}
&type=checkpoint&consumer={consumer}
```

Request syntax

```
POST /logstores/<logstoreName>/consumergroups/<consumerGroupName>? forceSuccess=<forceSucce
ss>&type=checkpoint&consumer=<consumer> HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/json
    Content-Length: <ContentLength>
    Connection: Keep-Alive
    {
    "shard": <shardID>,
    "checkpoint": <checkpoint>
    }
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore to which the consumer group belongs.
consumerGroup	String	Yes	The name of the consumer group.
forceSuccess	Bool	No	Specifies whether to force update.
consumer	String	No	The consumer of the shard.
shard	Integer	Yes	The ID of the shard.

Parameter	Type	Required	Description
checkpoint	String	Yes	The value of the checkpoint.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
400	InvalidShardCheckPoint	shard checkpoint not encoded by base64
404	ProjectNotExist	The Project does not exist : {Project}
404	LogStoreNotExist	logstore {logstoreName} dose not exist
404	ConsumerGroupNotExist	consumer group not exist
404	ShardNotExist	shard not exist
500	InternalServerError	Specified Server Error Message

Detailed description

If the consumer is not specified, the checkpoint of the shard can be updated only when forceSuccess is set to true.

Examples

Sample requests:

```
POST /logstores/logstore-4/consumergroups/consumer_group_test? forceSuccess=false&type=checkpo
int&consumer=consumer_1 HTTP/1.1
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Sun, 06 May 2018 09:14:53 GMT
    Content-Type: application/json
    Content-MD5: 59457BAFB3F85A5117BDE243947583B0
    Content-Length: 55
    Connection: Keep-Alive
    {
    "shard": 0,
    "checkpoint": "MTUyNDE1NTM3OTM3MzkwODQ5Ng=="
    }
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx/1.12.1
    Content-Length: 0
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Sun, 06 May 2018 09:14:54 GMT
    x-log-requestid: 5AEEC78E1FFC0366B24F1C63
```

2.15.1.10.7. UpdateConsumerGroup

You can call this operation to modify the attributes of a specified consumer group.

Examples:

```
PUT /logstores/{logstoreName}/consumergroups/{consumerGroupName}
```

Request syntax

```
PUT /logstores/<logstoreName>/consumergroups/<consumerGroupName> HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/json
    Content-MD5: F58544E4D022CC28A93D0B7CC208A5AA
    Content-Length: <ContentLength>
    {
    "timeout": <timeout>,
    "order": <order>
    }
```

Request parameters

Parameter	Type	Required	Description
logstoreName	String	Yes	The name of the Logstore to which the consumer group belongs.
consumerGroup	String	Yes	The name of the consumer group.
timeout	Integer	No	The heartbeat timeout. If no heartbeat packet is received during this period, the consumer group will be deleted.
order	Bool	No	Specifies whether to consume log data in order.

Note You must specify `timeout` or `order`, or both.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
400	JsonInfoInvalid	timout is of error value type
404	ProjectNotExist	The Project does not exist : {Project}
404	ConsumerGroupNotExist	consumer group not exist
404	LogStoreNotExist	logstore {logstoreName} dose not exist
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
PUT /logstores/logstore-test/consumergroups/consumer-group-1 HTTP/1.1
    Header:
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Fri, 04 May 2018 08:02:22 GMT
    Content-Type: application/json
    Content-MD5: F58544E4D022CC28A93D0B7CC208A5AA
    Content-Length: 65
    Connection: Keep-Alive
    Body:
    {
    "order": false,
    "timeout": 100
    }
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx/1.12.1
    Content-Length: 0
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Fri, 04 May 2018 08:15:11 GMT
    x-log-requestid: 5AEC168FA796F4195BF404CB
```

2.15.1.11. Project operations

2.15.1.11.1. CreateProject

You can call this operation to create a project.

Examples:

```
POST /
```

Request syntax

```
POST / HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/json
    Content-MD5: <Content-MD5>
    Content-Length: <ContentLength>
    Connection: Keep-Alive
    {
    "projectName": <ProjectName>,
    "description": <Description>
    }
```

Request parameters

Parameter	Type	Required	Description
projectName	String	Yes	The name of the project to be created.

Parameter	Type	Required	Description
description	String	Yes	The description of the project to be created.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
400	ProjectAlreadyExist	Project {project} already exist
400	ParameterInvalid	The body is not valid json string
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
POST / HTTP/1.1
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project-test.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Sun, 27 May 2018 07:43:26 GMT
    Content-Type: application/json
    Content-MD5: A7967D81EFF5E3CD447FB6D8DF294E20
    Content-Length: 80
    Connection: Keep-Alive
    {
    "projectName": "my-project-test",
    "description": "Description of my-project-test"
    }
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx
    Content-Length: 0
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Sun, 27 May 2018 07:43:27 GMT
    x-log-requestid: 5B0A619F205DC3F30EDA9322
```

2.15.1.11.2. DeleteProject

You can call this operation to delete a specified project.

Examples:

```
DELETE /
```

Request syntax

```
DELETE / HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/x-protobuf
    Connection: Keep-Alive
```

Request parameters

Parameter	Type	Required	Description
projectName	String	Yes	The name of the project to be deleted. The name is a part of the host in the header.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

The HTTP status code 200 is returned.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
404	ProjectNotExist	The Project does not exist : {Project}
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
DELETE / HTTP/1.1
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project-test.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Sun, 27 May 2018 08:25:04 GMT
    Content-Type: application/x-protobuf
    Connection: Keep-Alive
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx
    Content-Length: 0
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Sun, 27 May 2018 08:25:04 GMT
    x-log-requestid: 5B0A6B60BB6EE39764D458B5
```

2.15.1.11.3. GetProject

You can call this operation to query a project by project name.

Examples:

```
GET /
```

Request syntax

```
GET / HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Project Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/x-protobuf
    Connection: Keep-Alive
```

Request parameters

Parameter	Type	Required	Description
projectName	String	Yes	The name of the project to be queried. The name is a part of the host in the header.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

When the request is successful, the response body contains the detailed information of the project in the following format.

Parameter	Type	Description
createTime	String	The time when the project was created.
description	String	The description of the project.
lastModifyTime	String	The last time when the project was modified.
owner	String	The account ID of the project creator.

Parameter	Type	Description
projectName	String	The name of the project.
status	String	The status of the project.
region	String	The region to which the project belongs.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
404	ProjectNotExist	The Project does not exist : {Project}
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
DELETE / HTTP/1.1
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: my-project-test.cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Sun, 27 May 2018 08:25:04 GMT
    Content-Type: application/x-protobuf
    Connection: Keep-Alive
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx
    Content-Length: 0
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Sun, 27 May 2018 08:25:04 GMT
    x-log-requestid: 5B0A6B60BB6EE39764D458B5
```

2.15.1.11.4. ListProject

You can call this operation to query the list of all projects in a region.

Examples:

```
GET /? offset={offset}&size={size}
```

Request syntax

```
GET /? offset={offset}&size={size} HTTP/1.1
    Authorization: <AuthorizationString>
    x-log-bodyrawsize: 0
    User-Agent: <UserAgent>
    x-log-apiversion: 0.6.0
    Host: <Endpoint>
    x-log-signaturemethod: hmac-sha1
    Date: <GMT Date>
    Content-Type: application/x-protobuf
    Connection: Keep-Alive
```

Request parameters

Parameter	Type	Required	Description
offset	Integer	No	The starting position of returned records. Default value: 0.
size	Integer	No	The maximum number of entries to return on each page. Default and maximum value: 500.

Request header

No special request header is required. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

No special response header is returned. For more information about the common response headers of Log Service APIs, see Common response headers.

Response parameters

When the request is successful, the response body contains the project list in the following format.

Parameter	Type	Description
count	Integer	The number of returned projects.

Parameter	Type	Description
total	Integer	The total number of projects in a region.
projects	Array	The list of all projects in a region.

Parameters of projects are described as follows.

Parameter	Type	Description
createTime	String	The time when the project was created.
description	String	The description of the project.
lastModifyTime	String	The last time when the project was modified.
owner	String	The account ID of the project creator.
projectName	String	The name of the project.
status	String	The status of the project.
region	String	The region to which the project belongs.

Error codes

In addition to Common error codes of Log Service APIs, this operation may also return the following special error codes.

HTTP status code	Error code	Error message
500	InternalServerError	Specified Server Error Message

Examples

Sample requests:

```
GET /? offset=0&size=2&projectName= HTTP/1.1
    Authorization: LOG <yourAccessKeyId>:<yourSignature>
    x-log-bodyrawsize: 0
    User-Agent: sls-java-sdk-v-0.6.1
    x-log-apiversion: 0.6.0
    Host: cn-shanghai.log.aliyuncs.com
    x-log-signaturemethod: hmac-sha1
    Date: Sun, 27 May 2018 09:03:33 GMT
    Content-Type: application/x-protobuf
    Connection: Keep-Alive
```

Sample responses:

```
HTTP/1.1 200
    Server: nginx
    Content-Type: application/json
    Content-Length: 345
    Connection: close
    Access-Control-Allow-Origin: *
    Date: Sun, 27 May 2018 09:03:33 GMT
    x-log-requestid: 5B0A7465AAEA20CA70DE3064
    {
    "count": 2,
    "total": 11,
    "projects": [
    {
    "projectName": "project1",
    "status": "Normal",
    "owner": "",
    "description": "",
    "region": "cn-shanghai",
    "createTime": "1524222931",
    "lastModifyTime": "1524539357"
    },
    {
    "projectName": "project123456",
    "status": "Normal",
    "owner": "",
    "description": "",
    "region": "cn-shanghai",
    "createTime": "1471963876",
    "lastModifyTime": "1524539357"
    }
    ]
    }
```

2.15.1.11.5. GetProjectLogs

You can call this operation to count all the logs in a project.

Request syntax

```
GET /logs/? query=SELECT * FROM <logStoreName> where __line__ = 'abc' and __date__ >'2017-09-01 00:0
0:00' and __date__ < '2017-09-02 00:00:00'&line=20&offset=0 HTTP/1.1
    Authorization: <AuthorizationString>
    Date: Wed, 3 Sept. 2014 08:33:46 GMT
    Host: big-game.cn-hangzhou.log.aliyuncs.com
    x-log-bodyrawsize: 0
    x-log-apiversion: 0.4.0
    x-log-signaturemethod: hmac-sha1
```

Request parameters

Attribute name	Type	Required	Description
query	String	Yes	The SQL query criteria

Request header

The GetProjectLogs API does not have any special request headers. For more information about the common request headers of Log Service APIs, see Common request headers.

Response header

For more information about the common response headers of Log Service APIs, see Common response headers.

The response header contains a special element that indicates whether the returned results of the request are complete. The specific response element format is as follows:

Name	Type	Description
x-log-progress	String	The status of the query results. The two values, Incomplete and Complete, indicate whether the results are complete.
x-log-count	Integer	The total number of logs in the current query results.
x-log-processed-rows	Integer	The number of rows processed in this calculation.
x-log-elapsed-millisecond	Integer	The time (in milliseconds) spent in this calculation.

Response elements

After the successful request, the response body contains the computing results. The response body of GetProjectLogs is an array, and each element in the array is a log. The element formats are as follows.

Name	Type	Description
__time__	Integer	The log timestamp (the number of seconds since 1970-1-1 00:00:00 UTC).
__Source __	String	The log source, which is specified when logs are written.
[content]	Key-value pair	The original content of the log, which is organized in key-value pairs.

Detailed description

- The query of this API is a standard SQL query statement.
- Specify the project you want to query in the domain name of the request.
- Specify the Logstore you want to query in the FROM condition of the query statement. Logstore is equivalent to a table in SQL.
- You must specify the time range you want to query in the SQL query condition. The time range is specified by __date__ (timestamp type) or __time__ (integer type, the unit is in UNIX time).
- Each call to this API must return results within a specified time, and each query can only scan a specified number of logs. The results returned from this request are incomplete if the log volume to be processed for this request is large (whether the results are complete is indicated by using the x-log-progress in the response header). At the same time, Log Service caches the query results within 15 minutes. When part of the query request results matches those in the cache, the server continues to scan the log data that is not hit in the cache for this request. To reduce the workload of merging multiple query results, the query results of server cache hits and the new hits of the current query are merged and returned. Therefore, Log Service allows you to repeatedly call the API with the same parameters to eventually obtain the complete results. Log Service API cannot predict how many times the API must be called before obtaining the complete results API because the volume of the logs to be queried fluctuates dramatically. Therefore, you must check the x-log-progress status in the returned results of each request to determine whether to continue the query. You must note that each call to this API consumes the same number of query CUs.

Special error codes

In addition to the Common error codes of Log Service APIs, the API may also return the following special error codes.

HTTP status code	Error code	Error message	Description
400	ParameterInvalid	parameter is invalid	The error message returned when the request parameter is invalid. For more information, see the detailed error message.

Examples

Take a project named big-game in the region Hangzhou as an example. Query the logs whose topic is groupA in the app_log Logstore of the big-game project. The time interval for this query is 2014-09-01 00:00:00-2014-09-01 22:00:00. The keyword for this query is error. The query starts from the start the time interval, and up to 20 logs will be returned.

Sample requests

```
GET /logs/? query=SELECT * FROM <logStoreName> where __line__ = 'abc' and __date__ >'2017-09-01 00:0
0:00' and __date__ < '2017-09-02 00:00:00'&line=20&offset=0 HTTP/1.1
    Authorization: <AuthorizationString>
    Date: Wed, 3 Sept. 2014 08:33:46 GMT
    Host: big-game.cn-hangzhou.log.aliyuncs.com
    x-log-bodyrawsize: 0
    x-log-apiversion: 0.4.0
    x-log-signaturemethod: hmac-sha1
```

Sample responses

```
HTTP/1.1 200 OK
    Content-MD5: 36F9F7F0339BEAF571581AF1B0AAAFB5
    Content-Type: application/json
    Content-Length: 269
    Date: Wed, 3 Sept. 2014 08:33:47 GMT
    x-log-requestid: efag01234-12341-15432f
    x-log-progress : Complete
    x-log-count : 10000
    x-log-processed-rows: 10000
    x-log-elapsed-millisecond:5
    {
    "progress": "Complete",
    "count": 2,
    "logs": [
    {
    "__time__": 1409529660,
    "__source__": "10.237.0.17",
    "Key1": "error",
    "Key2": "Value2"
    },
    {
    "__time__": 1409529680,
    "__source__": "10.237.0.18",
    "Key3": "error",
    "Key4": "Value4"
    }
    ]
    }
```

In this sample response, the x-log-progress status is Complete, which indicates the log query is completed and the returned results are complete. For this request, two logs meet the query condition and are displayed as the values of logs. If the x-log-progress status is Incomplete in the response result, you must repeat the request to obtain the complete results.

2.15.1.12. Description of common resources

2.15.1.12.1. Data model

This topic describes commonly used terms in Log Service to help you better understand and use Log Service.

project

The basic unit of management in Log Service. A project is used to isolate and control resources. You can use a project to manage all the logs and related log sources of an application.

Logstore

The unit used in Log Service for data collection, storage, and consumption. Each Logstore belongs to a project, and each project can have multiple Logstores. You can create multiple Logstores for a project as needed. Typically, an independent Logstore is created for each type of logs of an application. For example, you have a game application named big-game, and it stores three types of logs on the server: operation_log, application_log, and access_log. You can create a project named big-game, and then create three Logstores in this project to collect, store, and consume these three types of logs, respectively.

log

The smallest unit of data that can be processed in Log Service. Log Service uses a semi-structured data model to define a log. The data model is as follows:

- **Topic**: The user-defined field used to mark a batch of logs. For example, access logs can be marked based on the sites. By default, this field is an empty string, which is also a valid topic.
- **Time**: The reserved field in a log used to indicate the time when a log is generated (the number of seconds that have elapsed since 00:00:00 Thursday, January 1, 1970 UTC). Typically, this field is generated based on the time in the log.
- **Content**: The field used to record the detailed content of a log. The content consists of one or more content items. Each content item is a key-value pair.
- **Source**: The field used to indicate the source of a log. For example, the IP address of the machine where a log is generated. This field is empty by default.

Log Service has different requirements for the values of different fields, as described in Log fields.

Log fields

Field	Requirement
time	An integer in the UNIX timestamp format, in seconds.
topic	A UTF-8 encoded string that is up to 128 bytes in length.
source	A UTF-8 encoded string that is up to 128 bytes in length.
content	One or more key-value pairs. A key is a UTF-8 encoded string that is up to 128 bytes in length. It can contain only letters, underscores (_), and digits. It cannot start with a digit. A value is a UTF-8 encoded string that is up to 1024 × 1024 bytes in length.

Note The key in the content cannot use any of the following keywords: `__time__`, `__source__`, `__topic__`, `__partition_time__`, `_extract_others_`, and `__extract_others__`.

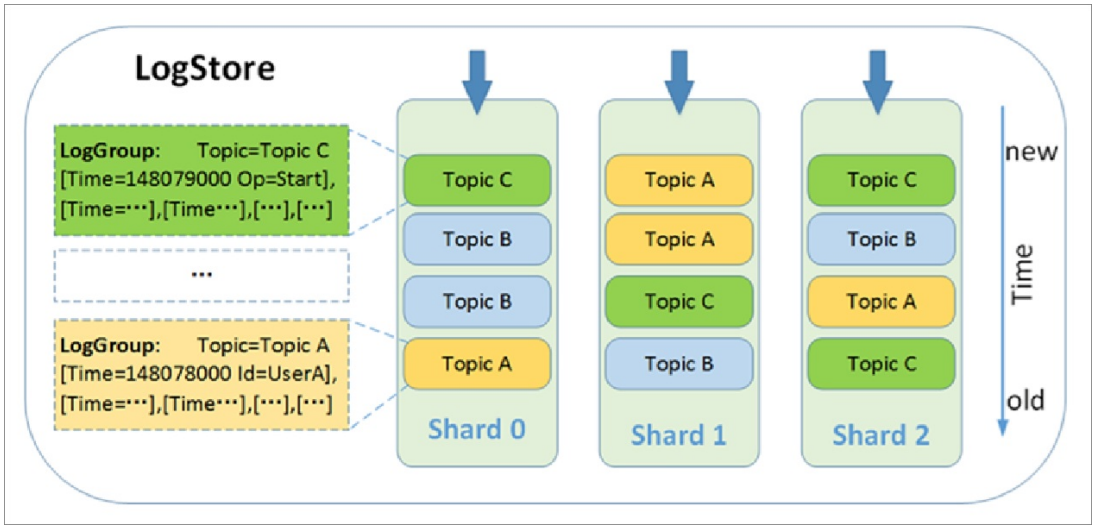
topic

A topic is used to classify logs in a Logstore. Topics can be specified when you write logs. For example, you can use your ID as the log topic when writing logs. If you do not need to classify logs in a Logstore, use the same topic for all logs.

> **Note** An empty string is a valid log topic and is the default log topic.

The relationship among Logstores, log topics, and logs shows the relationship among Logstores, log topics, and logs.

The relationship among Logstores, log topics, and logs



Various log formats are used in actual scenarios. The following example shows you how to map an original NGINX access log to the log data model of Log Service. Assume that the IP address of your NGINX server is 10.10.10.1. A raw log on this server is as follows:

```
10.1.1.1 - - [01/Mar/2012:16:12:07 +0800] "GET /Send? AccessKeyId=<yourAccessKeyId> HTTP/1.1" 200 5 "-
" "Mozilla/5.0 (X11; Linux i686 on x86_64; rv:10.0.2) Gecko/20100101 Firefox/10.0.2"
```

Log data model of Log Service shows how to map the raw log to the log data model of Log Service.

Log data model of Log Service

Field	Content	Description
topic	“”	The default value (empty string) is used.
time	1330589527	The precise time when the log is generated (in seconds), which is converted from the timestamp of the raw log.
source	“10.10.10.1”	The IP address of the server is used as the log source.
content	Key-value pair	The specific content of a log.

You can decide how to extract the raw log content and combine the extracted content into key-value pairs, as described in Custom key-value pairs.

Custom key-value pairs

Key	Value
ip	10.1.1.1
method	GET
status	200
length	5
ref_url	-
browser	Mozilla/5.0 (X11; Linux i686 on x86_64; rv:10.0.2) Gecko/20100101 Firef

Logs

A collection of log entries.

LogGroup

A collection of logs.

LogGroupList

A collection of log groups used to return the results.

Encoding method

As described in Supported encoding method, the system supports the following content encoding method and allows future extensions. The RESTful API layer is indicated by Content-Type.

Supported encoding method

Definition	Content-Type	Example
Protocol buffers	The data model is encoded by protocol buffers.	application/x-protobuf

Protocol buffers are used to define the objects in the data model as follows:

```
message Log
{
   required uint32 Time = 1;// UNIX Time Format
   message Content
   {
      required string Key = 1;
      required string Value = 2;
   }
   repeated Content Contents= 2;
}
message LogGroup
{
   repeated Log Logs= 1;
   optional string Reserved = 2; // reserved fields
   optional string Topic = 3;
   optional string Source = 4;
}
message LogGroupList
{
   repeated LogGroup logGroupList = 1;
}
```

Note Protocol buffers do not require the key-value pair to be unique. However, you cannot use the same key. Otherwise, the behavior is undefined.

2.15.1.12.2. Data encoding methods

Protocol Buffer is a structured data interchange format developed by Google. It is widely used in both internal and external Google services. Currently, Log Service uses Protocol Buffer format as the standard log writing format. You must serialize the original log data into Protocol Buffer data streams before writing logs to Log Service by using APIs.

```
message Log
{
   required uint32 time = 1; // UNIX Time Format
   message Content
   {
      required string key = 1;
      required string value = 2;
   }
   Repeated content contents = 2;
}
message LogGroup
{
   repeated Log logs= 1;
   optional string reserved =2; // Internal field, which does not need to be specified
   optional string topic = 3;
   optional string source = 4;
}
message LogGroupList
{
   repeated LogGroup logGroupList = 1;
}
```

Note

- PB does not require the key-value pair to be unique. You must avoid such situation. Otherwise, the behavior is undefined.
- For more information about Protocol Buffer format, see Github.
- For more information about the API for writing logs to Log Service, see PostLogStoreLogs.

2.15.1.12.3. Logstores

A data storage unit is referred to as a Logstore. By default, you can create up to 10 Logstores for each project. A Logstore name is unique in a project. A Logstore is the portal for all log data. You can read from or write to the Logstore.

The Logstore naming rules are as follows:

- The name contains only lowercase letters, numbers, hyphens (-), and underscores (_).
- The name must begin and end with a lowercase letter or number.
- The name must be 2 to 63 bytes in length.

Example of the complete resource:

```
{
    “logstoreName" : "access_log",
   "ttl": 1,
   "shardCount": 2,
   "createTime":1439538649,
   "lastModifyTime":1439538649
}
```

The meaning of each parameter is described in Parameter description.

Parameter description

Parameter	Type	Required	Description
logstoreName	String	Yes	The Logstore name, which must be unique in the same project.
TTL	Integer	Yes	The Time to Live (TTL) of log data. The unit is in days and the minimum value is 1 day.
shardCount	Integer	Yes	The log data service unit.
createTime (OutputOnly)	Integer	No	The time when the resource is created in Log Service (output only).
lastModifyTime (OutputOnly)	Integer	No	The time when the resource is updated in Log Service (output only).

2.15.1.12.4. Shard

A shard is a basic read and write unit in each Logstore. You can specify the number of shards in each Logstore. Each shard has certain service capabilities:

- Writing: 5 MBit/s, 2000 times/s
- Read: 10 MBit/s, 100 times/s

To read data from a shard, you must specify the corresponding shard. To write data to a shard, you can use Server Load Balancer. By using Server Load Balancer, data is automatically written to shards based on the system load in the backend, which guarantees the high availability of log writing.

The example of the complete resource is described in Example of the complete resource.

Example of the complete resource

Parameter	Type	Required	Description

Parameter	Type	Required	Description
shardID	Integer	Yes	The unique ID of a shard in the Logstore, which is automatically generated by the system.

2.15.1.12.5. Logtail configuration

You can create up to 100 Logtail configurations for a project. The configuration name is unique under a project.

You can use the configuration to specify the location, method, and parameters for log collection.

The configuration naming rules are as follows:

- The name can only contain lowercase letters, numbers, hyphens (-), and underscores (_).
- The name must begin and end with a lowercase letter or number.
- The name must be 2 to 128 characters in length.

Example of the complete resource:

```
{
   "configName": "testcategory1",
   "inputType": "file",
   "inputDetail": {
      "logType": "common_reg_log",
      "logPath": "/var/log/httpd/",
      "filePattern": "access.log",
      "localStorage": true,
      "timeFormat": "%Y/%m/%d %H:%M:%S",
      "logBeginRegex": ".*",
      "regex": "(\w+)(\s+)",
      "key" :[ “key1”,  “key2"],
      "filterKey":["key1"],
      "filterRegex":[ “regex1"],
      "topicFormat":  “none"
   },
   "outputType": "sls",
   "outputDetail":
   {
      "logstoreName": "perfcounter"
   },
   "createTime": 1400123456,
   "lastModifyTime": 1400123456
}
```

The configuration parameters and descriptions are described in Configuration.

Configuration

Attribute name	Type	Required	Description
configName	String	Yes	The log configuration name, which is unique in the same project.
inputType	String	Yes	The input type. The default type is file.
inputDetail	JSON	Yes	See the following table.
outputType	String	Yes	The output type. Currently, only LogService is supported.
outputDetail	String	Yes	See the following table.
createTime(output-only)	Integer	No	The creation time of the configuration.
lastModifyTime(output-only)	Integer	No	The time when the resource is updated on the server.

The inputDetail types and descriptions are described in inputDetail.

inputDetail

Attribute name	Type	Required	Description
logType	String	Yes	The log type. Currently, only common_reg_log is supported.
logPath	String	Yes	The parent directory where the log is located, for example, `/var/logs/`.
filePattern	String	Yes	The pattern of a log file, for example, `access*.log`.
localStorage	Boolean	Yes	Indicates whether to activate the local cache. Logs of 1 GB can be locally cached when the link to Log Service is disconnected.
timeFormat	String	Yes	The format of log time, for example, `%Y/%m/%d %H:%M:%S`.

Attribute name	Type	Required	Description
logBeginRegex	String	Yes	The characteristics (regular expression) of the first log line, which is used to match with logs that are composed of multiple lines.
regex	String	Yes	The regular expression for extracting logs.
key	Array	Yes	The key that is generated after logs are extracted.
filterKey	Array	Yes	The key for filtering logs. The log meets the requirements only when the key value matches the regular expression specified in the corresponding filterRegex column.
filterRegex	Array	Yes	The regular expression corresponding to each filterKey. The length of filterRegex must be the same as that of filterKey.
topicFormat	String	No	Uses part of the log file path as the topic, for example, `/var/log/(.*).log`. The default value is none, which indicates that the topic is empty.
preserve	Boolean	No	true indicates that the monitored directory never times out. false indicates that the timeout for monitored directory is 30 minutes. The default value is true.
preserveDepth	Integer	No	If preserve is set to false, specify the depth of the directories without monitoring timeout. The maximum depth is 3.

The outputDetail types and their descriptions are described in outputDetail.

outputDetail

Attribute name	Type	Required	Description
logstoreName	String	Yes	The Logstore name.

2.15.1.12.6. Logtail machine group

After a machine with Logtail installed is started normally, the machine is automatically associated with the current user based on the user information in the Logtail configuration. Currently, the machine can be identified in the following three ways:

- IP: The IP address corresponding to the hostname. This is the easiest way to understand, but the IP address may be duplicated in environments such as Virtual Private Cloud (VPC).
- UUID (machine-uniqueid): The UUID in DMI devices. For more information, see RFC 4122.
- Userdefined-id: You can customize the machine identifier in the Logtail directory.

Attributes of each machine are as follows:

```
{
   "ip" : "testip1",
   "machine-uniqueid" : "testuuid1",
   "userdefined-id" : "testuserdefinedid1",
   "lastHeartbeatTime”  :1397781420
}
```

The machine attributes are described in Parameter description.

Parameter description

Parameter	Type	Description
ip	String	The IP address corresponding to the machine hostname.
uuid	String	The unique primary key marked by the machine, uploaded by Logtail.
userdefined-id	String	The user-defined machine identification, uploaded by Logtail.
lastHeartbeatTime(output-only)	Integer	The last heartbeat time of the machine (the number of seconds since the epoch time).

machinegroup

Machinegroup is the machine group that belongs to the current user in the project. The machine group can be identified in two ways (IP address and user-defined). The IP address is more easily identified while the user-defined identifier can solve the problem of identical IP addresses in the VPC environment. You can select either of the two machine identification methods.

Machine group naming rules:

- The name contains only lowercase letters, numbers, hyphens (-), and underscores (_).
- The name must begin and end with a lowercase letter or number.
- The name must be 2 to 128 characters in length.

Example of the complete resource:

```
{
  "groupName" : "testgroup",
  "groupType" : "",
  "groupAttribute" : {
    "externalName" : "testgroup",
     “groupTopic” :  “testgrouptopic”
  },
   “machineIdentifyType” : "ip",
  "machineList" : [
    "ip1",
    "ip2"
    ...
  ],
   “createTime” : 1431705075,
  "lastModifyTime" : 1431705075
}
```

The machinegroup parameter is described in Parameter description.

Parameter description

Attribute name	Type	Required	Description
groupName	String	Yes	The machine group name, which is unique in the same project.
groupType	String	No	The machine group type, which is empty by default.
machineIdentifyType	String	Yes	The machine identification type, which can be IP address or user-defined identifier.
groupAttribute	Object	Yes	The machine group attribute, which is empty by default.
machineList	Array	Yes	The specific machine identifier, which can be an IP address or user-defined identifier.

Attribute name	Type	Required	Description
createTime(output-only)	Integer	No	The resource creation time.
lastModifyTime(output-only)	Integer	No	The time when the resource is updated on the server.

The groupAttribute types and descriptions are described in groupAttribute description.

groupAttribute description

Attribute name	Type	Required	Description
groupTopic	String	No	The topic of a machine group, which is empty by default.
externalName	String	No	The external identification that the machine group depends on, which is empty by default.

2.15.2. SDK reference

2.15.2.1. Introduction

2.15.2.1.1. Overview

To facilitate the use of Log Service., Log Service provides software development kits (SDKs) in multiple programming languages (Java, .NET, Python, PHP, and C). Select to use an appropriate version as per your needs.

Log Service SDKs are implemented based on Log Service APIs and provide the same capabilities as Log Service APIs. For more information about Log Service APIs, see API references.

Similar to using Log Service APIs, you must have an active Alibaba Cloud AccessKey (consisting of an AccessKey ID and AccessKey Secret).

To use the Log Service SDK, you need to understand the endpoint of Log Service. For more information about how to specify the root endpoint in an SDK, see SDK configurations.

Though the implementation details of Log Service SDKs vary with different languages, the SDKs can be considered as Log Service APIs encapsulated in different languages and basically implement the similar functions as follows.

- Log Service APIs are uniformly encapsulated, removing the need for constructing specific API requests and parsing responses. The APIs in different languages are similar, facilitating the switchover between different languages.
- The digital signature logic is implemented for Log Service APIs, greatly simplifying the use of APIs and removing the need for understanding the details of the API signature logic.
- The logs collected to Log Service are encapsulated in ProtoBuffer format, allowing you to write logs without a deep understanding of the ProtoBuffer format.
- Implementation of the compression method defined in the Log Service APIs removes the need to

focus on the compression details. SDKs in some languages allow you to specify whether to write logs in the compression mode. The compression mode is used by default.

- Unified error handling method is provided, allowing you to handle request exceptions in the method that languages are familiar with.
- Currently, SDKs in all languages only support synchronous requests.

SDK-related documents and source code describes the download addresses, usage instructions, and complete programming references for the SDKs of different languages.

SDK-related documents and source code

SDK language	Related document
Java	Java SDK
.NET	.NET SDK
PHP	PHP SDK
Python	Python SDK
C	C SDK
GO	GO SDK
iOS	iOS SDK
Android	Android SDK

2.15.2.1.2. SDK configurations

You must specify the basic configurations before you use SDKs to interact with Log Service, just as you use APIs to interact with Log Service. All SDKs provided by Alibaba Cloud define a Client class, which serves as the entry point for constructing client instances. The basic configurations are specified when the client instances are constructed.

The following basic configurations are used:

- Endpoint: You must determine the endpoint that is used by the client to access Log Service.
- An AccessKey pair that consists of an AccessKey ID and an AccessKey Secret: You must specify the AccessKey pair that is used by the client to access Log Service.

The following sections describe how to use both configurations:

Endpoint

When you use the SDK, you must first determine the access method and endpoint.

1. When you select an endpoint for a client instance, make sure that the region where your project is located is the same as the region of your endpoint. Otherwise, you cannot use the SDK to access your project.
2. All API endpoints support only HTTP.

AccessKey pair

As described in the "AccessKey pair" section of the API reference document, all requests that interact with Log Service must be authenticated. An AccessKey pair is used to authenticate the requests. An AccessKey pair consists of an AccessKey ID and an AccessKey Secret. When you create a client instance, you must specify both an AccessKey ID and an AccessKey Secret. You must obtain an AccessKey pair in the Apsara Stack console.

> Note
>
> - An Apsara Stack account can have multiple AccessKey pairs. You must specify the AccessKey ID and AccessKey Secret of the same AccessKey pair when you create a client instance. Otherwise, authentication fails.
> - You must enable the AccessKey pair used to create the client instance. Otherwise, requests are rejected by the server. You can also log on to the Apsara Stack console to view the status of the AccessKey pair.

Examples

Assume that you want to access a project, and have an AccessKey pair that is enabled. The following AccessKey pair is used:

```
AccessKeyId = "<yourAccessKeyId>"
AccessKeySecret = "<yourAccessKeySecret>"
```

The following code snippets show you how to create a client instance:

Java:

```
String endpoint = "regionid.example.com"; // During actual usage, specify the endpoint based on your re
gion and access method.
String accessKeyId = "<youraccessKeyId>"; // Specify your AccessKey ID.
String accessKeySecret = "<youraccessKeySecret>"; // Specify your AccessKey Secret.
Client client = new Client(endpoint, accessKeyId, acccessKeySecret);
//use client to operate log service project.....
```

.NET(C#):

```
String endpoint = "regionid.example.com"; // During actual usage, specify the endpoint based on your re
gion and access method.
String accessKeyId = "<youraccessKeyId>"; // Specify your AccessKey ID.
String accessKeySecret = "<youraccessKeySecret>"; // Specify your AccessKey Secret.
SLSClient client = new SLSClient(endpoint, accessKeyId, accessKeySecret);
//use client to operate sls project.....
```

PHP:

```
$endpoint = 'regionid.example.com'; // The Hangzhou region is used in this example. During actual usag
e, specify the endpoint based on your region and access method.
$accessKeyId = '<youraccessKeyId>'; // Specify your AccessKey ID.
$accessKey = '<youraccessKey>'; // Specify your AccessKey Secret.
$client = new Aliyun_Sls_Client($endpoint, $accessKeyId, $accessKey);
//use client to operate sls project.....
```

Python:

```
# // During actual usage, specify the endpoint based on your region and access method.
endpoint = 'regionid.example.com'
# Specify your AccessKey ID.
accessKeyId = '<youraccessKeyId>'
# Specify your AccessKey Secret.
accessKey = '<youraccessKey>'
client = LogClient(endpoint, accessKeyId, accessKey)
#use client to operate log project.....
```

2.15.2.1.3. Troubleshooting

The possible SDK errors can be classified into the following types:

- Errors returned by the server. This type of errors are returned by the server and handled by SDKs. For more information about this type of errors, see the common error codes of Log Service APIs and the description of each API.
- Network errors that occur when you send requests to the server by using SDKs. This type of errors include network disconnection and server response timeout.
- Errors that are generated by SDKs and related to platforms or programming languages, for example, memory overflows.

All SDKs provided by Alibaba Cloud handle errors by throwing exceptions based on the following principles:

- The first and second types of errors are encapsulated as the LogException class and thrown to users by SDKs.
- The third type of errors are not handled by SDKs, but are thrown to users as the platform- or language-specific native exception class.

LogException

The LogException class is defined by SDKs to handle the logical errors of Log Service. It inherits the base class for all exceptions from each programming language, and provides the following exception information:

- Error code: indicates the error type. Errors returned by the server share the same error codes as the APIs. The error code for network errors that occur when you send requests by using SDKs is RequestError. For more information about error codes, see the API reference for the programming language that is relevant to your case.
- Error message: indicates the message that is returned together with an error. Errors returned by

the server share the same error messages as that returned by APIs. The error message for network errors that occur when you send requests by using SDKs is "request is failed". For more information about error messages, see the API reference for the programming language that is relevant to your case.

- Request ID: indicates the server request ID that corresponds to the current error. This ID is returned only when the error message is returned by the server. Otherwise, an empty string is returned. You can provide the request ID to the Log Service team to track and locate the error.

Failed requests and retries

When you use SDKs to access Log Service, the request may fail due to temporary network disconnection, transmission delay, and slow server response. These errors are thrown as exceptions. Log Service does not implement any retry logic. Therefore, you must define custom processing logic such as retrying failed requests or reporting errors to handle such exceptions.

Examples

You want to access a project named **big-game**, and retry the request for a specified number of times if network exceptions occur. The following code snippets can be used:

Java:

```
// Other code...
String accessId = "<youraccessId>"; // Specify your AccessKey ID.
String accessKey = "<youraccessKey>"; // Specify your AccessKey Secret.
String project = "big-game";
String endpoint = "regionid.example.com";
int max_retries = 3;
/*
 * Create a client instance.
 */
Client client = new Client(accessId, accessKey, endpoint);
ListLogStoresRequest lsRequest = new ListLogStoresRequest(project);
for (int i = 0; i < max_retries; i++)
{
   try
   {
      ListLogStoresResponse res = client.ListLogStores(lsRequest)
      // Process the returned data...
      break;
   }
   catch(LogException ex)
   {
      if (e.GetErrorCode() == "RequestError")
      {
         if ( i == max_retries - 1)
         {
```

```
            System.out.println("request is still failed after all retries.");
            break;
        }
        else
            System.out.println("request error happens, retry it!") ;
    }
    else
    {
        System.out.println("error code :" + e.GetErrorCode());
        System.out.println("error message :" + e.GetErrorMessage());
        System.out.println("error requestId :" + e.GetRequestId());
        break;
    }
  }
  catch(...)
  {
    System.out.println("unrecoverable exception when listing logstores.");
    break;
  }
}
// Other code...
```

.NET (C#):

```
// Other code...
String accessId = "your_access_id"; // Specify your AccessKey ID.
String accessKey = "your_access_key"; // Specify your AccessKey Secret.
String project = "big-game";
String endpoint = "regionid.example.com";
int max_retries = 3;
// Create a client instance.
SLSClient client = new SLSClient(endpoint, accessId, accessKey);
ListLogstoresRequest request = new ListLogstoresRequest();
request.Project = project;
for (int i = 0; i < max_retries; i++)
{
  try
  {
    ListLogstoresResponse response = client.ListLogstores(request);
    // Process the returned data...
    break;
  }
```

```
    catch(LogException ex)
    {
        if (e.errorCode == "SLSRequestError")
        {
            if ( i == max_retries - 1)
            {
                Console.Writeline( “request is still failed after all retries.” );
                break;
            }
            else
            {
                Console.Writeline("request error happens, retry it!") ;
            }
        }
        else
        {
            Console.Writeline("error code :" + e.errorCode;
            Console.Writeline("error message :" + e.Message;
            Console.Writeline("error requestId :" + e.RequestId;
            break;
        }
    }
    catch(...)
    {
        Console.Writeline("unrecoverable exception when listing logstores.");
        break;
    }
}
// Other code...
```

PHP:

```
<? php
// Other code...
$endpoint = 'regionid.example.com';
$accessId = 'your_access_id'; // Specify your AccessKey ID.
$accessKey = 'your_access_key'; // Specify your AccessKey Secret.
$maxRetries = 3;
// Create an SLS client.
$client = new Aliyun_Sls_Client($endpoint, $accessId, $accessKey);
$project = 'big-game';
$request = new Aliyun_Sls_Models_ListLogstoresRequest($project);
```

```
for($i = 0; $i < $maxRetries; ++$i)
{
    try
    {
        $response = $client->ListLogstores($request);
        // Process the returned data...
        break;
    }
    catch (Aliyun_Sls_Exception $e)
    {
        if ($e->getErrorCode()=='RequestError')
        {
            if ($i+1 == $maxRetries)
            {
                echo "error code :" . $e->getErrorCode() . PHP_EOL;
                echo "error message :" . $e->getErrorMessage() .  PHP_EOL;
                break;
            }
            echo 'request error happens, retry it!' . PHP_EOL;
        }
        else
        {
            echo "error code :" . $e->getErrorCode() .  PHP_EOL;
            echo "error message :" . $e->getErrorMessage() .  PHP_EOL;
            echo "error requestId :" . $e->getRequestId() . PHP_EOL;
            break;
        }
    }
    catch (Exception $ex)
    {
        echo 'unrecoverable exception when listing logstores.' . PHP_EOL;
        var_dump($ex);
        break;
    }
}
// Other code...
```

Python:

```
// Other code...
endpoint = 'regionid.example.com'
accessId = 'your_access_id' # Specify your AccessKey ID.
accessKey = 'your_access_key' # Specify your AccessKey Secret.
maxRetries = 3
# Create a client instance.
client = Client(endpoint, accessId, accessKey)
project = 'big-game'
lsRequest = ListLogstoresRequest(project)
for i in xrange(maxRetries):
    try:
        res = client.ListLogstores(lsRequest)
        # Process the returned data...
        break
    except LogException as e:
        if e.getErrorCode() == "RequestError":
            if i+1 == maxRetries:
                print "error code :" + e.getErrorCode()
                print "error message :" + e.getErrorMessage()
                break
            else:
                print "request error happens, retry it!"
        else:
            print "error code :" + e.getErrorCode()
            print "error message :" + e.getErrorMessage()
            print "error requestId :" + e.getRequestId()
            break
    except Exception as e:
        print 'unrecoverable exception when listing logstores.'
        break
// Other code...
```

2.15.2.1.4. API specifications

SDKs of different programming languages have different implementations. However, all APIs comply with the request-response principle. You can call these APIs by using the following methods:

1. Create a request instance by using request parameters.
2. Call the corresponding API in the SDK and pass in the request instance.
3. The results from the API call are returned in the form of a response instance.

The following code snippets explain how to obtain the names of all the Logstores in a project:

Java

```
// Other code...
String accessId = "<youraccessId>"; // Specify your AccessKey ID.
String accessKey = "<youraccessKey>"; // Specify your AccessKey Secret.
String project = "your_project"; // Specify your project name.
String endpoint = "region_endpoint"; // The Hangzhou region is used in this example. During actual usag
e, specify the endpoint based on your region and access method.
// Create a client instance.
Client client = new Client(endpoint, accessId, accessKey);
// Specify the project request parameter to initialize the ListLogstores request class.
ListLogStoresRequest lsRequest = new ListLogStoresRequest(project);
// Use the request instance to call the ListLogstores API. The response parameter is the corresponding
response instance.
ListLogStoresResponse res = client.ListLogStores(lsRequest);
// Access the response instance to retrieve the request results.
ArrayList<String> names = res.GetLogStores();
// Other code...
```

.NET(C#)

```
// Other code...
String accessId = "<youraccessId>"; // Specify your AccessKey ID.
String accessKey = "<youraccessKey>"; // Specify your AccessKey Secret.
String project = "your_project"; // Specify your project name.
String endpoint = "region_endpoint"; // The Hangzhou region is used in this example. During actual usag
e, specify the endpoint based on your region and access method.
// Create a client instance.
SLSClient client = new SLSClient(endpoint, accessId, accessKey);
// Specify the project request parameter to initialize the ListLogstores request class.
ListLogStoresRequest lsRequest = new ListLogStoresRequest();
lsRequest.Project = project;
// Use the request instance to call the ListLogstores API. The response parameter is the corresponding
response instance.
ListLogStoresResponse res = client.ListLogStores(lsRequest);
// Access the response instance to retrieve the request results.
List<String> names = res.Logstores;
// Other code...
```

PHP

```
// Other code...
$accessId = "<youraccessId>"; // Specify your AccessKey ID.
$accessKey = "<youraccessKey>"; // Specify your AccessKey Secret.
$project = "your_project"; // Specify your project name.
$endpoint = "region_endpoint"; // The Hangzhou region is used in this example. During actual usage, sp
ecify the endpoint based on your region and access method.
// Create an SLS client instance.
$client = new Aliyun_Sls_Client($endpoint, $accessId, $accessKey);
// Specify the project request parameter to initialize the ListLogstores request class.
$request = new Aliyun_Sls_Models_ListLogstoresRequest($project);
// Use the request instance to call the ListLogstores API. The response parameter is the corresponding
response instance.
$response = $client->listLogstores($request);
// Access the response instance to retrieve the request results.
$names = $response->getLogstores();
// Other code...
```

Python

```
// Other code...
accessId = '<youraccessId>'; // Specify your AccessKey ID.
accessKey = '<youraccessKey>'; // Specify your AccessKey Secret.
project = 'your_project'; // Specify your project name.
endpoint = 'region_endpoint'; // The Hangzhou region is used in this example. During actual usage, spec
ify the endpoint based on your region and access method.
# Create a client instance.
client = LogClient(endpoint, accessId, accessKey)
# Specify the project request parameter to initialize the ListLogstores request class.
lsRequest = ListLogstoresRequest(project)
# Use the request instance to call the ListLogstores API. The response parameter is the corresponding r
esponse instance.
res = client.list_logstores(lsRequest)
# Access the response instance to retrieve the request results.
names = res.get_logstores();
// Other code...
```

SDKs implement multiple sets of APIs similar to ListLogstores. SDKs also define the corresponding request and response classes. In addition to the basic request-response APIs, SDKs of different programming languages provide auxiliary APIs that encapsulate these basic APIs. This eliminates the need to create requests and parse the final responses on your own. For more information about the auxiliary APIs, see the API reference of each SDK.

2.15.2.2. Java SDK

This is a quick start guide for the Log Service Java SDK.

Download URL

The Log Service Java SDK provides a suite of development tools to help simplify the use of Log Service. You can choose to download the SDK or configure the SDK as a Maven dependency. The SDK supports Java SE 6.0 and later. Click here to download the latest SDK.

Step 1 Create an account

You must create an account to access Log Service.

Step 2 Obtain an AccessKey pair

You must request an AccessKey pair to use the Log Service Java SDK.

Log on to the Apsara Stack console. Select an AccessKey pair for the SDK.

The AccessKey pair is used in the following steps. It must be kept confidential. For more information about how to use the AccessKey pair, see SDK Configurations.

Step 3 Create a project and a Logstore

Use the Log Service Java SDK to create a project and a Logstore.

> Note
>
> - Make sure that you use the same account to obtain an AccessKey pair and create a project and a Logstore.
> - Names of each project must be unique within Log Service. Names of each Logstore must be unique within a project.
> - After a project is created, the region to which it belongs cannot be changed. A project cannot be migrated between different regions.

Step 4 Configure the Java development environment

The Log Service Java SDK supports Java SE 6.0 and later. You can download the SDK from the official Java website and set up the Java development environment as instructed.

Step 5 Install the Log Service Java SDK

You must install the Log Service Java SDK after setting up the Java development environment. You can install the Log Service Java SDK by using the following two methods:

We recommend that you use Apache Maven to obtain the latest SDK. You can add the following configurations to your Maven project:

```
<dependency>
      <groupId>com.google.protobuf</groupId>
      <artifactId>protobuf-java</artifactId>
      <version>2.5.0</version>
</dependency>
<dependency>
<groupId>com.aliyun.openservices</groupId>
<artifactId>aliyun-log</artifactId>
<version>0.6.7</version>
<exclusions>
     <exclusion>
        <groupId>com.google.protobuf</groupId>
        <artifactId>protobuf-java</artifactId>
    </exclusion>
</exclusions>
</dependency>
```

You can also download the Java SDK and reference the local package in your Java project.

1. Download the Java SDK. The Java SDK is updated periodically. Use Maven to obtain the latest version.
2. Extract the downloaded SDK into a directory. The Java SDK does not require additional installation steps.
3. Add all .jar packages including third-party dependencies in the SDK to your Java project. For more information, see IDE documents.

Step 6 Start a new Java project

To interact with Log Service and obtain the output, you can run the following code in any text editor or Java IDE:

```
package sdksample;
import java.util.ArrayList;
import java.util.List;
import java.util.Vector;
import java.util.Date;
import com.aliyun.openservices.log.Client;
import com.aliyun.openservices.log.common.*;
import com.aliyun.openservices.log.exception.*;
import com.aliyun.openservices.log.request.*;
import com.aliyun.openservices.log.response.*;
import com.aliyun.openservices.log.common.LogGroupData;
import com.aliyun.openservices.log.common.LogItem;
import com.aliyun.openservices.log.common.Logs.Log;
```

```
import com.aliyun.openservices.log.common.Logs.Log.Content;
import com.aliyun.openservices.log.common.Logs.LogGroup;
import com.aliyun.openservices.log.common.Consts.CursorMode;
public class sdksample {
    public static void main(String args[]) throws LogException, InterruptedException {
        String endpoint = "<log_service_endpoint>"; // Select the endpoint that matches the region of the p
roject created in the preceding step.
        // Endpoint
        String accessKeyId = "<youraccessKeyId>"; // Specify your AccessKey ID.
        String accessKeySecret = "<youraccessKeySecret>"; // Specify your AccessKey Secret.
        // AccessKeySecret
        String project = "<project_name>"; // The name of the project created in the preceding step.
        String logstore = "<logstore_name>"; // The name of the Logstore created in the preceding step.
        // Create a client instance.
        Client client = new Client(endpoint, accessKeyId, accessKeySecret);
        // List the names of all Logstores in the current project.
        int offset = 0;
        int size = 100;
        String logStoreSubName = "";
        ListLogStoresRequest req1 = new ListLogStoresRequest(project, offset, size, logStoreSubName);
        ArrayList<String> logStores = client.ListLogStores(req1).GetLogStores();
        System.out.println("ListLogs:" + logStores.toString() + "\n");
        // Write logs.
        String topic = "";
        String source = "";
        // Send 10 packets continuously, with each packet containing 10 log entries.
        for (int i = 0; i < 10; i++) {
            Vector<LogItem> logGroup = new Vector<LogItem>();
            for (int j = 0; j < 10; j++) {
                LogItem logItem = new LogItem((int) (new Date().getTime() / 1000));
                logItem.PushBack("index"+String.valueOf(j), String.valueOf(i * 10 + j));
                logGroup.add(logItem);
            }
            PutLogsRequest req2 = new PutLogsRequest(project, logstore, topic, source, logGroup);
            client.PutLogs(req2);
            /*
             * You can specify the shard to which data is sent by setting the shard hash key.
             * Data is written to the shard whose range contains the hash key. For more information about th
e API, see public PutLogsResponse.
             * PutLogs( String project, String logStore, String topic,
             * List<LogItem> logItems, String source, String shardHash //
             * Write data to the shard based on the hash key, which can be MD5(ip) or MD5(id).
```

```
            */
        }
        // Read all the data written to Shard 0 in the last minute.
        int shard_id = 0;
        long curTimeInSec = System.currentTimeMillis() / 1000;
        GetCursorResponse cursorRes = client.GetCursor(project, logstore, shard_id, curTimeInSec - 60);
        String beginCursor = cursorRes.GetCursor();
        cursorRes = client.GetCursor(project, logstore, shard_id, CursorMode.END);
        String endCursor = cursorRes.GetCursor();
        String curCursor = beginCursor;
        while (curCursor.equals(endCursor) == false) {
            int loggroup_count = 2; // Read two log groups at a time.
            BatchGetLogResponse logDataRes = client.BatchGetLog(project, logstore, shard_id, loggroup_cou
nt, curCursor,
                    endCursor);
            // Read the list of log groups.
            List<LogGroupData> logGroups = logDataRes.GetLogGroups();
            for(LogGroupData logGroup: logGroups){
                FastLogGroup flg = logGroup.GetFastLogGroup();
                System.out.println(String.format("\tcategory\t:\t%s\n\tsource\t:\t%s\n\ttopic\t:\t%s\n\tmach
ineUUID\t:\t%s",
                        flg.getCategory(), flg.getSource(), flg.getTopic(), flg.getMachineUUID()));
                System.out.println("Tags");
                for (int tagIdx = 0; tagIdx < flg.getLogTagsCount(); ++tagIdx) {
                    FastLogTag logtag = flg.getLogTags(tagIdx);
                    System.out.println(String.format("\t%s\t:\t%s", logtag.getKey(), logtag.getValue()));
                }
                for (int lIdx = 0; lIdx < flg.getLogsCount(); ++lIdx) {
                    FastLog log = flg.getLogs(lIdx);
                    System.out.println("--------\nLog: " + lIdx + ", time: " + log.getTime() + ", GetContentCount: " +
log.getContentsCount());
                    for (int cIdx = 0; cIdx < log.getContentsCount(); ++cIdx) {
                        FastLogContent content = log.getContents(cIdx);
                        System.out.println(content.getKey() + "\t:\t" + content.getValue());
                    }
                }
            }
            String next_cursor = logDataRes.GetNextCursor();
            System.out.println("The Next cursor:" + next_cursor);
            curCursor = next_cursor;
        }
```

```
        // ! ! ! Note: You must enable the index feature before calling the following APIs.
        // Wait one minute before querying logs.
        try {
            Thread.sleep(60 * 1000);
        } catch (InterruptedException e) {
            e.printStackTrace();
        }
        // Query the distribution of logs.
        String query = "<Specify the query keywords here. To query all the contents, leave this field empty.
>";
        int from = (int) (new Date().getTime() / 1000 - 300);
        int to = (int) (new Date().getTime() / 1000);
        GetHistogramsResponse res3 = null;
        while (true) {
            GetHistogramsRequest req3 = new GetHistogramsRequest(project, logstore, topic, query, from, to
);
            res3 = client.GetHistograms(req3);
            if (res3 ! = null && res3.IsCompleted()) // IsCompleted()
            // If true is returned, query results are accurate.
            // If false is returned, queries are performed repeatedly.
            {
                break;
            }
            Thread.sleep(200);
        }
        System.out.println("Total count of logs is " + res3.GetTotalCount());
        for (Histogram ht : res3.GetHistograms()) {
            System.out.printf("from %d, to %d, count %d.\n", ht.GetFrom(), ht.GetTo(), ht.GetCount());
        }
        // Query log data.
        long total_log_lines = res3.GetTotalCount();
        int log_offset = 0;
        int log_line = 10;
        while (log_offset <= total_log_lines) {
            GetLogsResponse res4 = null;
            // Read 10 entries of logs at a time for each log offset. If a read operation fails, a maximum of thr
ee retries are allowed.
            for (int retry_time = 0; retry_time < 3; retry_time++) {
                GetLogsRequest req4 = new GetLogsRequest(project, logstore, from, to, topic, query, log_offse
t,
                        log_line, false);
```

```
            res4 = client.GetLogs(req4);
            if (res4 ! = null && res4.IsCompleted()) {
                break;
            }
            Thread.sleep(200);
        }
        System.out.println("Read log count:" + String.valueOf(res4.GetCount()));
        log_offset += log_line;
    }
    // Enable the analysis feature. You can use SQL features only after you have enabled the analysis f
eature. You can log on to the console or use the SDK to enable the analysis feature.
    IndexKeys indexKeys = new IndexKeys();
    ArrayList<String> tokens = new ArrayList<String>();
    tokens.add(",");
    tokens.add(".");
    tokens.add("#");
    IndexKey keyContent = new IndexKey(tokens,false,"text");
    indexKeys.AddKey("index0",keyContent);
    keyContent = new IndexKey(new ArrayList<String>(),false,"long");
    indexKeys.AddKey("index1",keyContent);
    keyContent = new IndexKey(new ArrayList<String>(),false,"double");
    indexKeys.AddKey("index2",keyContent);
    IndexLine indexLine = new IndexLine(new ArrayList<String>(),false);
    Index index = new Index(7,indexKeys,indexLine);
    CreateIndexRequest createIndexRequest = new CreateIndexRequest(project,logstore,index);
    client.CreateIndex(createIndexRequest);
    // Use the analysis feature.
    GetLogsRequest req4 = new GetLogsRequest(project, logstore, from, to, "", " index0:value | select a
vg(index1) as v1,sum(index2) as v2, index0 group by index0");
    GetLogsResponse res4 = client.GetLogs(req4);
    if(res4 ! = null && res4.IsCompleted()){
        for (QueriedLog log : res4.GetLogs()){
            LogItem item = log.GetLogItem();
            for(LogContent content : item.GetLogContents()){
                System.out.print(content.GetKey()+":"+content.GetValue());
            }
            System.out.println();
        }
    }
  }
}
```

Precautions

- If you improve the I/O performance of your system, do not use the SDK to write data to Log Service. For more information about the common practices of writing data. See the "Producer Library" section of *User Guide* .
- If you consume log data, do not call the API to pull log data by using the SDK. Alibaba Cloud provides an advanced consumer library, which shields the implementation details of Log Service and provides advanced features such as load balancing and ordered consumption. For more information about the consumer library. See the "Consumer Library" section of *User Guide* .

2.15.2.3. .NET SDK

Log Service provides you with the .NET SDK to improve operation efficiency.

Where to download

The Log Service .NET SDK allows developers in the Windows platform to use Log Service with .NET Framework. At present, this SDK supports .NET Framework 3.5, 4.0, and 4.5. SDK files vary with .NET Framework versions but provides the same interfaces and functions.

Step 1 Create an account

Before accessing Log Service, you must obtain an Apsara Stack Management Console account.

Step 2 Obtain an AccessKey pair

Before using the Log Service .NET SDK, you must obtain an AccessKey pair.

Log on to Apsara Stack Management Console and obtain an AccessKey pair for the SDK.

The AccessKey pair is required to perform the following steps. Keep your AccessKey pair confidential to prevent security issues. For more information about how to use the AccessKey pair in Log Service SDKs, see SDK configuration.

Step 3 Create a Log Service project and a Logstore

Use the Log Service Java SDK to create a project and a Logstore.

> Note
>
> - Make sure you use the same account to obtain the AccessKey pair and create the Log Service project and Logstore.
> - A project name must be globally unique in Log Service, and a Logstore name must be unique across a project.
> - Once a project is created, you cannot modify the region or migrate the project between regions.

Step 4 Install the .NET development environment

At present, the Log Service .NET SDK supports .NET Framework 3.5, 4.0, and 4.5. To enable the use of Log Service SDKs, we recommend that you install:

- Microsoft .NET Framework 3.5, 4.0, or 4.5 (The actual version depends on the target environment required by your programs.)
- Visual Studio 2010 and later

Step 5 Download and prepare the Log Service .NET SDK

Install the .NET development environment before you download and prepare the Log Service .NET SDK. The preparation steps are as follows:

1. Download the SDK: Click here.
2. Decompress the downloaded package to a directory. The Log Service .NET SDK is a software development kit that does not require installation. You can perform the following steps to use the SDK in your Visual Studio projects.

Step 6 Start a new Log Service .NET project

If the Log Service .NET development environment and the .NET SDK are in place, you can create a Log Service .NET project.

2.15.2.4. Use .NET Core SDK

Context

The Log Service .NET Core SDK allows developers across different platforms to use Log Service with .NET Core.

Procedure

1. Create an account. Before accessing Log Service, you must obtain an Apsara Stack Management Console account.
2. Obtain an AccessKey pair.

   Before using the Log Service .NET Core SDK, you must obtain an AccessKey pair.

   Log on to Apsara Stack Management Console and obtain an AccessKey pair for the SDK.

   The AccessKey pair is required to perform the following steps. Keep your AccessKey pair confidential to prevent security issues. For more information about how to use the AccessKey pair in Log Service SDKs, see SDK configuration.
3. Create a Log Service project and a Logstore.

   Before using the SDK, you must create a Log Service project and a Logstore in the console.

   i. Log on to Apsara Stack Management Console.

   ii. Click **Create Project** in the upper-right corner.

   iii. Enter **Project Name** and **Region**, and click **OK**.

   iv. On the **Projects** page, click the name of the project, and then click **Create** to create a Logstore.

   After you have created a project, you can also click **Create** to create a Logstore as prompted.

   v. Complete the configurations and click **OK**.

   You must specify the Logstore name, data retention time, and number of shards. Set the number of shards as needed. In this example, you need to configure four shards.

> Note
>
> - Make sure you use the same account to obtain the AccessKey pair and create the Log Service project and Logstore.
> - A project name must be globally unique in Log Service, and a Logstore name must be unique across a project.
> - Once a project is created, you cannot modify the region or migrate the project between regions.

4. Install .NET Core.

   At present, the Log Service .NET Core SDK supports the following versions:

   - .NET Core 2.0
   - .NET Framework 4.6.2 (with .NET Core 1.x SDK)
   - .NET Framework 4.6.1 (with .NET Core 2.0 SDK)

5. Download and prepare the Log Service .NET Core SDK. Install .NET Core before you download and prepare the Log Service .NET Core SDK.
   i. Download the .NET Core SDK.
   ii. Decompress the downloaded package to a directory. The Log Service .NET Core SDK is a software development kit that does not require installation. You can perform the following steps to use the SDK in your Visual Studio projects.
6. Create a new Log Service .NET Core project.

2.15.2.5. PHP SDK

The Log Service PHP SDK provides a suite of development tools to help simplify the use of Log Service.

Download URL

Download the SDK from GitHub at .

Step 1 Create an account

You must create an account to access Log Service.

Step 2 Obtain an AccessKey pair

You must request an AccessKey pair to use the Log Service PHP SDK.

Log on to the Apsara Stack console and select an AccessKey pair for the SDK.

The AccessKey pair is used in the following steps. It must be kept confidential. For more information about how to use the AccessKey pair, see SDK configurations.

Step 3 Create a project and a Logstore

Use the Log Service PHP SDK to create a project and a Logstore.

Note

- Make sure that you use the same account to obtain an AccessKey pair and create a project and a Logstore.
- Names of each project must be unique within Log Service. Names of each Logstore must be unique within a project.
- After a project is created, the region to which it belongs cannot be changed. A project cannot be migrated between different regions.

Step 4 Configure the PHP development environment

The PHP SDK supports PHP 5.2.1 and later. Install any PHP version supported by the SDK on your local computer and set up the corresponding PHP development environment.

Step 5 Download and install the PHP SDK

Install the PHP SDK after setting up your PHP development environment. The detailed procedure is as follows:

1. Download the latest PHP SDK from GitHub.
2. Extract the downloaded SDK into a specified directory. The PHP SDK does not require additional installation steps. In addition to SDK code, the PHP SDK provides a set of third-party dependencies and an autoloader class for easy use. The following steps show you how to use the PHP SDK for your project.

Step 6 Start a new PHP project

To interact with Log Service and obtain the output, you can run the following sample code in any text editor or PHP IDE:

```
<? php
 /* Use the autoloader class to load all necessary PHP modules. Specify the path of the file that contains
the autoloader class.*/
require_once realpath(dirname(__FILE__) . '/.. /Log_Autoload.php');
$endpoint = 'regionid.example.com'; // The Hangzhou region is used in this example. During actual usag
e, specify the endpoint based on your region and access method.
$accessKeyId = '<youraccessKeyId>'; // Specify your AccessKey ID.
 $accessKey = '<youraccessKey>'; // Specify your AccessKey Secret.
$project = 'your_project'; // The name of the project created in the preceding step.
 $logstore = 'your_logstore'; // The name of the Logstore created in the preceding step.
$client = new Aliyun_Log_Client($endpoint, $accessKeyId, $accessKey);
# List the names of all Logstores in the current project.
$req1 = new Aliyun_Log_Models_ListLogstoresRequest($project);
$res1 = $client->listLogstores($req1);
var_dump($res1);
# Create a Logstore.
$req2 = new Aliyun_Log_Models_CreateLogstoreRequest($project,$logstore,3,2);
$res2 = $client -> createLogstore($req2);
```

```
 # Wait until the Logstore takes effect.
sleep(60);
# Write logs.
$topic = "";
$source = "";
$logitems = array();
for ($i = 0; $i < 5; $i++)
{
   $contents = array('index1'=> strval($i));
   $logItem = new Aliyun_Log_Models_LogItem();
   $logItem->setTime(time());
   $logItem->setContents($contents);
   array_push($logitems, $logItem);
}
$req2 = new Aliyun_Log_Models_PutLogsRequest($project, $logstore, $topic, $source, $logitems);
$res2 = $client->putLogs($req2);
var_dump($res2);
# Pull the data immediately.
# List the shard IDs in the Logstore.
$listShardRequest = new Aliyun_Log_Models_ListShardsRequest($project,$logstore);
$listShardResponse = $client -> listShards($listShardRequest);
foreach($listShardResponse-> getShardIds()  as $shardId)
{
   # Obtain the cursor corresponding to each shard ID.
   $getCursorRequest = new Aliyun_Log_Models_GetCursorRequest($project,$logstore,$shardId,null, tim
e() - 60);
   $response = $client -> getCursor($getCursorRequest);
   $cursor = $response-> getCursor();
   $count = 100;
   while(true)
   {
      # Start to read data from a cursor.
      $batchGetDataRequest = new Aliyun_Log_Models_BatchGetLogsRequest($project,$logstore,$shardI
d,$count,$cursor);
      var_dump($batchGetDataRequest);
      $response = $client -> batchGetLogs($batchGetDataRequest);
      if($cursor == $response -> getNextCursor())
      {
         break;
      }
      $logGroupList = $response -> getLogGroupList();
```

```
    foreach($logGroupList as $logGroup)
    {
        print ($logGroup->getCategory());
        foreach($logGroup -> getLogsArray() as $log)
        {
            foreach($log -> getContentsArray() as $content)
            {
                print($content-> getKey().":".$content->getValue()."\t");
            }
            print("\n");
        }
    }
    $cursor = $response -> getNextCursor();
  }
}
# Wait one minute before querying logs.
sleep(60);
# Query the distribution of logs. Note: Make sure that indexes are created before you query logs. The PHP SDK does not provide the interface which is used to create indexes. Therefore, you must create indexes in the console.
$topic = "";
$query='';
$from = time()-3600;
$to = time();
$res3 = NULL;
while (is_null($res3) || (! $res3->isCompleted()))
{
  $req3 = new Aliyun_Log_Models_GetHistogramsRequest($project, $logstore, $from, $to, $topic, $query);
  $res3 = $client->getHistograms($req3);
}
var_dump($res3);
# Query log data.
$res4 = NULL;
while (is_null($res4) || (! $res4->isCompleted()))
{
  $req4 = new Aliyun_Log_Models_GetLogsRequest($project, $logstore, $from, $to, $topic, $query, 5, 0, False);
  $res4 = $client->getLogs($req4);
}
var_dump($res4);
```

2.15.2.6. Python SDK

Log Service provides developers with the Python SDK to facilitate the use of Log Service.

Download link

Download link: Click to download.

SDK GitHub:

https://github.com/aliyun/aliyun-log-python-sdk

1. Create an account

An Apsara Stack Management Console account is required for accessing Log Service.

2. Obtain an AccessKey

Before using the Log Service Python SDK, you must request an AccessKey.

Log on to Apsara Stack Management Console and obtain an AccessKey for the SDK.

The AccessKey will be used in the following steps and must be kept confidential. For more information about how to use the AccessKey in the Log Service SDK, see SDK configuration.

3. Create a Log Service project and a Logstore

Before using the SDK, you must create a Log Service project and a Logstore in the console.

1. Log on to Apsara Stack Management Console.
2. Click **Create Project** in the upper-right corner.
3. Enter a **project name** and **region**, and click **OK**.
4. On the **Projects** page, click the name of the project, and then click **Create**.

   After you create a project, you can also click **Create** to create a Logstore as prompted.
5. Complete the configurations, and click **Confirm**.

   You must specify the Logstore name ,data retention time, and number of shards. Set the number of shards as needed. In this example, you must configure four shards.

> **Note**
>
> - Make sure you use the same account to obtain the AccessKey and create the Log Service project and Logstore.
> - A project name must be globally unique in Log Service, and a Logstore name must be unique in the same project.
> - After the project is created, you cannot modify the region or migrate the project between regions.

4 Install the Python environment

The Python SDK is a pure Python library and supports all Python operating systems, including Linux, Mac OS X and Windows. Install Python as follows:

1. Download and install the latest Python installation package.

> Note
>
> - Currently, Python SDK supports Python 2.6, 2.7, 3.3, 3.4, 3.5, and 3.6 environments. You can run the `python -V` command to query the current version of Python.
> - Python does not support Python 2.6 and Python 3.3. We recommend that you use Python 2.7, Python 3.4, and later versions.

2. Download and install the Python package management tool pip.

   After pip is installed, run the `pip -V` command to check whether the installation is successful and query the current pip version.

5 Install Python SDK

Run the following command as an administrator in Shell to install Python SDK.

```
pip install -U aliyun-log-python-sdk
```

6 Start a Python program

Now, you can start using the Python SDK. To interact with Log Service and obtain the relevant output, run the following sample code in a text editor or Python IDE.

For more information, see Github.

```
# encoding: utf-8
import time
from aliyun.log.logitem import LogItem
from aliyun.log.logclient import LogClient
from aliyun.log.getlogsrequest import GetLogsRequest
from aliyun.log.putlogsrequest import PutLogsRequest
from aliyun.log.listlogstoresrequest import ListLogstoresRequest
from aliyun.log.gethistogramsrequest import GetHistogramsRequest
def main(_):
    endpoint = '' # Select the endpoint that matches the region of the project created in the preceding ste
p.
    accessKeyId = '' # Use your Alibaba Cloud AccessKey ID.
    accessKey = '' # Use your Alibaba Cloud AccessKey Secret.
    project = '' # The name of the project created in the preceding step.
    logstore = '' # The name of the Logstore created in the preceding step.
    # Note: Configure four shards for the created Logstore for later testing.
    # Construct a client
    client = LogClient(endpoint, accessKeyId, accessKey)
    # List all LogStores
    req1 = ListLogstoresRequest(project)
    res1 = client.list_logstores(req1)
    res1.log_print()
```

```
topic = ""
source = ""
# Send 10 data packets, each of which contains 10 logs.
for i in range(10):
    logitemList = []  # LogItem list
    for j in range(10):
        contents = [('index', str(i * 10 + j))]
        logItem = LogItem()
        logItem.set_time(int(time.time()))
        logItem.set_contents(contents)
        logitemList.append(logItem)
    req2 = PutLogsRequest(project, logstore, topic, source, logitemList)
    res2 = client.put_logs(req2)
    res2.log_print()
# List all shards and read the data written in the last minute.
listShardRes = client.list_shards(project, logstore)
for shard in listShardRes.get_shards_info():
    shard_id = shard["shardID"]
    start_time = int(time.time() - 60)
    end_time = start_time + 60
    res = client.get_cursor(project, logstore, shard_id, start_time)
    res.log_print()
    start_cursor = res.get_cursor()
    res = client.get_cursor(project, logstore, shard_id, end_time)
    end_cursor = res.get_cursor()
    while True:
        loggroup_count = 100 # Read 100 packets each time.
        res = client.pull_logs(project, logstore, shard_id, start_cursor, loggroup_count, end_cursor)
        res.log_print()
        next_cursor = res.get_next_cursor()
        if next_cursor == start_cursor:
            break
        start_cursor = next_cursor
# Note: You can use the following interfaces to query data only when the index function is enabled.
time.sleep(60)
topic = ""
query = "index"
From = int(time.time()) - 600
To = int(time.time())
res3 = None
# Query the number of logs that match the query criteria during the past 10 minutes. Retry if not all ex
```

```
ecution results are correct.
    while (res3 is None) or (not res3.is_completed()):
        req3 = GetHistogramsRequest(project, logstore, From, To, topic, query)
        res3 = client.get_histograms(req3)
    res3.log_print()
    # Obtain the number of logs that match the query conditions.
    total_log_count = res3.get_total_count()
    log_line = 10
    # Read 10 logs each time until all log data is queried. Retry three times if not all query results are corr
ect during each query.
    for offset in range(0, total_log_count, log_line):
        res4 = None
        for retry_time in range(0, 3):
            req4 = GetLogsRequest(project, logstore, From, To, topic, query, log_line, offset, False)
            res4 = client.get_logs(req4)
            if res4 is not None and res4.is_completed():
                break
            time.sleep(1)
        if res4 is not None:
            res4.log_print()
    listShardRes = client.list_shards(project, logstore)
    shard = listShardRes.get_shards_info()[0]
    # Split a shard
    if shard["status"] == "readwrite":
        shard_id = shard["shardID"]
        inclusiveBeginKey = shard["inclusiveBeginKey"]
        midKey = inclusiveBeginKey[:-1] + str((int(inclusiveBeginKey[-1:])) + 1)
        client.split_shard(project, logstore, shard_id, midKey)
    # Merge shards.
    shard = listShardRes.get_shards_info()[1]
    if shard["status"] == "readwrite":
        shard_id = shard["shardID"]
        client.merge_shard(project, logstore, shard_id)
    # Delete shards
    shard = listShardRes.get_shards_info()[-1]
    if shard["status"] == "readonly":
        shard_id = shard["shardID"]
        client.delete_shard(project, logstore, shard_id)
if __name__ == '__main__':
    main()
```

2.15.2.7. Android SDK

The Log Service Android SDK is used to collect user data on an Android platform and currently provides a log data writing function.

Through GitHub

2.15.2.8. C SDK

The C SDK of Log Service is used to access logs from various platforms, such as the MIPS and OpenWrt systems.

The C SDK uses libCurl as the network library. The *apr/apr-util* library solves the issues of memory and different platforms. You only need to simply compile the source code to use the C SDK.

In addition, the C Producer Library and C Producer Lite Library provide you with a one-stop log collection solution that is simple, highly available, resource-efficient, and applicable to different platforms.

2.15.2.9. GO SDK

Log Service provides developers with the Go SDK to facilitate the use of Log Service.

The Log Service Go SDK provides the following functions:

- Writing and consuming data in batches.
- Querying and indexing data by using keywords.
- Managing Logtail configurations and machine groups.

GitHub URL: https://github.com/aliyun/aliyun-log-go-sdk

For more information about the usage instructions and sample codes, see README.

2.15.2.10. iOS SDK

The Log Service SDK is implemented based on APIs and provides the log writing function.

Swift

```
/*
   Use the endpoint, AccessKey ID, and AccessKey Secret to construct the Log Service client.
   @endPoint: see https://help.aliyun.com/document_detail/29008.html
 */
let myClient = try! LOGClient(endPoint: "",
                      accessKeyID: "",
                      accessKeySecret: "",
                      projectName:"")
/* Create a log group. */
let logGroup = try! LogGroup(topic: "mTopic",source: "mSource")
  /* Store a log. */
   let log1 = Log()
        try! log1. PutContent("K11", value: "V11")
       try! log1. PutContent("K12", value: "V12")
       try! log1. PutContent("K13", value: "V13")
   logGroup.PutLog(log1)
  /* Store a log. */
   let log2 = Log()
        try! log2. PutContent("K21", value: "V21")
       try! log2. PutContent("K22", value: "V22")
       try! log2. PutContent("K23", value: "V23")
   logGroup.PutLog(log2)
 /* Send the log. */
 myClient.PostLog(logGroup,logStoreName: ""){ response, error in
       // handle response however you want
       if error?.domain == NSURLErrorDomain && error?.code == NSURLErrorTimedOut {
          print("timed out") // note, `response` is likely `nil` if it timed out
       }
   }
```

2.16. Apsara Stack Security

2.16.1. API overview

This document introduces all of the operations that you can call by using Apsara Stack Security service APIs.

2.16.2. Apsara Stack Security Console

2.16.2.1. List of operations

This topic introduces all of the Apsara Stack Security console operations that you can call. For more information, see the corresponding operation description.

Operation	Description
DescribeAliyunAccounts	Queries Alibaba Cloud accounts.
ModifyAliyunAccount	Modifies the information of an Alibaba Cloud account.
DescribeFeatures	Queries the deployed Apsara Stack Security features.

2.16.2.2. Make API requests

2.16.2.2.1. Request structure

Apsara Stack Security API is based on Remote Procedure Call (RPC). This topic describes the structure of the API requests.

Description

You can send an HTTP request to call an API operation. The URL of the request must be in the following format:

```
http://endpoint/?Action=xx&parameters
```

Where:

- `endpoint`: the endpoint used to call a cloud service. The endpoint for the Apsara Stack Security console is `yundunprivate.[ RegionId].example.com`.
- `Action`: the operation that you want to perform.

  For example, you can set this parameter to DescribeFeatures to query the deployed Apsara Stack Security features.
- `parameters`: the request parameters. Request parameters include common request parameters and custom request parameters. Request parameters must be separated with ampersands (&).
  - Common request parameters include information such as the API version and authentication information.
  - For more information about the custom request parameters, see the corresponding operation description.

Example

Call the DescribeFeatures operation to query the deployed Apsara Stack Security features.

```
https://yundunprivate.[ RegionId].example.com/?Action=DescribeFeatures&AccessKeyId=key-test&Format=JSON&SecureTransport=true&SignatureMethod=HMAC-SHA1&SignatureNonce=15215528852396&SignatureVersion=1.0&SourceIp=1xxxx6&Timestamp=2018-03-02Txxxxxxx&Version=2018-01-16&Signature=xxxx%xxxx%3D
```

API requests are presented in the following easy-to-read format in this document:

```
https://yundunprivate.[ RegionId].example.com/?Action=DescribeFeatures
&Format=JSON
&Version=2018-01-16
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2012-06-01T12:00:00Z
```

2.16.2.2.2. Signature mechanism

Apsara Stack Security authenticates each access request. You need to include a signature for the submitted HTTP or HTTPS request.

API authorization

To ensure the security of your account, we recommend that you use a Resource Access Management (RAM) user to call API operations. Before using a RAM user to call an API operation, you must grant the RAM user the corresponding permission to call the API by creating an authorization policy and attaching the policy to the RAM user.

API signature

To ensure secure calls to the API, Alibaba Cloud authenticates each API request through the signature. When you manually make an API request, you need to use AccessKey Secret to calculate the signature, that is, the hash-based message authentication code (HMAC) value, based on the encoded and sorted request string. For more information, see the definition in RFC 2104.

This topic uses the raw access parameters in the following table to describe how to create an API signature.

Parameter	Description
Access point	`http://yundunprivate.[ RegionId].example.com/?`
API-specific parameters	`Action=DescribeFeatures`

Parameter	Description
Common parameters (excluding the Signature parameter)	&Timestamp=2016-02-23T12:46:24Z &Format=JSON &AccessKeyId=<yourAccessKeyId> &SignatureMethod=HMAC-SHA1 &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf &Version=2018-01-16 &SignatureVersion=1.0
AccessKey secret	<yourAccessKeySecret>

1. Use the request parameters to construct a canonicalized query string.

   > **Note** The request parameters include common request parameters (excluding the Signature parameter) and API-specific parameters.

   i. Sort the parameters.

   Sort the request parameters in alphabetical order.

   ii. Encode the parameters.

   Use UTF-8 to URL-encode the parameter names and values. The encoding rules are as follows:

   - Letters, digits, hyphens (-), underscores (_), periods (.), and tildes (~) are not encoded.
   - Other characters are encoded in the %XY format, where XY is the hexadecimal representation of the character in ASCII. For example, the double quotation mark (") is encoded as %22.
   - Extended UTF-8 characters are encoded in the %XY%ZA... format.
   - Note that a space is encoded as %20, instead of a plus sign (+).

   iii. Connect the encoded parameter names and values with equal signs (=).

   iv. Then, sort the parameter name and value pairs connected by equal signs in alphabetical order, and connect them with ampersands (&) to produce the canonicalized query string.

2. Use the canonicalized query string to construct the string for signature calculation based on the following rules:

```
StringToSign=HTTPMethod + “&” + percentEncode( “/” ) + ” &” +
percentEncode(CanonicalizedQueryString)
```

3. Calculate the HMAC value of the StringToSign string according to the definition in RFC 2104.

   > **Note** The key used for signature calculation is your AccessKey secret adding the ampersand (&) (ASCII 38). Secure Hash Algorithm 1 (SHA1) is used as the hash algorithm.

4. Encode the preceding HMAC value into a string based on Base64 encoding rules to obtain the signature value.

   ```
   LEW8N4y7Uasop******
   ```

5. Set the Signature parameter in the request parameters to this signature value to sign the request.

2.16.2.2.3. Common request parameters

The following table describes the common request parameters that are used to indicate information such as the API version and authentication information.

Name	Type	Required	Description
Version	String	Yes	The API version in the format of YYYY-MM-DD. Set the value to *2018-01-16*.
AccessKeyId	String	Yes	The key ID that Alibaba Cloud assigns to a user for service access.
Signature	String	Yes	The signature string.
SignatureMethod	String	Yes	The signature method. Set the value to *HMAC-SHA1*.
Timestamp	String	Yes	The timestamp of the request. Follow the ISO 8601 standard to specify the date and use the offset from Coordinated Universal Time (UTC) to specify the time zone. The format is `YYYY-MM-DDThh:mm:ssZ`. For example, 2014-05-26T12:00:00Z indicates 20:00:00 on May 26, 2014, Beijing time.
SignatureVersion	String	Yes	The signature algorithm version. Set the value to *1.0*.

Name	Type	Required	Description
SignatureNonce	String	Yes	The unique random number used to prevent network replay attacks. You must use different random numbers for different requests.
ResourceOwnerAccount	String	No	The owner account of the resource to be accessed through this API request, that is, the logon username.
Format	String	No	The format of the response. Set the value to *JSON or XML*. Note Default value: XML.

2.16.2.2.4. Response structure

Apsara Stack Security API responses support both the XML and JSON formats. The system always returns a unique identification code RequestId each time you send a request to call an operation, no matter whether the call is successful or not.

Sample responses (XML format)

```
<? xml version="1.0" encoding="UTF-8"? >
<! -- The root node of the result -->
<Operation name+Response>
   <! -- Returned request ID -->
   <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
   <! -- Returned data -->
</Operation name+Response>
```

Sample responses (JSON format)

```
{
"RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
/* Returned data */
}
```

2.16.2.3. APIs

2.16.2.3.1. DescribeAliyunAccounts

Description

You can call this operation to query Alibaba Cloud accounts.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeAliyunAccounts*.
CurrentPage	Integer	Yes	The number of the page to return.
PageSize	Integer	Yes	The number of records to return on each page.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
TotalCount	Integer	The total number of returned pages.
HttpStatusCode	Integer	The HTTP status code returned.
AliyunAccounts	Array	The Alibaba Cloud accounts. For more information, see the following descriptions.
Id	Integer	The account record ID.
Aliuid	Long	The ID of the Alibaba Cloud account.
Account	String	The name of the Alibaba Cloud account.
AccessKey	String	The AccessKey ID of the Alibaba Cloud account.
AccessSecret	String	The AccessKey secret of the Alibaba Cloud account.
DataSecret	String	The DataSecret of the Alibaba Cloud account.
LicenseAegisNum	Integer	The number of Server Guard licenses.
LicenseTime	Long	The time when the licenses expire, in timestamp format.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://yundunprivate.[ RegionId].example.com/?Action=DescribeAliyunAccounts
&CurrentPage=1
&PageSize=10
&<Common request parameters>
```

- Sample response (JSON format)

```
{
 "TotalCount":1,
 "PageSize":30,
 "RequestId":"7E33A454-20AA-49B1-8A9B-8979EFBDEDFC",
 "CurrentPage":1,
 "AliyunAccounts":[
  {
   "Account":"1113454564",
   "AccessSecret":"*****",
   "AccessKey":"<yourAccessKeyId>",
   "Id":2,
   "LicenseAegisNum":0,
   "Aliuid":1441871509587522,
   "LicenseTime":1589596257000,
   "DataSecret":"*****"
  }
 ],
 "HttpStatusCode":200
}
```

2.16.2.3.2. ModifyAliyunAccount

Description

You can call this operation to modify the information of an Alibaba Cloud account with a specified account record ID.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *ModifyAliyunAccount*.

Parameter	Type	Required	Description
Id	Integer	Yes	The account record ID.
Aliuid	Long	No	The ID of the Alibaba Cloud account.
Account	String	No	The name of the Alibaba Cloud account.
AccessKey	String	No	The AccessKey ID of the Alibaba Cloud account.
AccessSecret	String	No	The AccessKey secret of the Alibaba Cloud account.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://yundunprivate.[ RegionId].example.com/?Action=ModifyAliyunAccount
&Id=2
&Account=1113454564
&Aliuid=1441871509587522
&AccessKey=<yourAccessKeyId>
&AccessSecret=xxxxxxxxx
&<Common request parameters>
```

- Sample response (JSON format)

```
{
 "RequestId":"C92B6187-603B-4E01-B0D7-74817F43852D"
}
```

2.16.2.3.3. DescribeFeatures

Description

You can call this operation to obtain a list of the deployed Apsara Stack Security features.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeFeatures*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Features	List	The list of the deployed Apsara Stack Security features.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://yundunprivate.[ RegionId].example.com/?Action=DescribeFeatures
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"BAEF6CE3-9990-4BDA-A056-4D269A724817",
 "Features":[
  "Basic",
  "Audit",
  "Sas",
  "Waf"
 ]
}
```

2.16.3. Threat Detection Service (TDS)

2.16.3.1. List of operations

This topic introduces all the Threat Detection Service (TDS) operations that you can call. For more information, see the corresponding operation description.

Security overview operations

Operation	Description
DescribeDomain	Queries the domain names for Threat Detection Service and Rainbow.
DescribeEventsCount	Queries the number of security events, attacks, and vulnerabilities on the current day in security overview.
DescribeOverviewEventsTrend	Queries the chart data on overall security trends, including trends in security incidents, threats, and vulnerabilities.

Network traffic management operations

Operation	Description
DescribeHostTraffic	Obtains the chart data on network traffic.
DescribeHostTrafficTrend	Queries the chart data on traffic trends at the network ingress or egress.
DescribeTopTraffic	Queries detailed information about a type of network traffic within a time frame.

Access analysis operations

Operation	Description
DescribeAccessCount	Queries the number of times an online application is accessed.
DescribeTopAccess	Queries the 10 most accessed domain names in yesterday's application access records.
DescribeAccessList	Obtains a list of online application access records.
DescribeAccessTypeCount	Queries the number of times an online application is accessed by a malicious IP address or a crawler.
DescribeMaliciousIpDetail	Queries the information about a specified malicious IP address.
DescribeMaliciousIpBehaviorList	Queries attack events triggered by a malicious IP address.
DescribeMaliciousIpBehaviorMap	Queries the attack region chart based on malicious IP addresses.

Large screen operations

Operation	Description
DescribeScreenName	Queries the name of the screen that displays the traffic data on the Internet boundary.
ModifyScreenName	Modifies the name of the screen that displays the traffic security data on the Internet boundary.
DescribeFlowMap	Queries the network traffic and request information in the last two minutes as well as network traffic map information on the Internet Perimeter Traffic Security Monitoring screen.
DescribeFlowTop	Obtains the top N regions with most normal access requests or attacks in the last two minutes on the Internet Perimeter Traffic Security Monitoring screen.
DescribeScore	Obtains a security score on the Service Security Situation and Score screen.
DescribeDailyCount	Queries the number of system flaws, information leaks, and intrusions of the current day on the Service Security Situation and Score screen.
DescribeScreenAttackCount	Queries the number of attacks occurred on the current day from the Service Security Situation and Score screen.
DescribeScreenAttackTrend	Queries the attack trend in the last seven days on the Service Security Situation and Scoring screen.
DescribeScreenHighRiskAssets	Queries the top 5 attackers' favorite assets displayed on the Service Security Situation and Score screen.

Event analysis operations

Operation	Description
DescribeEventsTrend	Queries the urgent event trend in the last 30 days.
DescribeEventTypeCount	Queries the chart data on the distribution of emergencies in the last 30 days.
DescribeSecurityEventCount	Queries the types and numbers of security events.
DescribeSecurityEventList	Obtains the detailed list of security events.
DescribeListByType	Queries the security event information by asset.

Operation	Description
DescribeDdosAnalyse	Queries the analysis on DDoS attack events.
DescribeDdosFlowDetail	Queries DDoS attack traffic details.

Security report operations

Operation	Description
AddReportConfig	Adds security report settings.
DescribeReportConfigs	Query the security report configuration records.
ModifyReportConfig	Modifies the security report configuration information.
DeleteReportConfigs	Deletes the security report configuration records.

Threat awareness operations

Operation	Description
DescribeTrendCount	Queries the number of common and targeted attacks that occurred today and in the last seven days.
DescribeAttackDistribute	Queries the chart data of attacks in the last seven days by type.
DescribeAttackTrend	Obtains the chart data on attack trends in the last seven days.
DescribeAttackTypeCount	Queries the types of all application attacks that meet specified conditions and the number of attacks of each type.
DescribeAttackList	Obtains a list of attacks.
DescribeCountByType	Queries the number of threat events by type, such as threats to hosts, networks, or applications.
DescribeSecurityThreatCount	Queries the statistics on security threats.
DescribeSecurityThreatList	Obtains the detailed list of threat events.
DescribeThreatCount	Queries the number of common attack events detected during threat analysis.
DescribeThreatCountByType	Queries the number of targeted attacks detected in threat analysis by type.

Operation	Description
DescribeThreatTop	Obtains a list of attack and threat events in the last seven days.
DescribeThreatAnalyseList	Queries attack events in threat analysis.
DescribeHighRiskAssets	Queries high-risk assets.

Vulnerability scan operations

Operation	Description
DescribeVulList	Obtains a list of application vulnerabilities.
DescribeVulDistribute	Queries the report chart data on the distribution of application vulnerabilities.
DescribeVulTrend	Queries the chart data on the trends of application vulnerabilities classified by severity.
DescribeVmVulList	Queries server vulnerabilities.
DescribeVerifyVul	Verifies a specified vulnerability and query the vulnerability status.
CreateWeakPwd	Adds a custom weak password rule.
DescribeTypeList	Obtains a list of weak password rule types.
DescribeProtocolList	Obtains a list of the protocols that the weak password rules have been applied to.
DescribeWeakPwdList	Obtains a list of weak password rules.
ModifyPwd	Modifies a custom weak password rule.
ModifyStatus	Changes the weak password status to ignore a specified weak password.
DeletePwd	Deletes a custom weak password rule.

Asset management operations

Operation	Description
DescribeDistributionByCodeType	Queries the information about all regions in Apsara Stack.

Operation	Description
DescribeSystemByCodeType	Queries the information about all operating system versions used in Apsara Stack.
DescribeAssetGroup	Queries asset group details in Apsara Stack.
CreateNatAsset	Adds an NAT asset.
ModifyRegion	Modifies the region of an asset.
ModifyAssetGroup	Modifies asset group information.
ModifyGroup	Modifies the group of an asset.
ModifyAsset	Modifies asset information.
DescribeTotalAssetNumber	Obtains the total number of assets.
DescribeAllDistribution	Queries the percentages of assets in different regions in Apsara Stack.
DescribeAssetsList	Obtains a list of assets.
DescribeUuidIpList	Queries the IP address of a specified asset based on the asset UUID.
DescribeIpList	Obtains a list of asset IP addresses based on keywords.
DescribePortList	Queries ports of the server with the specified IP address.
DescribeThisMonthAssets	Queries the number of new assets added in the last 30 days.
DescribeAssetsTotalCount	Queries the chart data on the total number of assets in the last seven days.
DeleteAsset	Deletes asset information.

Alert settings operations

Operation	Description
CreateContact	Adds alert recipients.
DescribeContactsList	Obtains a list of alert recipients.
ModifyContact	Modifies alert recipients.
DeleteContact	Deletes alert recipients.
DescribeAlarmConfig	Queries the alert settings.

Operation	Description
ModifyAlarmConfig	Modifies alert settings.
DescribeReadStatus	Queries the number of unread alert messages.

2.16.3.2. Make API requests

2.16.3.2.1. Request structure

Apsara Stack Security API is based on Remote Procedure Call (RPC). This topic describes the structure of the API requests.

Description

You can send an HTTP request to call an API operation. The URL of the request must be in the following format:

```
http://endpoint/?Action=xx&parameters
```

Where:

- `endpoint` : the endpoint used to call a cloud service. The endpoint for Threat Detection Service is `sasprivate.[ RegionId].example.com` .
- `Action` : the operation that you want to perform.

  For example, you can set this parameter to DescribeScore query the overall score of the service security situation.
- `parameters` : the request parameters. Request parameters include common request parameters and custom request parameters. Request parameters must be separated with ampersands (&).
  - Common request parameters include information such as the API version and authentication information.
  - For more information about the custom request parameters, see the corresponding operation description.

Example

Call the DescribeFeatures operation to query the deployed Apsara Stack Security features.

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeScore&AccessKeyId=key-test&Format=JSON&SecureTransport=true&SignatureMethod=HMAC-SHA1&SignatureNonce=15215528852396&SignatureVersion=1.0&SourceIp=1xxxx6&Timestamp=2018-03-02Txxxxxxx&Version=2018-01-16&Signature=xxxx%xxxx%3D
```

API requests are presented in the following easy-to-read format in this document:

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeScore
&Format=JSON
&Version=2018-01-16
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2012-06-01T12:00:00Z
```

2.16.3.2.2. Signature mechanism

Apsara Stack Security authenticates each access request. You need to include a signature for the submitted HTTP or HTTPS request.

API authorization

To ensure the security of your account, we recommend that you use a Resource Access Management (RAM) user to call API operations. Before using a RAM user to call an API operation, you must grant the RAM user the corresponding permission to call the API by creating an authorization policy and attaching the policy to the RAM user.

API signature

To ensure secure calls to the API, Alibaba Cloud authenticates each API request through the signature. When you manually make an API request, you need to use AccessKey Secret to calculate the signature, that is, the hash-based message authentication code (HMAC) value, based on the encoded and sorted request string. For more information, see the definition in RFC 2104.

This topic uses the raw access parameters in the following table to describe how to create an API signature.

Parameter	Description
Access point	`http://yundunprivate.[ RegionId].example.com/?`
API-specific parameters	`Action=DescribeFeatures`

Parameter	Description
Common parameters (excluding the Signature parameter)	&Timestamp=2016-02-23T12:46:24Z &Format=JSON &AccessKeyId=<yourAccessKeyId> &SignatureMethod=HMAC-SHA1 &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf &Version=2018-01-16 &SignatureVersion=1.0
AccessKey secret	<yourAccessKeySecret>

1. Use the request parameters to construct a canonicalized query string.

   > **Note** The request parameters include common request parameters (excluding the Signature parameter) and API-specific parameters.

   i. Sort the parameters.

   Sort the request parameters in alphabetical order.

   ii. Encode the parameters.

   Use UTF-8 to URL-encode the parameter names and values. The encoding rules are as follows:

   - Letters, digits, hyphens (-), underscores (_), periods (.), and tildes (~) are not encoded.
   - Other characters are encoded in the %XY format, where XY is the hexadecimal representation of the character in ASCII. For example, the double quotation mark (") is encoded as %22.
   - Extended UTF-8 characters are encoded in the %XY%ZA... format.
   - Note that a space is encoded as %20, instead of a plus sign (+).

   iii. Connect the encoded parameter names and values with equal signs (=).

   iv. Then, sort the parameter name and value pairs connected by equal signs in alphabetical order, and connect them with ampersands (&) to produce the canonicalized query string.

2. Use the canonicalized query string to construct the string for signature calculation based on the following rules:

   ```
   StringToSign=HTTPMethod + “&” + percentEncode( “/” ) + ” &” +
   percentEncode(CanonicalizedQueryString)
   ```

3. Calculate the HMAC value of the StringToSign string according to the definition in RFC 2104.

   > **Note** The key used for signature calculation is your AccessKey secret adding the ampersand (&) (ASCII 38). Secure Hash Algorithm 1 (SHA1) is used as the hash algorithm.

4. Encode the preceding HMAC value into a string based on Base64 encoding rules to obtain the

signature value.

```
LEW8N4y7Uasop******
```

5. Set the Signature parameter in the request parameters to this signature value to sign the request.

2.16.3.2.3. Common request parameters

The following table describes the common request parameters that are used to indicate information such as the API version and authentication information.

Name	Type	Required	Description
Version	String	Yes	The API version in the format of YYYY-MM-DD. Set the value to *2018-01-16*.
AccessKeyId	String	Yes	The key ID that Alibaba Cloud assigns to a user for service access.
Signature	String	Yes	The signature string.
SignatureMethod	String	Yes	The signature method. Set the value to *HMAC-SHA1*.
Timestamp	String	Yes	The timestamp of the request. Follow the ISO 8601 standard to specify the date and use the offset from Coordinated Universal Time (UTC) to specify the time zone. The format is `YYYY-MM-DDThh:mm:ssZ`. For example, 2014-05-26T12:00:00Z indicates 20:00:00 on May 26, 2014, Beijing time.
SignatureVersion	String	Yes	The signature algorithm version. Set the value to *1.0*.
SignatureNonce	String	Yes	The unique random number used to prevent network replay attacks. You must use different random numbers for different requests.
ResourceOwnerAccount	String	No	The owner account of the resource to be accessed through this API request, that is, the logon username.

Name	Type	Required	Description
Format	String	No	The format of the response. Set the value to *JSON or XML*. Note Default value: XML.

2.16.3.2.4. Response structure

Apsara Stack Security API responses support both the XML and JSON formats. The system always returns a unique identification code RequestId each time you send a request to call an operation, no matter whether the call is successful or not.

Sample responses (XML format)

```
<? xml version="1.0" encoding="UTF-8"? >
<! -- The root node of the result -->
<Operation name+Response>
   <! -- Returned request ID -->
   <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
   <! -- Returned data -->
</Operation name+Response>
```

Sample responses (JSON format)

```
{
"RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
/* Returned data */
}
```

2.16.3.3. Security overview operations

2.16.3.3.1. DescribeDomain

Description

You can call this operation to query the domain names for Threat Detection Service and Rainbow.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeDomain*.
Lang	String	No	The value of this parameter is automatically obtained by the system.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
RainbowDomain	String	The domain name for Rainbow.
SasDomain	String	The domain name for Threat Detection Service.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeDomain
&<Common request parameters>
```

- Sample response (JSON format)

```
{
   "RequestId":"AEC7335C-51B5-414F-9ADD-3AF47A3C5BAE",
   "RainbowDomain":"rainbow.example.com",
   "SasDomain":"sas.example.com"
}
```

2.16.3.3.2. DescribeEventsCount

Description

You can call this operation to query the number of security events, attacks, and vulnerabilities on the current day in security overview.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeEventsCount*.
Distribution	String	No	The region name.
StartDate	String	No	The start time of the time frame specified for query, in timestamp format.
EndDate	String	No	The end time of the time frame specified for query, in timestamp format.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Event	Integer	The number of security events in the current day.
EventTrend	Integer	The increment or decrement of security events in the current day compared to the security events in the last day.
HackerCount	Integer	The number of attack events in the last 30 days.
Threat	Integer	The number of attack events in the current day.
ThreatTrend	Integer	The increment or decrement of attack events in the current day compared to the attack events in the last day.
Vul	Integer	The number of vulnerabilities in the current day.
VulTrend	Integer	The increment or decrement of vulnerabilities in the current day compared to the vulnerabilities in the last day.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeEventsCount
&EndDate=1234567891
&StartDate=1234566456
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "EventTrend":0,
 "RequestId":"27B97133-D561-4F46-ADEF-A0858736D5C3",
 "ThreatTrend":0,
 "Event":0,
 "HackerCount":0,
 "Vul":0,
 "VulTrend":0,
 "Threat":0
}
```

2.16.3.3.3. DescribeOverviewEventsTrend

Description

You can call this operation to query the chart data on overall security trends, including trends in security incidents, threats, and vulnerabilities.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeOverviewEventsTrend*.
Distribution	String	No	The region name.
StartDate	String	Yes	The start time of the query, in timestamp format.
EndDate	String	Yes	The end time of the query, in timestamp format.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Name	Type	Description
TotalCount	Integer	The total number of records.
TimeScope	Struct	The time range of the query. For more information, see the following parameter descriptions.
Interval	Integer	The time interval of the query.
Start	Long	The start time of the query.
LineDatas	Array	The list of security trends. For more information, see the following parameter descriptions.
Name	String	The event type.
Data	List	The number of events detected.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeOverviewEventsTrend
&EndDate=1519886538
&StartDate=1519886538
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"F7D239C2-C534-4032-8B8F-D288F22AB945",
 "TimeScope":{
  "Start":-28800000,
  "Interval":86400000
 },
 "LineDatas":[
  {
   "Data":[
    0
   ],
   "Name":"Emergency"
  },
  {
   "Data":[
    0
   ],
   "Name":"Attack"
  },
  {
   "Data":[
    0
   ],
   "Name":"Vulnerability"
  }
 ]
}
```


2.16.3.4. Network traffic management operations

2.16.3.4.1. DescribeHostTraffic

Description

You can call this operation to obtain the chart data on network traffic.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeHostTraffic*.
Distribution	String	No	The name of the region.
StartTime	String	No	The start time of the time frame specified for query, in timestamp format.
EndTime	String	No	The end time of the time frame specified for query, in timestamp format.
Type	String	Yes	The type of the network traffic chart. This parameter determines the time frame during which the traffic details is returned. Valid values: • *Default*: indicates that the traffic data in the last 24 hours is returned by default. • *Six_hour*: indicates that the traffic data in the last 6 hours is returned. • *One_day*: indicates that the traffic data in the last day is returned. By default, the traffic data in the last 24 hours is returned.
Interval	String	Yes	The interval for displaying traffic data. Note This parameter takes effect only when the Type parameter is set to Default.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of records.
TimeScope	Struct	The time frame during which the data is collected and returned. For more information, see the following parameter descriptions.

Name	Type	Description
Interval	Integer	The time length of the time frame specified for query.
Start	Long	The start time of the time frame specified for query.
LineBars	Array	The list of network traffic. For more information, see the following parameter descriptions.
Name	String	The traffic data type.
Data	List	The traffic data.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeHostTraffic
&EndTime=1519886538
&Interval=300
&StartTime=1519886538
&Type=DEFAULT
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"50EBF449-96B3-457B-91C1-8FAC448C1F67",
 "LineBars":[
     {
         "data":[
            0,
            1355,
            0,
            0
         ],
         "name":"Inbound traffic"
      },
      {
         "data":[
            0,
            272601536,
            467252288,
            0,
            0
         ],
         "name":"Outbound traffic"
      },
      {
         "data":[
            0
         ],
         "name":"QPS"
      }
   ]
}
```


2.16.3.4.2. DescribeHostTrafficTrend

Description

You can call this operation to query the chart data on traffic trends at the network ingress or egress.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeHostTrafficTrend*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Categories	List	The horizontal axis information, which is generally the timeline information in timestamp format.
LineBars	Array	The list of network traffic. For more information, see the following parameter descriptions.
Name	String	The traffic data type.
Data	List	The traffic data.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeHostTrafficTrend
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
    "RequestId":"085208CE-65DF-4A72-A207-C1ED83602081",
    "Categories":[
  "2018-02-11 16:39:00",
  "2018-02-11 16:40:00",
        "2018-02-11 16:41:00",
        "2018-02-11 16:42:00"
    ],
    "LineBars":[
  {
   "data":[
              0,
              2257,
              0,
              2257
           ],
           "name":"Traffic at the network ingress"
       },
       {
           "data":[
              577215272,
              569825463,
              574829082,
              586378445
           ],
           "name":"Traffic at the network egress"
       }
    ]
}
```


2.16.3.4.3. DescribeTopTraffic

Description

You can call this operation to query detailed information about a type of network traffic within a time range.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeTopTraffic*.
Distribution	String	No	The name of the region.
Field	String	Yes	The type of the traffic. Valid values: • *inbps*: indicates inbound traffic. • *outbps*: indicates outbound traffic. • *qps*: indicates queries per second (QPS).
DateTime	String	Yes	The beginning of the time range where data is queried, in timestamp format.
Size	Integer	No	The number of records to return.
Type	String	Yes	The type of the network traffic chart. This parameter determines the time range of the returned traffic details. Valid values: • *Default*: indicates that the traffic data in the last 24 hours is returned. • *Six_hour*: indicates that the traffic data in the last 6 hours is returned. • *One_day*: indicates that the traffic data in the last day is returned. By default, the traffic data in the last 24 hours is returned.
Interval	String	Yes	The time range of the returned traffic details. Note This parameter takes effect only when the Type parameter is set to Default.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
Traffics	Array	The network traffic details. For more information, see the following descriptions.

Parameter	Type	Description
Ip	String	The IP address.
Service	String	The type of the cloud product, such as RDS, SLB, or ECS.
Value	Long	The traffic data.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeTopTraffic
&DateTime=123456478
&Field=inbps
&Interval=5
&Size=10
&Type=SIX_HOUR
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"8D1511FF-64BD-4AB2-B8EA-E7336F7F9A57",
  "Traffics":[
    {
      "ip": "x.x.x.x",
      "product": "ECS",
      "value": 186971775440
      }
  ]
}
```

2.16.3.5. Access analysis operations

2.16.3.5.1. DescribeAccessCount

Description

You can call this operation to query the number of times an online application is accessed.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAccessCount*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
AccessCount	Struct	The number of times the application is accessed. For more information, see the following parameter descriptions.
CrawlerCount	Integer	The number of times the application is accessed by a crawler. Note If the value is 0, this parameter is not returned.
MaliciousCount	Integer	The number of times the application is accessed from a malicious IP address. Note If the value is 0, this parameter is not returned.
NormalCount	Integer	The number of normal access records. Note If the value is 0, this parameter is not returned.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAccessCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"68233B45-CAA5-4433-9E15-A8B77BA7E017",
 "AccessCount":{
  "NormalCount":10,
  "MaliciousCount":10,
  "CrawlerCount":10
 }
}
```

2.16.3.5.2. DescribeTopAccess

Description

You can call this operation to query the 10 most accessed domain names in the application access records of the previous day.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeTopAccess*.
Distribution	String	No	The region.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
StatisticsValues	Array	The 10 most accessed domain names. For more information, see the following descriptions.
StatKey	String	The domain name.
Count	Integer	The number of visits.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeTopAccess
&<Common request parameters>
```

- Sample response (JSON format)

```
{
   "RequestId":"B4913E57-31D6-49D7-8C95-E504F2C8F6A2",
   "StatisticsValues":[
        {
           "StatKey":"www.example.com",
           "Count":1
        }
    ]
}
```

2.16.3.5.3. DescribeAccessList

Description

You can call this operation to query online application access records.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeAccessList*.
Size	Integer	Yes	The number of records to return.
Start	Integer	Yes	The position of the first record to return.
AccessType	Integer	No	The type of the access. Valid values: • *0*: indicates the access from a normal IP address. • *1*: indicates the access from a malicious IP address. • *2*: indicates the access from a crawler IP address.
Distribution	String	No	The region.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
ApplicationAccesses	Array	The detailed application access records. For more information, see the following descriptions.
Id	Integer	The ID of the access record.
ReportDate	String	The date of the access.
Domain	String	The accessed domain name.
AccessType	Integer	The type of the access. Valid values: • *0*: indicates the access from a normal IP address. • *1*: indicates the access from a malicious IP address. • *2*: indicates the access from a crawler IP address.
AccessPageCount	Integer	The number of accessed pages.
FirstAccessDate	Long	The first access time of the day, in timestamp format.
SourceIp	String	The IP address of the visitor.
SourceLocation	String	The home region of the IP address of the visitor.
MaxQPS	Integer	The maximum number of accesses per second.
HasAttack	Boolean	Indicates whether Web attacks were detected during the access. Valid values: • *false*: indicates no. • *true*: indicates yes.
UserAgent	String	The proxy used for the access.
Aliuid	String	The ID of the Alibaba Cloud account.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAccessList
&Size=10
&Start=5
&AccessType=0
&Distribution=UNKNOWN
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":1,
  "RequestId":"793163EF-DEEE-4783-804D-7C600DFA234B",
  "ApplicationAccesses":[
    "AccessPageCount":1,
    "AccessType":0,
    "Aliuid":0,
    "Domain":"aaa.example.com",
    "FirstAccessDate":158956478944,
    "HasAttack":true,
    "Id":123456,
    "MaxQps":15,
    "ReportDate":"20150601",
    "SourceIp:"x.x.x.x",
    "SourceLocation":"Hangzhou",
    "UserAgent":"xxxxx"
  ]
}
```

2.16.3.5.4. DescribeAccessTypeCount

Description

You can call this operation to query the number of times an online application is accessed by a malicious IP address or a crawler.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAccessTypeCount*.

Name	Type	Required	Description
Distribution	String	No	The home region.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
AccessCounts	Array	The number of records involving malicious or crawler access to an application. For more information, see the following parameter descriptions.
AccessType	Integer	The access type. Valid values: • *1*: indicates access with a malicious IP address. • *2*: indicates crawler access.
Count	Integer	The number of access records.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAccessTypeCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"2877C944-4310-441C-AB9B-0CBA86E8AA96",
 "AccessCounts":[
  {
   "Count":0,
   "AccessType":1
  },
  {
   "Count":0,
   "AccessType":2
  }
 ]
}
```


2.16.3.5.5. DescribeMaliciousIpDetail

Description

You can call this operation to query the information about a specified malicious IP address.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeMaliciousIpDetail*.
Ip	String	Yes	The malicious IP address.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
AttackType	Integer	The ID of the attack event type.
AttackTypeName	String	The type of the attack event.
CcServer	String	The IP address of the C&C server.
Domain	String	The domain name.
Idc	String	The operator.
Ip	String	The malicious IP address.

Parameter	Type	Description
IsBotnet	String	Indicates whether the malicious IP address belongs to a Botnet (regardless of whether the IP address belongs to the Botnet controller or a device controlled by the Botnet). Valid values: • *0*: indicates no. • *1*: indicates yes.
Location	String	The home region.
TotalCount	Integer	The number of times that the malicious IP address has been reported.
TotalIpCount	Integer	The number of client IP addresses that have launched attacks.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeMaliciousIpDetail
&Ip=192.168.x.x
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId": "2191ECA9-57B5-4B35-98C3-8DCD69E1C4B7",
  "TotalIpCount": 0,
  "AttackType": 0,
  "Ip": "192.168.x.x",
  "Domain": "aaa.example.com",
  "CcServer": "aaa",
  "Idc": "aaa",
  "Location": "aaa",
  "AttackTypeName": "aaa",
  "IsBotnet": 0,
  "TotalCount": 0,
}
```

2.16.3.5.6. DescribeMaliciousIpBehaviorList

Description

You can call this operation to query attack events triggered by a malicious IP address.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeMaliciousIpBehaviorList*.
Distribution	String	No	The name of the region.
Limit	Integer	Yes	The number of records to return.
Offset	Integer	Yes	The position of the first record to return.
Ip	String	Yes	The malicious IP address.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
MaliciousIpBehaviorList	Array	The attack events. For more information, see the following descriptions.
AttackInfo	String	The victim URL.
AttackType	Integer	The ID of the attack event type.
AttackTypeName	String	The type of the attack event.
Ip	String	The malicious IP address.
RequestType	String	The type of the attack request.
Time	String	The time when the attack was launched.
VictimDomain	String	The domain name that has been attacked.
VictimIp	String	The IP address of the server that has been attacked.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeMaliciousIpBehaviorList
&Ip=192.168.x.x
&Limit=2
&Offset=0
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"F1686A4C-6D08-4596-85F3-44A1577AE26F",
  "TotalCount":1,
  "Items":[
    {
      "attackInfo":"test.example.com/to/be/attacked.html? a=b",
      "attackType":1,
      "attackTypeName":"Web attack,
      "ip":"xx.xx.xx.xx",
      "requestType":"GET",
      "time":"2015-07-07 10:43:05",
      "victimDomain":"test.example.com",
      "victimIp":"10.0.x.x"
    }
  ]
}
```

2.16.3.5.7. DescribeMaliciousIpBehaviorMap

Description

You can call this operation to query the attack region chart based on malicious IP addresses.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeMaliciousIpBehaviorMap*.
Limit	Integer	Yes	The number of records to return.

Parameter	Type	Required	Description
Ip	String	Yes	The malicious IP address.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
Ip	String	The malicious IP address.
To	List	The attack destination.
Location	Struct	The detailed information about the region of the malicious IP address. For more information, see the following descriptions.
Area	String	The name of the area.
AreaId	String	The code of the area.
City	String	The name of the city.
CityId	String	The code of the city.
Continent	String	The name of the continent.
Country	String	The name of the country.
CountryId	String	The code of the country.
Region	String	The region. For a region in China, the value is the province name and city name.
RegionId	String	The ID of the region.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeMaliciousIpBehaviorMap
&Ip=192.168.xx.xx
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"189A498F-427A-4635-9076-3749A8EC7669",
  "Ip":"192.168.x.x",
  "To":[
    {
          "ip" : "xx.xx.xx.xx",
          "isMine" : false,
          "location": {
                "area" : "East China",
                "areaId" : "300000",
                "city" : "Hangzhou",
                "cityId" : "330100",
                "continent" : "Asia",
                "country" : "China",
                "countryId" : "CN",
                "region" : "Zhejiang Province",
                "regionId" : "330000"
          }
        }
  ],
  "Location":{
    "CountryId":"IANA",
    "Area":"",
    "Continent":"Unallocated or internal IP address",
    "CityId":"",
    "AreaId":"",
    "Region":"",
    "Country":"Unallocated or internal IP address",
    "RegionId":"",
    "City":""
  }
}
```


2.16.3.6. Large screen operations

2.16.3.6.1. DescribeScreenName

Description

You can call this operation to query the name of the screen that displays the traffic data on the Internet boundary.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeScreenName*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Company	String	The name of the screen.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeScreenName
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "Company":"test",
 "RequestId":"C5490100-FB39-4AF5-879F-FD75837020BA"
}
```

2.16.3.6.2. ModifyScreenName

Description

You can call this operation to modify the name of the screen that displays the traffic security data on the Internet boundary.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyScreenName*.

Name	Type	Required	Description
Name	String	Yes	The modified screen name.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=ModifyScreenName
&Name=test
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"C5490100-FB39-4AF5-879F-FD75837020BA"
}
```

2.16.3.6.3. DescribeFlowMap

Description

You can call this operation to query the network traffic and request information in the last two minutes as well as network traffic map information on the Internet Perimeter Traffic Security Monitoring screen.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeFlowMap*.

Response parameters

Name	Type	Description

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
FlowCount	Integer	The total traffic.
RequestCount	Integer	The total number of access requests.
SasScreenFlowMaps	Array	The information on the Internet Perimeter Traffic Security Monitoring screen. For more information, see the following parameter descriptions.
City	String	The city code.
Continent	String	The continent information.
Country	String	The international code.
Region	String	The region name, which displays a city name in China or a country name outside China.
Requests	Integer	The number of access requests.
Type	Integer	The access request type. Valid values: • *0*: indicates a normal request. • *1*: indicates an attack.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeFlowMap
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"B2175A71-E1DD-44F9-AD5B-F7EC22439A8A",
 "FlowClount":13597562841,
   "SasScreenFlowMaps":[
     {
        "Region":"Hangzhou",
         "Continent":"Asia",
         "Country":"CN",
         "City":"hz",
         "Requests":1,
         "Type":0
      }
   ],
   "RequestCount":0
}
```


2.16.3.6.4. DescribeFlowTop

Description

You can call this operation to obtain the top N regions with most normal access requests or attacks in the last two minutes on the Internet Perimeter Traffic Security Monitoring screen.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeFlowTop*.
Type	Integer	Yes	The type of access requests whose statistics are to be returned. Valid values: • *5*: indicates that the top 5 regions with most access requests (including normal access requests and attacks) are returned. • *1*: indicates that the top N regions with most normal access requests are returned. • *2*: indicates that the top N regions with most attacks are returned.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of records.
SasScreenFlowMaps	Array	The information on the Internet Perimeter Traffic Security Monitoring screen. For more information, see the following parameter descriptions.
Region	String	The region name, which displays a city name in China or a country name outside China.
Requests	Integer	The number of requests.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeFlowTop
&Type=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId":"3F156598-D362-45AB-BC87-E3199197B8D0",
  "SasScreenFlowMaps":[
    {
      "Region":"",
      "Requests":29616
    }
  ],
  "TotalCount":1
}
```

2.16.3.6.5. DescribeScore

Description

You can call this operation to obtain a security score on the service security situation and scoring dashboard.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeScore*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
Aliuid	Integer	The ID of the Alibaba Cloud account.
CountDate	String	The statistical time.
CreateDate	String	The creation time.
ModifiedDate	String	The modification time.
Id	Integer	The primary key ID.
Score	Integer	The security score.
Details	Array	The security score details. For more information, see the following descriptions.
EventName	String	The name of the event.
EventType	String	The type of the event.
HostName	String	The name of the server.
Product	String	The type of the cloud product.
Vmlp	String	The IP address of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeScore
&<Common request parameters>
```

- Sample response (JSON format)

```
{
   "RequestId":"441D233D-C05A-40C5-824C-0C301C328CB6",
      "Details":[
      {
         "EventName":"Webshell",
         "EventType":"SECURITY_EVENT",
         "HostName":"iZys605x4c3wlmdxkfy****",
         "Product":"HOST",
         "VmIp":"192.168.xx.xx"
      }
     ],
      "Score":33,
   "id":682292,
   "modifiedDate":"2018-03-22 11:33:09",
   "aliuid":-1,
   "countDate":"2018-03-22 00:00:00",
   "createDate":"2018-03-22 00:00:10"
}
```


2.16.3.6.6. DescribeDailyCount

Description

You can call this operation to query the number of system flaws, information leaks, and intrusions of the current day on the Service Security Situation and Score screen.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeDailyCount*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Event	Struct	The description and number of security events of the current day. For more information, see the following parameter descriptions.

Name	Type	Description
Info	String	The description of security events.
Total	Integer	The total number of security events of the current day.
Leakage	Struct	The description and number of information leak events of the current day. For more information, see the following parameter descriptions.
Info	String	The description of information leak events.
Total	Integer	The total number of information leak events of the current day.
Vul	Struct	The description and number of flaws of the current day. For more information, see the following parameter descriptions.
Info	String	The description of the flaws.
Total	Integer	The total number of flaws of the current day.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeDailyCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"D5B980D1-660D-4265-8E4E-7F7936533E40",
 "Event":[
  {
   " Total ":10
  }
 ],
 "Leakage":[
  {
   " Total ":10
  }
 ],
 "Vul":[
  {
   " Total ":10
  }
 ]
}
```


2.16.3.6.7. DescribeScreenAttackCount

Description

You can call this operation to query the number of attacks occurred on the current day from the Service Security Situation and Score screen.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeScreenAttackCount*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Crack	Integer	The number of brute-force attacks.
Web	Integer	The number of Web application attacks.

Name	Type	Description
Ddos	Integer	The number of DDoS attacks.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeScreenAttackCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "Ddos":0,
 "RequestId":"7A9D6B6B-D7BD-4D89-B77E-9AB21CEC15E7",
 "Web":0,
 "Crack":0
}
```

2.16.3.6.8. DescribeScreenAttackTrend

Description

You can call this operation to query the attack trend in the last seven days on the Service Security Situation and Score screen.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeScreenAttackTrend*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Interval	Integer	The time interval of the query.
Start	Long	The start time of the query.

Name	Type	Description
AttackItems	List	The list of attack events. For more information, see the following parameter descriptions.
AttackName	String	The attack description, such as targeted attacks or common attacks.
AttackData	String	The number of attacks.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeScreenAttackTrend
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"B787F4A8-C2DC-4CC8-9443-F2F655A9DDFD",
 "Start":1517673600000,
 "AttackItems":[
  {
   "AttackData":[
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0
   ],
   "AttackName":"Common attack"
  },
  {
   "AttackData":[
    0,
    0,
    0,
    0,
    0,
    0,
    0,
    0
   ],
   "AttackName":"Targeted attack"
  }
 ],
 "Interval":86400000
}
```


2.16.3.6.9. DescribeScreenHighRiskAssets

Description

You can call this operation to query the top 5 attackers' favorite assets displayed on the Service Security Situation and Score screen.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeScreenHighRiskAssets*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of returned records.
ScreenHighRiskAssets	List	A list of high-risk assets. For more information, see the following parameter descriptions.
AssetGroup	String	The name of the asset group.
Distribution	String	The region of the asset.
HostName	String	The customized asset names.
Ip	String	The IP address of the asset.
NormalCount	Integer	The number of normal attacks launched to the asset.
SepcificCount	Integer	The number of targeted attacks launched to the asset.
Service	String	The asset type, such as RDS, SLB, or ECS.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeScreenHighRiskAssets
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"05B2B418-3248-4F95-89CC-A3141E736E37",
 "Total":0,
 "ScreenHighRiskAssets":[
      {
           "Ip": "xx.xx.xx.xx",
            "Product": "",
            "HostName": "Group 1",
            "NormalCount": 3000,
            "SpecificCount": 500,
            "Distribution":"",
            "AssetGroup":""
 }
 ]
}
```


2.16.3.7. Event analysis operations

2.16.3.7.1. DescribeEventsTrend

Description

You can call this operation to query the urgent event trend in the last 30 days.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeEventsTrend*.
Distribution	String	No	The region name.
StartDate	String	No	The start time of the time frame specified for query, in timestamp format.
EndDate	String	No	The end time of the time frame specified for query, in timestamp format.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of returned records.
TimeScope	Struct	The time frame during which the urgent event trend is queried. For more information, see the following parameter descriptions.
Interval	Integer	The time interval between the query and response.
Start	Long	Start time of the time frame specified for query.
Events	Array	A list of security events. For more information, see the following parameter descriptions.
Name	String	The description of the security event.
Data	List	The number of security events.
ExtendData	Struct	The additional information about the security events. For more information, see the following parameter descriptions.
TodayCount	Integer	The number of events that occurred on the current day.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeEventsTrend
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"DB86A047-3153-4149-8301-6043CD7A4A9C",
 "events":[
  {
   "Data": [{
    0
   ],
   "Name":"Security event"
  }
 ],
 "ExtendData":{
  "TodayCount":0
 },
 "TimeScope":{
  "Start":1440000000,
  "Interval":86400000
 }
}
```


2.16.3.7.2. DescribeEventTypeCount

Description

You can call this operation to query the chart data on the distribution of emergencies in the last 30 days.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeEventTypeCount*.
Distribution	String	No	The name of the region.
StartDate	String	No	The start time of data collection, in timestamp format.
EndDate	String	No	The end time of data collection, in timestamp format.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of records.
PieItems	Struct	The chart data on security event types. For more information, see the following parameter descriptions.
Name	String	The name of the security event type.
Data	String	The percentage of each type of security event.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeEventTypeCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":2,
 "RequestId":"3E8B3881-1E05-4899-9973-1DD2AFC7C57B",
 "PieItems":[
{
        "data":0.02,
        "name":"Webpage defacement"
      },
      {
         "data":0.01,
         "name":"Successful brute-force attack"
      }]
}
```

2.16.3.7.3. DescribeSecurityEventCount

Description

You can call this operation to query the types and numbers of security events.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeSecurityEventCount*.
Distribution	String	No	The name of the region.
Status	Integer	No	The status of security events. Valid values: • *0*: indicates all security events. • *1*: indicates ignored security events. Default value: 0.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Categorys	Array	The list of security event types. For more information, see the following parameter descriptions.
Category	Integer	The ID of the security event type.
CategoryName	String	The name of the security event type.
Count	Integer	The number of security events.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeSecurityEventCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "Categorys":[
  {
   "Category":1,
   "CategoryName":"Webpage defacement",
   "Count":0
  }
 ],
 "RequestId":"1AD76A32-A3BE-4A1C-8273-3327A2226F93"
}
```


2.16.3.7.4. DescribeSecurityEventList

Description

You can call this operation to query security events.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeSecurityEventList*.
Distribution	String	No	The name of the region.
Size	Integer	Yes	The number of records to return.
Start	Integer	Yes	The position of the first record to return.
Category	Integer	No	The ID of the security event category.
Status	Integer	No	The type of security events to collect. Valid values: • *0*: indicates all events. • *1*: indicates ignored events. Default value: 0.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Parameter	Type	Description
TotalCount	Integer	The number of returned records.
SecurityEvents	Array	The security events. For more information, see the following descriptions.
Aliuid	Long	The ID of the Alibaba Cloud account.
Assets	String	The name of the asset.
Category	Integer	The ID of the main security event category.
CategoryName	String	The name of the main security event category.
Create	String	The time when the record was created.
DestinationIp	String	The destination IP address.
DetailStr	String	The detailed information about the security event.
Distribution	String	The region.
EventName	String	The name of the security event sub-category.
EventType	String	The ID of the security event sub-category.
FileMd5	String	The MD5 value of the Server Guard file, used as a supplement to global infection data.
Id	Integer	The primary key ID.
IsFinished	Integer	Indicates whether the event has finished, mainly used for distributed denial of service (DDoS) attacks, botnet attacks, and other security events of which the end time needs to be updated.
Modified	String	The time when the record was last modified.
Product	String	The cloud product.
Status	Integer	The type of security events that were collected. Valid values: • *0*: indicates all events. • *1*: indicates ignored events.
ThreatStr	String	The detailed information about the threat.
Time	String	The time when the event occurred.
Uuid	String	The universally unique identifier (UUID) of the asset.

Parameter	Type	Description
VmIp	String	The IP address of the asset.
UniqueInfo	String	The identifier that identifies whether the same event is occurring.
Detail	Struct	The detailed information about the event. For more information, see the following descriptions.
AssetGroup	String	The asset group.
Assets	String	The name of the asset.
Distribution	String	The region.
FilePath	String	The file path.
HasDownload	Boolean	Indicates whether the file has been downloaded.
Md5	String	The MD5 value of the file.
Status	Integer	The type of security events that were collected. Valid values: • *0*: indicates all events. • *1*: indicates ignored events.
TfsFileName	String	The name of the file.
Type	String	The name of the security event sub-category.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeSecurityEventList
&Category=4
&Size=5
&Start=1
&Status=0
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId": "C1B61C25-C3D6-4585-A680-152909697B68",
  "Total": 1,
  "SecurityEvents": [{
```

```
    "aliuid": 104341365258****,
    "assets": "192.168.xx.xx",
    "category": 4,
    "categoryName": "Webshell",
    "create": "2018-02-06 04:09:17",
    "destinationIp": "192.168.xx.xx",
    "detail": {
      "hasDownload": true,
      "assets": "(Host)192.168.xx.xx",
      "status": 0,
      "filePath": "/usr/local/nginx/html/test_9303.asp",
      "tfsFileName": "OSS://sas:webshell/9c5c0b439560234754157eecbcf192f4.aegis",
      "md5": "9c5c0b439560234754157eecbcf1****",
      "assetGroup": "1",
      "type": "webshell",
      "distribution": "cn-hangzhou-env6-d01",
      "departmentName": "****"
    },
    "detailStr":"{'assets':'192.168.xx.xx','protocol':'SSH','count':100,'sourceIp':'xx.xx.xx.xx(Xi'an City, Shaanxi Province, China)','assetGroup':'7','departmentName':'R&D','password':'*******','maliciousIp':'xx.xx.xx.xx','distribution':'cn-hangzhou-env6-d01'}",
    "distribution": "cn-hangzhou-env6-d01",
    "eventName": "webshell",
    "eventType": 5,
    "fileMd5": "9c5c0b439560234754157eecbcf1****",
    "id": 10367,
    "isFinished": 0,
    "modified": "2018-02-13 05:47:33",
    "product": "Host",
    "status": 0,
    "threatStr": "{}",
    "time": "2018-02-13 05:47:30",
    "uniqueInfo": "i3jUSiuaNfgbkqrpgYG+****",
    "uuid": "b166d72f-eb80-4fb8-bd83-ddc461d6****",
    "vmIp": "192.168.xx.xx"
  }]
}
```


2.16.3.7.5. DescribeListByType

Description

You can call this operation to query the security event information by asset.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeListByType*.
Distribution	String	No	The name of the region.
StartDate	String	No	The start time of the queried security events, in timestamp format.
EndDate	String	No	The end time of the queried security events, in timestamp format.
Limit	Integer	Yes	The number of returned records.
Start	Integer	Yes	The start position of the first record to be returned.
Type	String	No	The type of the asset. Valid values: • *Server* • *Application* • *Network* • *Personnel* • *Information*

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of records.
OverviewAssets	Array	The event information listed by asset. For more information, see the following parameter descriptions.
Index	String	The identifier of the record.
Details	String	The event details. For more information, see the following parameter descriptions.
Type	String	The type of the event.

Name	Type	Description
Category	String	The category of the event.
Content	String	The content of the event.
Page	String	The page on which the event occurred.
Time	String	The time when the event occurred.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeListByType
&Limit=10
&Start=0
&EndDate=1519886538
&StartDate=1519886538
&Type=server
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "RequestId":"DE2595A0-AC52-47F1-84D9-D3383E933AD4",
 "OverviewAssets":[
  {
            "Detail": [
               {
                  "Category": "cms_invalid_login",
                  "Content": "xx.xx.xx.xx (in xx city, xx province) initiated an unusual logon attempt. Thre
at level: 0.5.",
                  "Page": "THREAT_ANALYSE",
                  "Time": "2015-12-23 08:57:49",
                  "Type": "Unusual logon"
               }
            ],
            "Index": "aa.aa.aa.aa"
         }
 ]
}
```


2.16.3.7.6. DescribeDdosAnalyse

Description

You can call this operation to query the analysis on distributed denial of service (DDoS) attack events.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeDdosAnalyse*.
Limit	Integer	Yes	The number of records to return.
Offset	Integer	Yes	The position of the first record to return.
StartTime	String	No	The beginning of the time range where data is queried, in timestamp format.
EndTime	String	No	The end of the time range where data is queried, in timestamp format.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
DdosAnalyses	Array	The DDoS attack analysis report. For more information, see the following descriptions.
AssetType	String	The cloud product to which the victim IP address belongs.
Ip	String	The IP address of the victim server.
Num	Integer	The ID of the record in the attack analysis report.
Time	String	The time when the attack occurred.
Items	Array	The DDoS attack details.
Name	String	The type of the attack.
Pre	Float	The percentage of the attack type compared to all attack types.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeDdosAnalyse
&EndTime=1519886538
&Limit=10
&Offset=0
&StartTime=1517886538
&<Common request parameters>
```

- Sample response (JSON format)

```
{
 "TotalCount":1,
 "RequestId":"EAF74731-4EBF-456E-AD8B-4067AEF817F6",
 "DdosAnalyses":[{
      "Ip": "x.x.x.x",
      "Items": [
       {
         "Pre": 98.99311157999256,
         "Name": "ack"
       }
      ],
      "Num": 1,
      "Time": "2015-08-06 10:23:55",
       "AssetType":"HOST"
    }]
}
```


2.16.3.7.7. DescribeDdosFlowDetail

Description

You can call this operation to query DDoS attack traffic details.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeDdosFlowDetail*.
VmIp	String	Yes	The victim IP address.
Distribution	String	No	The region.
StartTime	String	No	The start time of the time frame specified for query, in timestamp format.
EndTime	String	No	The end time of the time frame specified for query, in timestamp format.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Categories	List	The X-axis information. This parameter typically indicates the timeline information in timestamp format.
CategoriesType	String	The type of the timeline, which is milliseconds (ms).
LineBars	List	The DDoS attack traffic information. For more information, see the sample response.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeDdosFlowDetail
&Vmlp=x.x.x.x
&EndDate=1534667456
&StartDate=1534567456
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"213C2229-0133-47E1-A5D5-75D68DC5F02D",
 "Categories":[
  "1520768550000",
  "1520768850000",
  "1520769150000",
  "1520769450000"
 ],
 "CategoriesType":"ms",
 "LineBars":[
  {
   "data": [
    0,
    0,
    0,
    0
   ],
   "name":"Inbound traffic"
  },
  {
   "data": [
    0,
    0,
    0,
    0
   ],
   "name":"Outbound traffic"
  },
  {
   "data": [
    0,
    0,
    0,
    0
   ],
   "name":"QPS"
  }
 ]
}
```

2.16.3.8. Security report operations

2.16.3.8.1. AddReportConfig

Description

You can call this operation to add security report settings.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *AddReportConfig*.
Name	String	Yes	The name of the security report.
Description	String	Yes	The description of the security report task.
Type	String	Yes	The type of the report. Valid values: • *1*: indicates a daily report. • *2*: indicates a weekly report. • *3*: indicates a monthly report.
ReportFormat	String	Yes	The format of the security report. Currently, this parameter can only be set to *html*, which indicates the HTML format.
ReportStatus	Integer	Yes	The status of the report sending feature. Valid values: • *0*: indicates disabled. • *1*: indicates enabled.
Email	String	Yes	The email address of the report recipient.
Content	String	Yes	The report content.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=AddReportConfig
&Content=aa
&Description=description
&Email=aaa@example.com
&Name=test
&ReportFormat=html
&ReportStatus=0
&Type=1
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"840C7302-A3CD-48B4-9B5A-7C025A946D0F"
}
```

2.16.3.8.2. DescribeReportConfigs

Description

You can call this operation to query the security report configuration records.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeReportConfigs*.
PageSize	String	Yes	The number of records to return on each page.
CurrentPage	String	Yes	The number of the page to return.
Name	String	No	The name of the security report.

Parameter	Type	Required	Description
Status	Integer	No	The status of the report sending feature. Valid values: • *0*: indicates disabled. • *1*: indicates enabled.
Type	String	Yes	The type of the report. Valid values: • *1*: indicates a daily report. • *2*: indicates a weekly report. • *3*: indicates a monthly report.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
ReportConfigResults	Array	The security report configuration details. For more information, see the following descriptions.
Content	List	The content of the security report.
DepartmentName	String	The name of the department.
Description	String	The description of the security report configuration.
Email	List	The email addresses of senders.
Format	List	The report formats.
Id	Integer	The ID of the security report configuration list.
Name	String	The name of the security report.
Status	Integer	The status of the report sending feature. Valid values: • *0*: indicates disabled. • *1*: indicates enabled.
Type	Integer	The type of the report. Valid values: • *1*: indicates a daily report. • *2*: indicates a weekly report. • *3*: indicates a monthly report.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeReportConfigs
&CurrentPage=1
&PageSize=10
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"55D22C46-5EA2-481C-9615-B6CE080B5E18",
  "Total":1,
  "ReportConfigResults":[
    {
      "Status":-1,
      "Type":1,
      "Format":[],
      "Description":"",
      "Email":[
        "xx@example.com"
      ],
      "Content":[
        "aaaaa"
      ],
      "DepartmentName":"****",
      "Id":6,
      "Name":""
    }
  ]
}
```

2.16.3.8.3. ModifyReportConfig

Description

You can call this operation to modify the security report configuration information.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *ModifyReportConfig*.
Id	Integer	Yes	The ID of the security report configuration record.
Name	String	Yes	The name of the security report.
Description	String	Yes	The description of the security report task.
Type	String	Yes	The type of the report. Valid values: • *1*: indicates a daily report. • *2*: indicates a weekly report. • *3*: indicates a monthly report.
ReportFormat	String	Yes	The format of the security report. This parameter can be set to *html* only, which indicates the HTML format.
Status	Integer	Yes	The status of the report sending feature. Valid values: • *0*: indicates disabled. • *1*: indicates enabled.
Email	String	Yes	The email address of the report recipient.
Content	String	Yes	The report content.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=ModifyReportConfig
&Content=test
&Description=test
&Email=test@example.com
&Id=123
&Name=111
&ReportFormat=html
&Status=0
&Type=1
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"840C7302-A3CD-48B4-9B5A-7C025A946D0F"
}
```

2.16.3.8.4. DeleteReportConfigs

Description

You can call this operation to delete the security report configuration records.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteReportConfigs*.
Id	String	Yes	The ID of the security report task.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DeleteReportConfigs
&Id=123321
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"840C7302-A3CD-48B4-9B5A-7C025A946D0F"
}
```

2.16.3.9. Threat Detection Service operations

2.16.3.9.1. DescribeTrendCount

Description

You can call this operation to query the number of common and targeted attacks that occurred today and in the last seven days.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeTrendCount*.
Distribution	String	No	The region name.
StartDate	String	Yes	The start time of the query, in timestamp format.
EndDate	String	Yes	The end time of the query, in timestamp format.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TodayCount	Integer	The number of common attacks that occurred today.
TodaySpecialCount	Integer	The number of targeted attacks that occurred today.

Name	Type	Description
TimeScope	Struct	The time range of the query. For more information, see the following parameter descriptions.
Interval	Integer	The time interval of the query.
Start	Long	The start time of the query.
Items	Array	The list of attack events. For more information, see the following parameter descriptions.
Name	String	The attack event description.
Data	List	The number of attacks on each of the last seven days.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeTrendCount
&EndDate=154451231211
&StartDate=154461231211
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TodayCount":0,
 "timeScope":{
  "Interval":86400000,
  "Start":1519920000000
 },
 "Items":[
  {
   "Data":[0,0,0,2,1,437290,0],
   "Name":"Common attack"
  },
  {
   "Data":[0,0,0,0,0,0,0],
   "Name":"Targeted attack"
  }
 ],
 "TodaySpecialCount":0,
 "RequestId":"5A725105-FE73-4D75-A88D-88E559AE452C"
}
```


2.16.3.9.2. DescribeAttackDistribute

Description

You can call this operation to query the chart data of attacks in the last seven days by type.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAttackDistribute*.
Distribution	String	No	The name of the region.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Name	Type	Description
PieItems	Array	The list of different types of attacks. For more information, see the following parameter descriptions.
Data	Integer	The number of the specific type of attacks.
Name	String	The name of the attack type.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAttackDistribute
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"D3155ED6-721C-4C40-8509-0E00861E2B5C",
 "PieItems":[
  {
        "data":100,
        "name":"Path traversal"
  },
  {
         "data":0,
         "name":"Trojan script"
      }
 ]
}
```

2.16.3.9.3. DescribeAttackTrend

Description

You can call this operation to obtain the chart data on attack trends in the last seven days.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAttackTrend*.
Distribution	String	No	The name of the region.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of records.
TimeScope	Struct	The time frame during which the data is collected and returned. For more information, see the following parameter descriptions.
Interval	Integer	The time length of the time frame during which the data is collected.
Start	Long	The start time of the time frame specified for query.
LineBarItems	Array	The list of attack trends. For more information, see the following parameter descriptions.
Name	String	The description of the attack.
Data	List	The number of attacks on each of the last seven days.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAttackTrend
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"50D070D7-9BE4-45A2-B234-1915ED487186",

 "TimeScope":{
  "Start":1517846400000,
  "Interval":86400000
 },
 "LineBarItems":[
  {
   "Data":[
    0,
    0,
    0,
    0,
    0,
    0,
    0
   ],
   "Name":"SQL injection"
  },
  {
   "Data":[
    0,
    0,
    0,
    0,
    0,
    0,
    0
   ],
   "Name":"XSS attack"
  }
 ]
}
```


2.16.3.9.4. DescribeAttackTypeCount

Description

You can call this operation to query the types of all application attacks that meet specified conditions and the number of attacks of each type.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAttackTypeCount*.
Distribution	String	No	The region name.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Attacks	Array	The list of attack types and number of attacks of each type. For more information, see the following parameter descriptions.
AttackType	String	The attack type.
AttackTypeDesc	String	The description of the attack type.
Count	Integer	The number of attack events of the attack type.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAttackTypeCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"5A725105-FE73-4D75-A88D-88E559AE452C",
 "Attacks":[
  {
   "AttackTypeDesc":"SQL injection",
   "AttackType":"sqli",
   "Count":0
  },
  {
   "AttackTypeDesc":"XSS attack",
   "AttackType":"xss",
   "Count":0
  }
 ]
}
```


2.16.3.9.5. DescribeAttackList

Description

You can call this operation to query attacks.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeAttackList*.
Distribution	String	No	The name of the region.
Size	Integer	Yes	The number of records to return.
Start	Integer	Yes	The position of the first record to return.
AttackType	String	No	The type of the attack.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.

Parameter	Type	Description
AttackList	Array	The attacks. For more information, see the following descriptions.
Id	Integer	The ID of the attack.
Aliuid	Long	The ID of the Alibaba Cloud account.
AssetGroup	String	The name of the asset group.
AttackDate	String	The time when the attack was launched.
AttackType	String	The type of the attack.
AttackTypeDesc	String	The name of the attack type.
Domain	String	The attacked domain name.
Method	String	The request method of the attack.
SourceIp	String	The attack source IP address.
SourceLocation	String	The source area where the attack was launched.
URL	String	The victim URL.
VmIp	String	The IP address of the victim server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAttackList
&Size=10
&Start=0
&<Common request parameters>
```

- Sample response (JSON format)

```
{
 "TotalCount":1,
 "RequestId":"A2A06A09-CB42-4B36-856E-9675CEB8C3C1",
 "ApplicationAttacks":[
  {
   "aliuid":-1,
            "assetGroup":"Default group",
            "attackDate":"2018-02-13 07:56:31",
            "attackType":"path",
            "attackTypeDesc":"Path traversal",
            "distribution":"IDC unspecified",
            "domain":"www.example.com",
            "id":628370,
            "method":"GET",
            "sourceIp":"192.168.x.x",
            "sourceLocation":"Internal IP address",
            "url":"GET /mypic1/bom.php? dir=./data/bak/HTTP/1.1..Host: www.example.com:445..Referer
: -..User-Agent: curl/7.47.0....",
            "vmIp":"10.36.x.x"
        }
 ]
}
```


2.16.3.9.6. DescribeCountByType

Description

You can call this operation to query the number of threat events by type, such as threats to servers, networks, or applications.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeCountByType*.
Distribution	String	No	The region name.
StartDate	String	No	The start time of the query, in timestamp format.
EndDate	String	No	The end time of the query, in timestamp format.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
ThreatTypes	Array	The list of threat types and number of threats of each type. For more information, see the following parameter descriptions.
Name	String	The threat type, such as threats to servers, networks, or applications.
Count	Integer	The number of threats.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeCountByType
&EndDate=1519886538
&StartDate=1517886538
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"D5B980D1-660D-4265-8E4E-7F7936533E40",
 "Items":[
  {
   "Count":0,
   "Name":"host"
  }
 ]
}
```

2.16.3.9.7. DescribeSecurityThreatCount

Description

You can call this operation to query the statistics on security threats.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeSecurityThreatCount*.
Distribution	String	No	The name of the region.
Status	Integer	No	The status of the threat. Valid values: • *0*: indicates all threats. • *1*: indicates ignored threats. Default value: *0*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Categorys	Array	The list of threat types. For more information, see the following parameter descriptions.
Category	Integer	The ID of the threat type.
CategoryName	String	The name of the threat type.
Count	Integer	The number of threats.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeSecurityThreatCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"05BE5EBD-A325-4556-919C-391BF623CDB0",
 "Categorys":[
  {
   "Category":1,
   "CategoryName":"Access from malicious IP addresses",
   "Count":0
  },
  {
   "Category":2,
   "CategoryName":"Weak password",
   "Count":0
  }
 ]
}
```


2.16.3.9.8. DescribeSecurityThreatList

Description

You can call this operation to query threat events.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeSecurityThreatList*.
Distribution	String	No	The name of the region.
Size	Integer	Yes	The number of records to return.
Start	Integer	Yes	The position of the first record to return.
Category	Integer	No	The ID of the threat event category.
Status	Integer	No	The type of threat events to collect. Valid values: • *0*: indicates all events. • *1*: indicates ignored events. Default value: *0*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
SecurityEvents	Array	The threat events. For more information, see the following descriptions.
Aliuid	Long	The ID of the Alibaba Cloud account.
Asset	String	The name of the asset.
Category	Integer	The ID of the main threat event category.
CategoryName	String	The name of the main threat event category.
Create	String	The time when the record was created.
DestinationIp	String	The destination IP address.
DetailStr	String	The detailed information about the threat event.
Distribution	String	The region.
FirstReportTime	String	The time when the threat event was detected for the first time.
Id	Integer	The primary key ID.
LastReportTime	String	The time when the threat event was last detected.
Modified	String	The time when the record was last modified.
Product	String	The cloud product.
Status	Integer	The type of threat events that were collected. Valid values: • *0*: indicates all events. • *1*: indicates ignored events.
Threat	String	The name of the threat event sub-category.
ThreatType	Integer	The ID of the threat event sub-category.
Uuid	String	The universally unique identifier (UUID) of the asset.
VmIp	String	The IP address of the asset.

Parameter	Type	Description
UniqueInfo	String	The identifier that identifies whether the same event is occurring.
Detail	Struct	The detailed information about the threat. For more information, see the following descriptions.
AssetGroup	String	The asset group.
Assets	String	The name of the asset.
Count	Integer	The number of threats.
DepartmentName	String	The name of the department.
Distribution	String	The region.
MaliciousIp	String	The malicious IP address.
Password	String	The weak password.
Protocol	String	The protocol.
SourceIp	String	The source IP address.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeSecurityThreatList
&Category=4
&Size=5
&Start=1
&Status=0
&<Common request parameters>
```

- Sample response (JSON format)

```
{
   "RequestId":"11C797AD-6F9A-44CF-AE8B-B3353AE96CA2",
   "Total":23,
   "SecurityThreats ":[
      {
            "aliuid":143841340822****,
            "asset":"192.168.xx.xx",
            "category":9,
```

```
            "categoryName":"brute-force attack",
            "create":"2018-02-11 17:23:48",
            "destinationIp":"192.168.xx.xx",
            "detail":{
               "assets":"192.168.xx.xx",
               "protocol":"SSH",
               "count":100,
               "sourceIp":"xx.xx.xx.xx(xx city, xx province)",
               "assetGroup":"7",
               "distribution":"cn-hangzhou-env6-d01",
               "maliciousIp":"xx.xx.xx.xx",
               "password":"*******",
               "departmentName":"R&D"
            },
            "detailStr":"{'assets':'192.168.xx.xx','protocol':'SSH','count':100,'sourceIp':'xx.xx.xx.xx(xx city, x
x province)','assetGroup':'7','departmentName':'R&D','password':'*******','maliciousIp':'xx.xx.xx.xx','distri
bution':'cn-hangzhou-env6-d01'}",
            "distribution":"cn-hangzhou-env6-d01",
            "firstReportTime":"2018-02-11 17:23:48",
            "id":219,
            "lastReportTime":"2018-02-11 17:23:48",
            "modified":"2018-02-11 17:23:48",
            "product":"HOST",
            "sourceIp":"xx.xx.xx.xx",
            "status":0,
            "threat":"192.168.xx.xx",
            "threatType":11,
            "uniqueInfo":"192.168.xx.xx#xx.xx.xx.xx",
            "uuid":"efbbeb4b-b6c7-4e82-a0ce-5548f20aa041",
            "vmIp":"192.168.xx.xx"
         }
   ]
}
```


2.16.3.9.9. DescribeThreatCount

Description

You can call this operation to query the number of common attack events detected during threat analysis, including the total number of Web application attacks and brute-force attacks detected by the traffic security monitoring module.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeThreatCount*.
Distribution	String	No	The region name.
StartDate	String	No	The start time of the query, in timestamp format.
EndDate	String	No	The end time of the query, in timestamp format.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
SpecificCount	Integer	The total number of attack events.
SourceIpCount	Integer	The number of attack events after deduplication.
TotalCount	Integer	The total number of records.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeThreatCount
&EndDate=2018-01-01  00:00:00
&StartDate=2018-01-02  00:00:00
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"AECA76BF-1878-43C3-BC23-DDE7CF8D6111",
 "TotalCount":0,
 "SpecificCount":0,
 "SourceIpCount":0
}
```

2.16.3.9.10. DescribeThreatCountByType

Description

You can call this operation to query the number of targeted attacks detected in threat analysis by type.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeThreatCountByType*.
Distribution	String	No	The name of the region.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Threats	Array	The list of threat events. For more information, see the following parameter descriptions.
Category	Integer	The ID of the threat event type.
CategoryName	String	The name of the threat event type.
Count	Integer	The number of threat events.
Tips	String	The description of the threat event type.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeThreatCountByType
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"E0BFC426-5DE0-4834-97AF-1CE609638623",
 " Threats ":[
  {
   "Category":"WEB_SPEC",
   "CategoryName":"Targeted Web attack",
   "Count":0,
   "Tips":"We have detected a Web attack that was targeted at you. This indicates that attackers are more interested in your website than others'. They have performed malicious operations such as SQL injections, command execution, and directory scanning."
  },
  {
   "Category":"PORT_SPEC",
   "CategoryName":"Brute-force password cracking against a targeted server",
   "Count":0,
   "Tips":"We have detected a brute-force attack that attempts to crack your logon password. Attackers usually attempt to crack the passwords of random servers. This targeted attack implies that your asset is targeted by the attacker."
  }
 ]
}
```


2.16.3.9.11. DescribeThreatTop

Description

You can call this operation to query attack and threat events in the last seven days.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeThreatTop*.
Distribution	String	No	The name of the region.
Limit	Integer	Yes	The number of records to return.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
Threats	Array	The attack and threat events. For more information, see the following descriptions.
Category	String	The type of the event.
Title	String	The event description.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeThreatTop
&Limit=2
&<Common request parameters>
```

- Sample response (JSON format)

```
{
   "RequestId":"DC128D02-B262-4ACF-B233-69F50394C6C1",
   "Threats":[ {
         "title":"Web application attack against the IP address 192.168.xx.xx. Attack type: path traversal
",
         "category":"ATTACK"
      },
      {
         "title":"Web application attack against the IP address 192.168.xx.xx. Attack type: path traversal
",
         "category":"ATTACK"
      }]
}
```

2.16.3.9.12. DescribeThreatAnalyseList

Description

You can call this operation to query threat events in threat analysis.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeThreatAnalyseList*.
Distribution	String	No	The name of the region.
Limit	Integer	Yes	The number of records to return.
Start	Integer	Yes	The position of the first record to return.
Category	String	No	The category of the threat events.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
ThreatAnalyseResults	Array	The threat events. For more information, see the following descriptions.
Aliuid	Long	The ID of the Alibaba Cloud account.
Category	Integer	The ID of the main threat event category.
CategoryName	String	The name of the main threat event category.
Count	Integer	The number that indicates how many times the attack event has occurred.
StartTime	String	The time when the attack event occurred for the first time.
EndTime	String	The time when the attack event last occurred.
Id	Integer	The primary key ID.
SourceIp	String	The IP address of the attacker.
SourceLocation	String	The source area where the attack was launched.
Service	String	The cloud product.

Parameter	Type	Description
Status	Integer	Indicates whether the threat has been blocked. Valid values: • *0*: indicates that the attack has not been blocked. • *1*: indicates that the attack has been blocked.
ThreatRate	String	The threat level.
Detail	Struct	The detailed asset information. For more information, see the following descriptions.
Assets	Array	The detailed asset information. For more information, see the following descriptions.
AssetGroup	String	The asset group.
DepartmentName	String	The name of the department.
Distribution	String	The region.
HostName	String	The custom name of the asset.
Ip	String	The IP address of the asset.
Service	String	The type of the cloud product, such as RDS, ECS, or SLB.
Info	Array	The detailed attack information. For more information, see the following descriptions.
Label	String	The tag of the threat.
LinkText	String	The hyperlink of the threat details.
Type	String	The type of the threat details. Valid values: • *0*: indicates the text type. • *1*: indicates the hyperlink type.
Value	String	The threat details.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeThreatAnalyseList
&Limit=5
&Start=0
&Category=SCANNER
&<Common request parameters>
```

- Sample response (JSON format)


```
{
  "TotalCount": 22,
  "RequestId": "4D76E738-1B32-4382-A47C-CD6957D3D565",
  "ThreatAnalyseResults": [{
      "aliuid": -1,
      "assetGroup": "Default group",
      "category": "PINGBACK",
      "categoryName": "Pingback Exploit",
      "count": 27,
      "detail": {
        "assets": [{
          "assetGroup": "Default group",
          "distribution": "cn-hangzhou-env6-d01",
          "hostName": "10.36.xx.xx",
          "ip": "10.36.xx.xx",
          "product": "NAT"
        }],
        "info": [{
            "label": "Exploited Assets and Ports",
            "linkText": "",
            "type": 0,
            "value": "10.36.xx.xx:80 (10.36.xx.xx)"
          },
          {
            "label": "Exploited Servers",
            "linkText": "",
            "type": 0,
            "value": "10.36.xx.xx"
          },
          {
            "label": "Exploited Articles",
            "linkText": "",
            "type": 0,
            "value": "http://www.example.com/any_blog_post/"
```

```
            }
          ]
        },
        "distribution": "cn-hangzhou-env6-d01",
        "endTime": "2018-01-03 10:26:24",
        "id": 21,
        "sourceIp": "10.254.xx.xx",
        "sourceLocation": "Unassigned or Internal IP",
        "startTime": "2018-01-03 10:17:39",
        "status": 1,
        "threatRate": "0.4"
      }

    ]
}
```


2.16.3.9.13. DescribeHighRiskAssets

Description

You can call this operation to query high-risk assets.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeHighRiskAssets*.
Limit	Integer	Yes	The number of records to return.
Distribution	String	No	The region.
StartDate	String	No	The beginning of the time range where data is queried, in timestamp format.
EndDate	String	No	The end of the time range where data is queried, in timestamp format.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Parameter	Type	Description
TotalCount	Integer	The number of returned records.
HighRiskAssets	Array	The high-risk assets. For more information, see the following descriptions.
AssetGroup	String	The name of the asset group.
Distribution	String	The region.
HostName	String	The custom name of the asset.
NormalAttack	Integer	The number of normal attacks that the asset has received.
Special_attack	Integer	The number of targeted attacks that the asset has received.
Service	String	The asset type, such as RDS, SLB, or ECS.
Score	Integer	The risk score.
VmIp	String	The IP address of the asset.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeHighRiskAssets
&EndDate=1519886538
&Limit=10
&StartDate=1519886538
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":1,
  "RequestId":"FDE94E23-5553-447E-818C-BBE7C2EB7250",
  "HighRiskAssets":[
      {
          "Vmlp":"192.168.xx.xx",
          "Normal_attack":12,
          "Special_attack":12,
          "Score":12,
          "Asset_group":"aaa",
          "Distribution":"aaa",
          "Product":"",
          "HostName":""
      }
    ]
}
```


2.16.3.10. Asset management operations

2.16.3.10.1. DescribeDistributionByCodeType

Description

You can call this operation to query the information about all regions in Apsara Stack.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeDistributionByCodeType*.
CodeType	String	No	The code type. A value of *distribution* indicates the region.
Code	String	No	The region code.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Name	Type	Description
CodeNames	Array	The list of regions. For more information, see the following parameter descriptions.
CodeType	String	The code type. A value of *distribution* indicates the region.
Code	String	The region code.
CodeName	String	The region name.
Description	String	The region description.
GmtCreate	Long	The creation time.
GmtModified	Long	The last modification time.
Id	Integer	The region ID.
Seq	Integer	The sequence number.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeDistributionByCodeType
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"1819325E-D09A-494B-BE9C-366E9996A974",
 "CodeNames":[
  {
   "GmtCreate":1463367238000,
   "Description":"Hybrid cloud IDC list",
   "CodeName":"Daxing IDC",
   "GmtModified":1463367238000,
   "CodeType":"distribution",
   "Id":17,
   "Code":"am1",
   "Seq":1
  }
 ]
}
```

2.16.3.10.2. DescribeSystemByCodeType

Description

You can call this operation to query the information about all operating system versions used in Apsara Stack.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeSystemByCodeType*.
CodeType	String	No	The code type. The value *platform_type* indicates the operating system version.
Code	String	No	The code of the operating system version.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CodeNames	Array	The list of operating system versions. For more information, see the following parameter descriptions.
CodeType	String	The code type. The value *platform_type* indicates the operating system version.
Code	String	The code of the operating system version.
CodeName	String	The name of the operating system version.
Description	String	The description of the operating system version.
GmtCreate	Long	The creation time.
GmtModified	Long	The last modification time.
Id	Integer	The primary key ID.
Seq	Integer	The sequence number.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeSystemByCodeType
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"0391CA5F-CFEF-49F6-A2A9-D425E94397B9",
 "CodeNames":[
  {
   "GmtCreate":1463453433000,
   "Description":"Operating system type",
   "CodeName":"Windows",
   "GmtModified":1463453433000,
   "CodeType":"platform_type",
   "Id":22,
   "Code":"1",
   "Seq":2
  }
 ]
}
```

2.16.3.10.3. DescribeAssetGroup

Description

You can call this operation to query asset group details in Apsara Stack.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAssetGroup*.
Distribution	String	No	The region name.
Type	String	No	The asset type, such as *RDS*, *SLB*, or *ECS*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
AssetsGroups	Array	A list of asset group. For more information, see the following parameter descriptions.
Id	Integer	The ID of the asset group record.
GroupId	Integer	The ID of the asset group.
GroupName	String	The name of the asset group.
Group	String	The name of the asset group.
GroupIndex	Integer	The sequence number of the asset group.
Name	String	The name of the asset group.
GroupFlag	Integer	The asset group flag. Valid values: • *0*: indicates a default asset group. • *1*: indicates a custom asset group.
Count	Integer	The number of assets in the asset group.
Data	Integer	The number of assets in the asset group.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAssetGroup
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"FA5D7665-7B3D-4776-88FF-EC2F7597AE7D",
 "AssetsGroups":[
  {
   "GroupName":"Default asset group",
   "Group":"Default asset group",
   "GroupIndex":1,
   "Data": {"Data ":{
   "count" : 0,
   "id": 1,
   "GroupFlag":0,
   "Name":"Default asset group",
   "GroupId": {
  }
 ]
}
```


2.16.3.10.4. CreateNatAsset

Description

You can call this operation to add an NAT asset.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateNatAsset*.
GroupId	String	Yes	The ID of the asset group.
Group	String	Yes	The name of the asset group.
Distribution	String	No	The region.
VmIp	String	Yes	The IP address of the NAT asset.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=CreateNatAsset
&Group=Default group
&GroupId=17
&VmIp=x.x.x.x
&Distribution=cn-hangzhou-dg-a01
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"840C7302-A3CD-48B4-9B5A-7C025A946D0F"
}
```

2.16.3.10.5. ModifyRegion

Description

You can call this operation to modify the home region of an asset.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *ModifyRegion*.
AssetType	String	Yes	The name of the asset, such as the server name.
Data	String	No	The Classless Inter-Domain Routing (CIDR) block information of the asset.
Distribution	String	No	The name of the region.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=ModifyRegion
&AssetType=Server name
&Data=192.168.xx.xx/25
&Distribution=cn-hangzhou-env6-d01
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"84A27393-D0E6-4AC3-8712-478D2129CD06"
}
```

2.16.3.10.6. ModifyAssetGroup

Description

You can call this operation to modify asset group information.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyAssetGroup*.
SasGroupRequestList.N.Flag	Integer	No	The type of change that you want to make. Valid values: • *-1*: deletes an asset group. • *0*: does not make any changes. • *1*: adds an asset group.
SasGroupRequestList.N.GroupFlag	Integer	No	The asset group flag. Valid values: • *0*: indicates a default asset group. • *1*: indicates a custom asset group.
SasGroupRequestList.N.GroupId	Integer	No	The ID of the asset group.
SasGroupRequestList.N.GroupIndex	Integer	No	The sequence number of the asset group.

Name	Type	Required	Description
SasGroupRequestList.N.GroupName	String	No	The name of the asset group.
SasGroupRequestList.N.Id	Long	No	The asset group record ID.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=ModifyAssetGroup
&SasGroupRequestList. 1. Flag=-1
&SasGroupRequestList. 1. GroupFlag=1
&SasGroupRequestList. 1. GroupId=1
&SasGroupRequestList. 1. GroupIndex=1
&SasGroupRequestList. 1. GroupName=test
&SasGroupRequestList. 1. Id=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"65ED9921-1A37-4362-9051-F467AF58CB69"
}
```

2.16.3.10.7. ModifyGroup

Description

You can call this operation to modify the home group of an asset.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *ModifyGroup*.
AssetType	String	Yes	The name of the asset, such as the server name.
Data	String	No	The Classless Inter-Domain Routing (CIDR) block information of the asset.
Group	String	Yes	The name of the asset group.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=ModifyGroup
&AssetType=Server name
&Data=192.168.xx.xx/25
&Group=Default group
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"84A27393-D0E6-4AC3-8712-478D2129CD06"
}
```

2.16.3.10.8. ModifyAsset

Description

You can call this operation to modify asset information.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyAsset*.
Id	String	Yes	The ID of the asset record.
GroupId	String	No	The ID of the asset group.
Distribution	String	No	The name of the region.
Group	String	No	The name of the asset group.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=ModifyAsset
&Group=Default group
&GroupId=17
&Id=123
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"84A27393-D0E6-4AC3-8712-478D2129CD06"
}
```

2.16.3.10.9. DescribeTotalAssetNumber

Description

You can call this operation to query the total number of assets.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeTotalAssetNumber*.
Distribution	String	No	The name of the region.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalAssetNumber	Array	The list of assets. For more information, see the following parameter descriptions.
Count	Integer	The total number of assets.
HostCount	Integer	The total number of servers.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeTotalAssetNumber
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"76842928-BB88-4007-8F27-23E17250AC6E",
 "TotalAssetNumber":{
  "HostCount":0,
  "Count":0
 }
}
```

2.16.3.10.10. DescribeAllDistribution

Description

You can call this operation to query the percentages of assets in different regions in Apsara Stack.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAllDistribution*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
RegionDatas	Array	The percentages of assets in different regions. For more information, see the following parameter descriptions.
Name	String	The name of the region.
Data	String	The percentage of the assets in the region.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAllDistribution
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"DE2595A0-AC52-47F1-84D9-D3383E933AD4",
 "RegionDatas":[
  {
          "name":"Unknown",
          "data":44.21
      },
      {
          "name":"cn-hangzhou-env6-d01",
          "data":55.79
      }
   ]
}
```


2.16.3.10.11. DescribeAssetsList

Description

You can call this operation to query assets.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeAssetsList*.
Size	Integer	Yes	The number of records to return.
Start	Integer	Yes	The position of the first record to return.
Distribution	String	No	The name of the region.
GroupName	String	No	The name of the asset group.
Platform	String	No	The operating system of the asset.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.

Parameter	Type	Description
SasAssets	Array	The assets. For more information, see the following descriptions.
ActiveTime	String	The time when the asset was enabled.
AegisStatus	Integer	The status of Server Guard on the asset.
Aliuid	String	The ID of the Alibaba Cloud account.
AssetType	String	The type of the asset, such as RDS, SLB, or ECS.
DataSource	Integer	The data source. Valid values: • *1*: indicates Server Guard. • *2*: indicates a custom data source. • *3*: indicates a cloud platform. • *4*: indicates Apsara Stack Security.
DepartmentName	String	The name of the department.
Distribution	String	The name of the region.
Event	Integer	The number of security events.
GmtCreate	String	The time when the asset record was created.
GmtModified	String	The time when the asset record was last modified.
Group	String	The name of the asset group.
GroupId	Integer	The ID of the asset group.
HostName	String	The custom name of the asset.
Id	Integer	The ID of the asset record.
Platform	String	The operating system.
Region	String	The name of the region.
Software	List	The application information.
Status	Integer	The status of the asset. Valid values: • *0*: indicates that the asset is disabled. • *1*: indicates that the asset is enabled.
Threat	Integer	The number of threat events.
Uuid	String	The universally unique identifier (UUID) of the asset.

Parameter	Type	Description
VmIp	String	The IP address of the asset.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAssetsList
&GroupName=1
&Platform=Linux/CentOS release 6.8 (Final)/null
&Size=10
&Start=0
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount": 0,
  "RequestId": "B78FD9E9-3ED5-4D8D-A716-F2F482BCBD4F",
  "SasAssets": [{
    "activeTime": "2018-02-13 09:28:56",
    "aegisStatus": 0,
    "aliuid": 143841340822****,
    "assetType": "Server",
    "dataSource": 1,
    "departmentName": "R&D",
    "distribution": "cn-hangzhou-env6-d01",
    "event": 0,
    "gmtCreate": "2018-02-06 15:04:43",
    "gmtModified": "2018-02-13 11:05:00",
    "group": "Default group",
    "groupId": 17,
    "hostName": "iZys605x4c311svakg2****",
    "id": 6945310,
    "platform": "Linux/CentOS release 5.11 (Final)/2.6.18-418.el5",
    "region": "cn-hangzhou-env6-d01",
    "software": [],
    "status": 1,
    "threat": 0,
    "uuid": "012613c2-f116-4a20-8ef8-1a19989c****",
    "vmIp": "192.168.xx.xx"
  }]
}
```


2.16.3.10.12. DescribeUuidIpList

Description

You can call this operation to query the IP address of a specified asset based on the universally unique identifier (UUID) of the asset.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeUuidIpList*.

Parameter	Type	Required	Description
Uuid	Integer	Yes	The UUID of the asset.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
IPs	String	The IP address of the asset.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeUuidIpList
&Uuid=121asdf4545ads****
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"737E5F87-6892-4711-BF00-BEBD0B2E1E03",
  "Ips":"192.168.xx.xx"
}
```

2.16.3.10.13. DescribeIpList

Description

You can call this operation to obtain a list of asset IP addresses based on keywords.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeIpList*.
Size	Integer	Yes	The number of returned records.
Keyword	String	No	The query keyword.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
IPs	List	The IP address list.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeIpList
&Size=1
&Keyword=0
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"F3A98AE4-BC02-421A-854E-198837ACEDF9",
 "IPs":["x.x.x.x"]
}
```

2.16.3.10.14. DescribePortList

Description

You can call this operation to query ports of the server with a specified IP address.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribePortList*.
Limit	Integer	Yes	The number of records to return.
Start	Integer	Yes	The position of the first record to return.
Ip	String	Yes	The IP address.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
HostPorts	Array	The ports. For more information, see the following descriptions.
FirstDetectTime	Long	The time when the port was detected for the first time.
LastDetectTime	Long	The time when the port was last detected.
Port	Integer	The port number.
Protocol	String	The protocol.
Service	String	The service provided by the port.
TodayVul	Integer	The number of ports enabled on the current day.
Version	String	The name and version of the application.
YesterdayVul	Integer	The number of ports enabled on the last day.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribePortList
&Ip=192.168.xx.xx
&Limit=5
&Start=1
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":0,
  "RequestId":"7F25EA4D-ABC4-47C6-8134-B23230E3BF67",
  "HostPorts":[
    {
      "firstDetectTime": 1519713424712,
      "lastDetectTime": 1519713424712,
      "port": 11,
      "protocol": "ftp",
      "service": "test",
      "status": 0,
      "todayVul": 0,
      "version": "1",
      "yesterdayVul": 0
    }
  ]
}
```


2.16.3.10.15. DescribeThisMonthAssets

Description

You can call this operation to query the number of new assets added in the last 30 days.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeThisMonthAssets*.
Distribution	String	No	The name of the region.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Count	Integer	The number of new assets.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeThisMonthAssets
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId":"E1668C9C-1301-4F93-9C20-8886A1A66A33",
  "Count":0
}
```

2.16.3.10.16. DescribeAssetsTotalCount

Description

You can call this operation to query the chart data on the total number of assets in the last seven days.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAssetsTotalCount*.
Distribution	String	No	The name of the region.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TimeScope	Struct	The time frame during which the data is collected and returned. For more information, see the following parameter descriptions.
Interval	Integer	The time length of the time frame during which the data is collected.
Start	Long	The start time of the time frame during which the data is collected.

Name	Type	Description
LineBars	Array	The asset quantity statistics. For more information, see the following parameter descriptions.
Name	String	The type of the asset, such as server or NAT.
Data	List	The total number of assets.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAssetsTotalCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"9954A060-03F4-4C3C-BCE0-F761F4330E30",
 "LineBars":[
  {
          "data":[
            487,
            690
          ],
          "name":"Server"
        },
        {
          "data":[
            91,
            91
          ],
          "name":"NAT"
        }
 ],
 "TimeScope":{
}
```

2.16.3.10.17. DeleteAsset

Description

You can call this operation to delete asset information.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteAsset*.
Uuid	String	Yes	The asset UUID.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DeleteAsset
&Uuid=d6613b93-1219-41d7-9d21-5c9a5b96d97e
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"840C7302-A3CD-48B4-9B5A-7C025A946D0F"
}
```

2.16.3.11. Alerting setting operations

2.16.3.11.1. CreateContact

Description

You can call this operation to add an alert contact.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *CreateContact*.
Id	Long	No	The ID of the alert contact.
Name	String	Yes	The name of the alert contact.
Email	String	Yes	The email address of the alert contact.
Mp	String	Yes	The mobile number of the alert contact.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=CreateContact
&Email=someone@example.com
&Mp=1300000****
&Name=<yourName>
&Id=123
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"840C7302-A3CD-48B4-9B5A-7C025A946D0F"
}
```

2.16.3.11.2. DescribeContactsList

Description

You can call this operation to query alert contacts.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeContactsList*.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The total number of records.
ContactsList	Array	The alert contacts. For more information, see the following descriptions.
Email	String	The email address of the alert contact.
Id	Integer	The ID of the alert contact.
Mp	String	The mobile number of the alert contact.
Name	String	The name of the alert contact.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeContactsList
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"D47D0CE4-B0FB-450D-B4B6-DB99824ADA0E",
  "Total":5,
  "ContactsList":[
    {
      "mp":"1300000****",
      "name":"test",
      "id":3,
      "email":"someone1@example.com"
    },
    {
      "mp":"1500000****",
      "name":"test",
      "id":4,
      "email":"someone2@example.com"
    }
  ]
}
```


2.16.3.11.3. ModifyContact

Description

You can call this operation to modify alert contacts.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *ModifyContact*.
Id	Integer	Yes	The ID of the alert contact.
Email	String	Yes	The email address of the alert contact.
Mp	String	Yes	The mobile number of the alert contact.
Name	String	Yes	The name of the alert contact.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://sasprivate.[ RegionId].example.com/?Action=ModifyContact
&Email=someone@example.com
&Id=123
&Mp=1300000****
&Name=John Smith
&<Common request parameters>
```

- Sample response (JSON format)

```
{
   "RequestId":"D47D0CE4-B0FB-450D-B4B6-DB99824ADA0E",
}
```

2.16.3.11.4. DeleteContact

Description

You can call this operation to delete an alert recipient.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteContact*.
Id	Long	Yes	The ID of the alert recipient.
Name	String	No	The name of the alert recipient.
Email	String	No	The email address of the alert recipient.
Mp	String	No	The mobile number of the alert recipient.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DeleteContact
&Id=123
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"840C7302-A3CD-48B4-9B5A-7C025A946D0F"
}
```

2.16.3.11.5. DescribeAlarmConfig

Description

You can call this operation to query the alert settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAlarmConfig*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of records.
AlarmConfigs	Array	The alert configuration information. For more information, see the following parameter descriptions.

Name	Type	Description
Id	Integer	The alert configuration record ID.
Category	Integer	The alert type. Valid values: • *1*: indicates a security event. • *2*: indicates a security threat.
Email	Boolean	Indicates whether to send a notification to the recipient's email address.
Mp	Boolean	Indicates whether to send a notification to the recipient's mobile phone.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeAlarmConfig
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"49A3041D-4FEC-42E5-9AE4-A2E5AD57CFDB",
 "Total":18,
 "AlarmConfigs":[
  {
   "mp":true,
   "id":1,
   "category":1,
   "email":true
  },
  {
   "mp":true,
   "id":2,
   "category":1,
   "email":true
  }
 ]
}
```

2.16.3.11.6. ModifyAlarmConfig

Description

You can call this operation to modify alert settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyAlarmConfig*.
Config	Struct	Yes	The modified alert settings in JSON format. For more information, see the following parameter descriptions.
Id	Integer	Yes	The alert setting record ID.
Title	String	Yes	The name of the alert.
Category	Integer	Yes	The type of the alert. Valid values: • *1*: indicates a security event. • *2*: indicates a threat.
Mp	Boolean	Yes	Indicates whether to send SMS notifications to alert the recipients.
Email	Boolean	Yes	Indicates whether to send emails to alert the recipients.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=ModifyAlarmConfig
&Config=[{"id":20,"title":"Logon security - remote logon","category":2,"mp":true,"email":true},{"id":1,"title":"Website tampering","category":1,"mp":true,"email":true},{"id":2,"title":"Bot behavior","category":1}]
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"49A3041D-4FEC-42E5-9AE4-A2E5AD57CFDB",
 "Total":18,
 "AlarmConfigs":[
  {
   "mp":true,
   "id": 1,
   "category":1,
   "email":true
  },
  {
   "mp":true,
   "Id":2,
   "category":1,
   "email":true
  }
 ]
}
```

2.16.3.11.7. DescribeReadStatus

Description

You can call this operation to query the number of unread alert messages.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeReadStatus*.
Distribution	String	No	The region.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
ReadStatus	Array	The information about unread alert messages. For more information, see the following parameter descriptions.
Type	String	The type of the unread alert message.
UnReadCount	Integer	The number of unread alert messages.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://sasprivate.[ RegionId].example.com/?Action=DescribeReadStatus
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"CFB09A1B-2653-40F7-A2E8-77C65D9C9732",
 "ReadStatus":[
  {
   "Type":"SECURITY_EVENT",
   "UnReadCount":0
  },
  {
   "Type":"APPLICATION_VULNERABILITY",
   "UnReadCount":0
  }
 ]
}
```

2.16.4. Server Guard

2.16.4.1. List of operations

This topic introduces all the Server Guard operations that you can call. For more information, see the corresponding operation description.

Asset management operations

Operation	Description
CreateGroup	Creates an asset group.
DescribeGroupSummary	Obtains a list of asset groups.
DescribeGroupStruct	Queries the structure of an asset group.
DeleteGroup	Deletes an asset group.
DescribeAllTag	Queries the tag information of all servers.
DescribeBetachTag	Queries the tag information of a specified server.
ModifyBetachTag	Modifies the tags of multiple specified servers.
DeleteTag	Deletes the tag of a server.
DescribeAllEntity	Queries information about all servers.
DescribeEntityList	Queries a type of servers.
ModifyEntityGroup	Modifies the asset group information for a specified server.
DescribeMachines	Queries servers that match the specified criteria.
DescribeMachineDetail	Queries the detailed information about the specified server.
DescribePropertyScheduleConfig	Queries the update cycle of server information.
ModifyPropertyScheduleConfig	Modifies the synchronization cycle of host asset information.
DescribePropertyStatistic	Queries server statistics.
DescribePropertyPortItem	Obtains a list of listener ports on servers.
DescribePropertyPortDetail	Queries detailed listening port information.
DescribePropertyPortDiff	Queries listening port changes.
DescribePropertyProcItem	Obtains a list of server processes.
DescribePropertyProcDetail	Queries server process details.
DescribePropertyProcDiff	Queries process changes of servers.
DescribePropertySoftwareItem	Queries servers that have been installed with the specified application.
DescribePropertySoftwareDetail	Obtains the details of application software installed on a server.

Operation	Description
DescribePropertySoftwareDiff	Queries changes of applications that have been installed on servers.
DescribePropertyUserItem	Queries user account information.
DescribePropertyUserDetail	Queries user account details.
DescribePropertyUserDiff	Queries user account changes.
PushAllTask	Performs a quick security check on specified servers.
DescribeTopRiskyAssets	Obtains a list of top N vulnerable servers.
UnbindAegis	Disables Server Guard for a specified server.
UninstallAegis	Uninstalls the Server Guard client from a specified server.

Vulnerability management operations

Operation	Description
DescribeTarget	Queries the servers that are checked for the specified type of risks in vulnerability management.
ModifyVulTarget	Modifies the servers for detecting a specified type of vulnerability in the vulnerability management settings.
DescribeVulTargetStatistics	Queries the information about target hosts for which vulnerability detection is enabled in the vulnerability management configuration.
DescribeTargetConfig	Queries the vulnerability scanning configuration information of a specified server.
ModifyTargetConfig	Modifies the vulnerability scanning configuration for a specified server.
DescribeVulConfig	Queries the global scanning configuration for each vulnerability type.
ModifyVulConfig	Modifies the global vulnerability scanning configuration.
DescribeAutoDelConfig	Queries the number of days that an invalid vulnerability is kept for before it is automatically deleted in the vulnerability management settings.
ModifyAutoDelConfig	Modifies the number of days that an invalid vulnerability is kept for before it is automatically deleted in the vulnerability management settings.

Operation	Description
DescribeVulLevel	Queries the vulnerability severities that require attention.
ModifyVulLevel	Changes the vulnerability severities that require attention.
CreateVulWhitelist	Adds a specified vulnerability to the whitelist.
DescribeVulWhitelist	Obtains the whitelist of vulnerabilities.
DeleteVulWhitelist	Deletes a specified vulnerability from the vulnerability whitelist.
DescribeGroupedVul	Queries information about the specified vulnerability group.
DescribeVulList	Obtains a list of application vulnerabilities.
DescribeVulDetails	Queries detailed information about a vulnerability.
DescribeVulNumStatistics	Queries vulnerability statistics.
DescribeVulLevelStatistics	Obtains the statistics on vulnerabilities by vulnerability severity.
DescribeVulMachineList	Queries the vulnerability statistics of a specified server.
OperateVul	Handles detected vulnerabilities.
ModifyBatchIgnoreVul	Ignores multiple vulnerabilities.
DeleteVulBatch	Deletes a specified batch of vulnerabilities.
ExportVul	Exports vulnerability records that match the specified criteria.
DescribeVulExportInfo	Queries the information about vulnerability record export tasks.

Baseline check operations

Operation	Description
DescribeStrategy	Obtains a list of baseline check policies.
DescribeStratetyDetail	Queries the details of a specified baseline check policy.
ModifyStrategy	Modifies the basic information of a baseline check policy.
DeleteStrategy	Deletes a specified baseline check policy.
DescribeStrategyTarget	Queries the information about asset groups to which a specified baseline check policy applies.

Operation	Description
ModifyStrategyTarget	Modifies the information about the asset groups that a specified baseline check policy applies to.
DescribeUuidConfig	Checks whether baseline check is enabled for a specified server.
ModifyMachineConfig	Configures whether to apply a specified baseline check policy to a specified server.
DescribeUserSetting	Queries the number of days an invalid risk is kept for before it is automatically deleted in baseline check.
CreateUserSetting	Specifies the number of days an invalid risk is kept for before it is automatically deleted in baseline check.
DescribeRiskWhiteList	Obtains the whitelist of risk items that are exempt from the baseline check.
BatchDeleteWhiteList	Deletes multiple risks from the whitelist for baseline check.
CreateUserWhiteList	Adds a specified risk to the baseline check whitelist.
DescribeStratety	Queries the execution details of a specified baseline check policy.
DescribeStrategyExecDetail	Queries the execution details of a baseline check policy.
DescribeRiskType	Queries all types of risks detected in baseline check and view the number of risks that have been detected by a baseline check policy or on the specified servers for a specific risk type.
Describesummary	Queries the risks detected in baseline check by risk type.
OperateWarning	Handles the risk alert records detected during the baseline check.
ExportWarning	Exports risks that match the specified criteria from baseline check.
DescribeExportInfo	Queries export task information, including the export progress and the download link of the exported file.

Unusual logon detection operations

Operation	Description
DescribeBaseConfigs	Queries the logon security settings.

Operation	Description
ModifyBaseConfig	Modifies logon security settings.
DeleteBaseConfig	Deletes a logon security setting, such as an approved logon location or IP address.
DescribeSwitchConfigs	Queries the logon security configuration records in the logon security settings.
ModifySwitchConfig	Modifies the setting about whether to enable a logon security configuration record to identify a valid logon to a host in the logon security settings.
DescribeConfigTarget	Queries the information about host assets to which a specified logon security configuration record applies.

Webshell detection operations

Operation	Description
DescribeWebPath	Queries the Web directories defined in webshell settings.
ModifyWebPath	Modifies the Web directory in webshell settings.
DescribeCategoryCount	Queries the number of webshells detected by Server Guard.
DescribeWebshell	Queries records of webshell files that have been detected by Server Guard, including the detection time and webshell file path.
OperateTrojan	Handles the detected webshells.
DescribeQuaraFile	Obtains a list of quarantined files.
RollbackQuaraFile	Restores a quarantined file.

Suspicious server detection operations

Operation	Description
DescribeSuspEventTypes	Queries the unusual event types.
DescribeSuspTrendStatistics	Queries the chart data on different types of unusual server events on each day.
OperateSuspiciousEvent	Handles detected unusual events.
OperateLoginLog	Labels a detected unusual logon event as handled.

Operation	Description
CreateSuspiciousExport	Exports the information about server unusual events based on search conditions.
DescribeSuspiciousExportInfo	Queries an unusual event export task.

Server log retrieval operations

Operation	Description
CreateLogQuery	Creates or saves server log search conditions.
DescribeLogQuery	Queries the saved server log search conditions.
DeleteLogQuery	Deletes the saved server log search conditions.
DescribeFilterFields	Queries the filter fields of a specified server log search condition.
DescribeHistogram	Obtains the statistics on server logs generated within a specified time frame.
DescribeLogInfo	Queries the host log fields based on specified query conditions.
DescribeLogItems	Queries the server log details that are returned by a query.

2.16.4.2. Make API requests

2.16.4.2.1. Request structure

Apsara Stack Security API is based on Remote Procedure Call (RPC). This topic describes the structure of the API requests.

Description

You can send an HTTP request to call an API operation. The URL of the request must be in the following format:

```
http://endpoint/?Action=xx&parameters
```

Where:

- `endpoint`: the endpoint used to call a cloud service. The endpoint for the Server Guard service is `aegis.[ RegionId].example.com`.
- `Action`: the operation that you want to perform.

  For example, you can set this parameter to DescribeFeatures to query the deployed Apsara Stack Security features.

- `parameters`: the request parameters. Request parameters include common request parameters and custom request parameters. Request parameters must be separated with ampersands (&).
  - Common request parameters include information such as the API version and authentication information.
  - For more information about the custom request parameters, see the corresponding operation description.

Example

Call the DescribeFeatures operation to query the deployed Apsara Stack Security features.

```
https://yundunprivate.[ RegionId].example.com/?Action=DescribeFeatures&AccessKeyId=key-test&Format=JSON&SecureTransport=true&SignatureMethod=HMAC-SHA1&SignatureNonce=15215528852396&SignatureVersion=1.0&SourceIp=1xxxx6&Timestamp=2018-03-02Txxxxxxx&Version=2018-01-16&Signature=xxxx%xxxx%3D
```

API requests are presented in the following easy-to-read format in this document:

```
https://yundunprivate.[ RegionId].example.com/?Action=DescribeFeatures
&Format=JSON
&Version=2018-01-16
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2012-06-01T12:00:00Z
```

2.16.4.2.2. Signature mechanism

Apsara Stack Security authenticates each access request. You need to include a signature for the submitted HTTP or HTTPS request.

API authorization

To ensure the security of your account, we recommend that you use a Resource Access Management (RAM) user to call API operations. Before using a RAM user to call an API operation, you must grant the RAM user the corresponding permission to call the API by creating an authorization policy and attaching the policy to the RAM user.

API signature

To ensure secure calls to the API, Alibaba Cloud authenticates each API request through the signature. When you manually make an API request, you need to use AccessKey Secret to calculate the signature, that is, the hash-based message authentication code (HMAC) value, based on the encoded and sorted request string. For more information, see the definition in RFC 2104.

This topic uses the raw access parameters in the following table to describe how to create an API signature.

Parameter	Description
Access point	http://yundunprivate.[RegionId].example.com/?
API-specific parameters	Action=DescribeFeatures
Common parameters (excluding the Signature parameter)	&Timestamp=2016-02-23T12:46:24Z &Format=JSON &AccessKeyId=<yourAccessKeyId> &SignatureMethod=HMAC-SHA1 &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf &Version=2018-01-16 &SignatureVersion=1.0
AccessKey secret	<yourAccessKeySecret>

1. Use the request parameters to construct a canonicalized query string.

   Note The request parameters include common request parameters (excluding the Signature parameter) and API-specific parameters.

   i. Sort the parameters.

   Sort the request parameters in alphabetical order.

   ii. Encode the parameters.

   Use UTF-8 to URL-encode the parameter names and values. The encoding rules are as follows:

   - Letters, digits, hyphens (-), underscores (_), periods (.), and tildes (~) are not encoded.
   - Other characters are encoded in the %XY format, where XY is the hexadecimal representation of the character in ASCII. For example, the double quotation mark (") is encoded as %22.
   - Extended UTF-8 characters are encoded in the %XY%ZA... format.
   - Note that a space is encoded as %20, instead of a plus sign (+).

   iii. Connect the encoded parameter names and values with equal signs (=).

   iv. Then, sort the parameter name and value pairs connected by equal signs in alphabetical order, and connect them with ampersands (&) to produce the canonicalized query string.

2. Use the canonicalized query string to construct the string for signature calculation based on the following rules:

```
StringToSign=HTTPMethod + “&” + percentEncode( “/” ) + ” &” +
percentEncode(CanonicalizedQueryString)
```

3. Calculate the HMAC value of the StringToSign string according to the definition in RFC 2104.

   > **Note** The key used for signature calculation is your AccessKey secret adding the ampersand (&) (ASCII 38). Secure Hash Algorithm 1 (SHA1) is used as the hash algorithm.

4. Encode the preceding HMAC value into a string based on Base64 encoding rules to obtain the signature value.

   ```
   LEW8N4y7Uasop******
   ```

5. Set the Signature parameter in the request parameters to this signature value to sign the request.

2.16.4.2.3. Common request parameters

The following table describes the common request parameters that are used to indicate information such as the API version and authentication information.

Name	Type	Required	Description
Version	String	Yes	The API version in the format of YYYY-MM-DD. Set the value to *2016-11-11*.
AccessKeyId	String	Yes	The key ID that Alibaba Cloud assigns to a user for service access.
Signature	String	Yes	The signature string.
SignatureMethod	String	Yes	The signature method. Set the value to *HMAC-SHA1*.
Timestamp	String	Yes	The timestamp of the request. Follow the ISO 8601 standard to specify the date and use the offset from Coordinated Universal Time (UTC) to specify the time zone. The format is `YYYY-MM-DDThh:mm:ssZ`. For example, 2014-05-26T12:00:00Z indicates 20:00:00 on May 26, 2014, Beijing time.
SignatureVersion	String	Yes	The signature algorithm version. Set the value to *1.0*.

Name	Type	Required	Description
SignatureNonce	String	Yes	The unique random number used to prevent network replay attacks. You must use different random numbers for different requests.
ResourceOwnerAccount	String	No	The owner account of the resource to be accessed through this API request, that is, the logon username.
Format	String	No	The format of the response. Set the value to *JSON or XML*. Note Default value: XML.

2.16.4.2.4. Response structure

Apsara Stack Security API responses support both the XML and JSON formats. The system always returns a unique identification code RequestId each time you send a request to call an operation, no matter whether the call is successful or not.

Sample responses (XML format)

```
<? xml version="1.0" encoding="UTF-8"? >
<! -- The root node of the result -->
<Operation name+Response>
   <! -- Returned request ID -->
   <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
   <! -- Returned data -->
</Operation name+Response>
```

Sample responses (JSON format)

```
{
"RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
/* Returned data */
}
```

2.16.4.3. Asset management operations

2.16.4.3.1. CreateGroup

Description

You can call this operation to create an asset group.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateGroup*.
GroupFather	Long	Yes	The parent asset group ID.
GroupFlag	Integer	Yes	The asset group type. Valid values: • *0*: indicates a default group. • *1*: indicates a custom group.
GroupIndex	Integer	Yes	The sequence number of the asset group.
GroupName	String	Yes	The name of the asset group.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=CreateGroup
&GroupFather=0
&GroupFlag=1
&GroupIndex=1
&GroupName=Web group
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"415AE1FC-3C11-4AA9-A06F-DE13D3430366"
}
```

2.16.4.3.2. DescribeGroupSummary

Description

You can call this operation to obtain a list of asset groups.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeGroupSummary*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Count	Integer	The number of asset groups.
Groups	List	The information about asset groups. For more information, see the following parameter descriptions.
GroupId	Long	The asset group ID.
GroupIndex	Integer	The sequence number of the asset group.
GroupLevel	Integer	The level of the asset group.
GroupName	String	The name of the asset group.
GroupFather	Integer	The ID of the parent asset group.
GroupFlag	Integer	The type of the asset group. Valid values: • *1*: indicates a non-leaf node group that contains child asset groups. • *0*: indicates a leaf node group.
MachineNum	Integer	The number of ECS instances contained in the group.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeGroupSummary
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "Groups":[
  {
   "GroupFlag":1,
   "GroupName":"Test group 21",
   "GroupIndex":1,
   "MachineNum":0,
   "GroupId":346
  },
  {
   "GroupFlag":1,
   "GroupName":"Test group 1",
   "GroupIndex":2,
   "MachineNum":0,
   "GroupId":343
  },
  {
   "GroupFlag":1,
   "GroupName":"Test group 2",
   "GroupIndex":3,
   "MachineNum":0,
   "GroupId":345
  },
  {
   "GroupFlag":0,
   "GroupName":"Not grouped",
   "GroupIndex":100,
   "MachineNum":1,
   "GroupId":336
  }
 ],
 "Count":4,
 "RequestId":"B9FB5483-3CA6-4520-9F89-068ED6AAC6EE"
}
```

2.16.4.3.3. DescribeGroupStruct

Description

You can call this operation to query the asset group structure.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeGroupStruct*.
Mark	String	No	The IP address or instance name of the server.
TagIdList	String	No	The server tag ID.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
GroupFather	Integer	The ID of the parent asset group.
GroupId	Long	The ID of the asset group.
Groups	List	The asset groups. For more information, see the following descriptions.
GroupId	Long	The ID of the asset group.
GroupIndex	Integer	The sequence number of the asset group.
GroupLevel	Integer	The level of the asset group.
GroupName	String	The name of the asset group.
GroupFather	Integer	The ID of the parent asset group.
GroupFlag	Integer	The type of the asset group. Valid values: • *1*: indicates a non-leaf node group that contains child asset groups. • *0*: indicates a leaf node group.
ChildGroups	List	The child asset groups.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeGroupStruct
&remark=x.x.x.x
&tagIdList=123
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "Groups":[
    {
      "groupIndex":2,
      "groupFather":0,
      "groupId":343,
      "groupName":"****",
      "groupLevel":1,
      "groupFlag":1,
      "childGroups":[]
    },
    {
      "groupIndex":3,
      "groupFather":0,
      "groupId":345,
      "groupName":"****",
      "groupLevel":1,
      "groupFlag":1,
      "childGroups":[
        {
          "groupIndex":1,
          "groupFather":345,
          "groupId":346,
          "groupName":"****",
          "groupLevel":2,
          "groupFlag":1,
          "childGroups":[]
        }
      ]
    },
    {
```

```
            "groupIndex":100,
            "groupFather":0,
            "groupId":336,
            "groupName":"****",
            "groupFlag":0,
            "childGroups":[]
        }
    ],
    "RequestId":"C4490A16-DDE4-4351-A366-57F9FCDC188F",
    "GroupFather":0,
    "GroupId":0
}
```


2.16.4.3.4. DeleteGroup

Description

You can call this operation to delete a specified asset group.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteGroup*.
GroupFlag	Integer	Yes	The type of the asset group. Valid values: • *0*: indicates a default group. • *1*: indicates a custom group.
GroupId	Long	Yes	The ID of the asset group.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DeleteGroup
&GroupFlag=1
&GroupId=123
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"415AE1FC-3C11-4AA9-A06F-DE13D3430366"
}
```

2.16.4.3.5. DescribeAllTag

Description

You can call this operation to query the tag information of all servers.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAllTag*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
EntityList	Array	The tag information of all servers. For more information, see the following parameter descriptions.
AliUid	Long	The Alibaba Cloud account ID.
GmtCreate	Long	The creation time of the asset tag.
GmtModified	Long	The last modification time of the asset tag.
Id	Long	The ID of the asset tag.
TagName	String	The name of the asset tag.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeAllTag
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"09D7C349-5306-4335-849A-10916F89E769",
 "EntityList":[
  {
   "AliUid":"123",
   "GmtCreate":"1508897933000",
   "GmtModified":"1508897933000",
   "Id":"1",
   "TagName":"test"
  },
 ]
}
```

2.16.4.3.6. DescribeBetachTag

Description

You can call this operation to query the tag information of a specified server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeBetachTag*.
UuidList	String	No	The UUID of the server.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Name	Type	Description
TagInfoList	Array	The tag information of the specified server. For more information, see the following parameter descriptions.
AliUid	Long	The Alibaba Cloud account ID.
GmtCreate	Long	The creation time of the asset tag.
GmtModified	Long	The last modification time of the asset tag.
Id	Long	The ID of the asset tag.
TagName	String	The name of the asset tag.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeBetachTag
&UuidList=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"09D7C349-5306-4335-849A-10916F89E769",
 "EntityList":[
  {
   "AliUid":"123",
   "GmtCreate":"1508897933000",
   "GmtModified":"1508897933000",
   "Id":"1",
   "TagName":"test"
  },
 ]
}
```

2.16.4.3.7. ModifyBetachTag

Description

You can call this operation to modify the tags of multiple specified servers.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyBetachTag*.
TagList	String	Yes	The server tag. Separate multiple tags with commas (,).
UuidList	String	Yes	The UUID of the server.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyBetachTag
&UuidList=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818
&TagList=test,test2
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"09D7C349-5306-4335-849A-10916F89E769",
}
```

2.16.4.3.8. DeleteTag

Description

You can call this operation to delete a server tag.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteTag*.
Id	Long	No	The ID of the server tag.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DeleteTag
&Id=123
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"415AE1FC-3C11-4AA9-A06F-DE13D3430366"
}
```

2.16.4.3.9. DescribeAllEntity

Description

You can call this operation to query information about all servers.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeAllEntity*.
GroupId	Long	No	The ID of the asset group.

Parameter	Type	Required	Description
Os	String	No	The operating system of the server. Valid values: • *win*: indicates the Windows operating system. • *linux*: indicates the Linux operating system.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
Count	Integer	The number of returned records.
EntityList	Array	The servers. For more information, see the following descriptions.
GroupId	Integer	The ID of the asset group.
Uuid	String	The universally unique identifier (UUID) of the server.
InstanceName	String	The instance name of the server.
Ip	String	The IP address of the server. Note The public IP address of the server is displayed preferentially. If no public IP address is assigned to the server, the private IP address of the server is displayed.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeAllEntity
&GroupId=123
&Os=win
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "Count":2,
  "RequestId":"09D7C349-5306-4335-849A-10916F89E769",
  "EntityList":[
    {
      "Uuid":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818",
      "Ip":"x.x.x.x",
      "GroupId":336,
      "InstanceName":"****"
    },
    ......
  ]
}
```


2.16.4.3.10. DescribeEntityList

Description

You can call this operation to query servers of a specified type. For example, you can query servers by security event type.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeEntityList*.
PageSize	Integer	No	The number of records to return on each page. Default value: *20*.
CurrentPage	Integer	No	The number of the page to return. Default value: *1*.
RegionNo	String	No	The ID of the region.
GroupId	Long	No	The ID of the asset group.

Parameter	Type	Required	Description
Os	String	No	The operating system of the server. Valid values: • *win*: indicates the Windows operating system. • *linux*: indicates the Linux operating system.
Account	String	No	Queries servers with unusual logons detected. Set this parameter to *remoteLogin*.
Health	String	No	Queries servers with baseline check issues detected. Set this parameter to *exception*.
Patch	String	No	Queries servers with vulnerabilities detected. Set this parameter to *vul*.
Suspicious	String	No	Queries servers with unusual events detected. Set this parameter to *exception*.
Trojan	String	No	Queries servers with webshells detected. Valid values: • *webshell*: indicates trojan files. • *process*: indicates trojan processes.
Status	String	No	The status of the Server Guard Agent. Valid values: • *offline*: indicates that the Server Guard Agent is offline. • *pause*: indicates that the Server Guard Agent is disabled.
TagIdList	String	No	The server tag ID.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The number of the current page returned.

Parameter	Type	Description
PageSize	Integer	The number of records returned on each page.
TotalCount	Integer	The number of returned records.
EntityList	Array	The servers. For more information, see the following descriptions.
AegisOnline	Boolean	Indicates whether the Server Guard Agent is online.
AegisVersion	String	The version of the Server Guard Agent.
BuyVersion	String	The version of the Server Guard package.
GroupId	Integer	The ID of the asset group.
ClientStatus	Boolean	Indicates whether the server is protected. A value of false indicates that the protection for the server is paused.
Flag	Integer	The type of the server. Valid values: • *0*: indicates an Alibaba Cloud ECS instance. • *1*: indicates an external server.
Uuid	String	The universally unique identifier (UUID) of the server.
InstanceName	String	The instance name of the server.
Os	String	The type of the operating system.
Region	String	The ID of the region.
Ip	String	The IP address of the server. Note The public IP address of the server is displayed preferentially. If no public IP address is assigned to the server, the private IP address of the server is displayed.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeEntityList
&Account=remoteLogin
&CurrentPage=1
&GroupId=1
&Health=exception
&Os=windows
&PageSize=20
&Patch=vul
&RegionNo=****
&Remark=x.x.x.x
&Status=offline
&Suspicious=exception
&TagIdList=1,2,3
&Trojan=webshell
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":1,
  "PageSize":1,
  "RequestId":"8BFB5273-6582-446A-9E0B-BAC0A1A468EA",
  "CurrentPage":1,
  "EntityList":[
    {
      "Uuid":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818",
      "Os":"linux",
      "ClientStatus":false,
      "Ip":"x.x.x.x",
      "Region":"****",
      "Flag":0,
      "BuyVersion":"4",
      "GroupId":336,
      "InstanceName":"****"
    }
  ]
}
```

2.16.4.3.11. ModifyEntityGroup

Description

You can call this operation to modify the asset group information for a specified server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyEntityGroup*.
GroupId	Long	No	The modified asset group ID.
Uuids	String	No	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyEntityGroup
&GroupId=11
&Uuids=inet-db626549-870c-4d3e-b0b5-4d8a5c7268a6,inet-db626549-870c-4d3e-b0b5-4d8a5c7268a7
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"C4490A16-DDE4-4351-A366-57F9FCDC188F",
}
```

2.16.4.3.12. DescribeMachines

Description

You can call this operation to query servers that match the specified criteria. For example, you can query all servers in an asset group.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeMachines*.
GroupId	Long	No	The ID of the asset group.
TagIdList	String	No	The server tag ID.
Mark	String	No	The IP address or instance name of the server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
Count	Integer	The number of returned records.
Machines	Array	The servers. For more information, see the following descriptions.
GroupId	Integer	The ID of the asset group.
InstanceName	String	The instance name of the server.
Os	String	The type of the operating system.
Ip	String	The IP address of the server. Note The public IP address of the server is displayed preferentially. If no public IP address is assigned to the server, the private IP address of the server is displayed.
Uuid	String	The universally unique identifier (UUID) of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeMachines
&GroupId=123
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "Count":1,
  "Machines":[
    {
      "groupId":336,
      "os":"linux",
      "instanceName":"****",
      "uuid":"inet-db626549-870c-4d3e-b0b5-4d8a5c7268a6",
      "ip":"192.168.x.x"
    }
  ],
  "RequestId":"C984123D-C8E0-4974-9CEE-ADD0596C46DB"
}
```

2.16.4.3.13. DescribeMachineDetail

Description

You can call this operation to query the detailed information about a specified server.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeMachineDetail*.
Uuid	String	No	The universally unique identifier (UUID) of the server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
MachineDetail	Array	The detailed information about the server. For more information, see the following descriptions.

Parameter	Type	Description
AegisOnline	Boolean	Indicates whether the Server Guard Agent is online.
AegisVersion	String	The version of the Server Guard Agent.
BuyVersion	String	The version of the Server Guard package.
GroupId	Integer	The ID of the asset group.
ClientStatus	Boolean	Indicates whether the server is protected. A value of false indicates that the protection for the server is paused.
Flag	Integer	The type of the server. Valid values: • *0*: indicates an Alibaba Cloud ECS instance. • *1*: indicates an external server.
GroupId	Long	The ID of the asset group.
GroupTrace	String	The full path of the asset group.
InstanceId	String	The instance ID of the server.
InstanceName	String	The instance name of the server.
Os	String	The type of the operating system.
Region	String	The ID of the region.
Ip	String	The IP address of the server. Note The public IP address of the server is displayed preferentially. If no public IP address is assigned to the server, the private IP address of the server is displayed.
IntranetIp	String	The private IP address of the server.
Uuid	String	The UUID of the server.
Tag	String	The server tag ID.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeMachineDetail
&Uuid=6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"5D5D6F8F-6986-4996-9321-8EEA9FC048D1",
  "MachineDetail":{
    "Uuid":"inet-db626549-870c-4d3e-b0b5-4d8a5c7268a6",
    "Ip":"192.168.x.x",
    "GroupTrace":"Not grouped",
    "Os":"linux",
    "ClientStatus":true,
    "Region":"outside-of-aliyun",
    "Tag":"",
    "AegisOnline":false,
    "InstanceName":"****"
  }
}
```

2.16.4.3.14. DescribePropertyScheduleConfig

Description

You can call this operation to query the update cycle of server information.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribePropertyScheduleConfig*.

Name	Type	Required	Description
Type	String	No	The type of the server information. Valid values: • *scheduler_account_period*: indicates the user information. • *scheduler_port_period*: indicates the port information. • *scheduler_process_period*: indicates the process information. • *scheduler_software_period*: indicates the application software information.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Config	String	The update cycle in hours.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyScheduleConfig
&Type=scheduler_account_period
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"C528C153-33E6-4CF5-8C90-A2E6FFD6191C",
 "Config": "2"
}
```

2.16.4.3.15. ModifyPropertyScheduleConfig

Description

You can call this operation to modify the synchronization cycle of server information.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyPropertyScheduleConfig*.
Type	String	Yes	The type of asset information whose synchronization cycle is to be modified. Valid values: • *scheduler_software_period*: indicates the synchronization cycle of application software information. • *scheduler_account_period*: indicates the synchronization cycle of user account information. • *scheduler_port_period*: indicates the synchronization cycle of port information. • *scheduler_process_period*: indicates the synchronization cycle of process information.
ScheduleTime	String	Yes	The new synchronization cycle. Unit: hours.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
ModifyResult	Boolean	Indicates whether the modification is successful.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyPropertyScheduleConfig
&Type=scheduler_software_period
&ScheduleTime=24
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "ModifyResult":true,
 "RequestId":"2932CB78-51FB-459C-A3E8-76BE2968069A"
}
```

2.16.4.3.16. DescribePropertyStatistic

Description

You can call this operation to query the server statistics.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribePropertyStatistic*.
Uuids	String	No	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
PropertyStatistics	Array	The list of server statistics. For more information, see the following parameter descriptions.
PortCount	String	The number of enabled ports.
PortGetDate	String	The port information update time.
ProcCount	String	The number of running processes.
ProcGetDate	String	The process information update time.
RootUserCount	String	The number of user accounts with root permission.
UserCount	String	The total number of user accounts.
UserGetDate	String	The user account information update time.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyStatistic
&Uuids=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "PropertyStatistics":[
  {
   "UserGetDate":1514373155000,
   "Uuid":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818",
   "RootUserCount":1,
   "UserCount":33,
   "ProcCount":89,
   "PortGetDate":1514115614000,
   "PortCount":6,
   "ProcGetDate":1514373133000
  }
 ],
 "RequestId":"C1CACE7E-E868-4E44-A52E-4CB1463B62BB"
}
```

2.16.4.3.17. DescribePropertyPortItem

Description

You can call this operation to obtain a list of listener ports on hosts.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribePropertyPortItem*.

Name	Type	Required	Description
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
Port	String	No	The port number.
ProcName	String	No	The process name.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of returned records.
Count	Integer	The number of records on the current page.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
PropertyPortItems	Array	The list of listener ports on hosts. For more information, see the following parameter descriptions.
Count	Integer	The number of hosts that have enabled the specified port.
Port	String	The port number.
Proto	String	The network protocol, such as TCP or UDP.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyPortItem
&Port=22
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "PageSize":20,
 "RequestId":"9D38986A-F145-4FA8-AE1C-1DB1C2BDF4C0",
 "CurrentPage":1,
 "PropertyPortItems":[
  {
   "Proto":"tcp",
   "Port":"22",
   "Count":2
  }
 ],
 "Count":1
}
```

2.16.4.3.18. DescribePropertyPortDetail

Description

You can call this operation to query detailed information about a listening port.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribePropertyPortDetail*.
PageSize	Integer	No	The number of records to return on each page. Default value: *20*.
CurrentPage	Integer	No	The number of the page to return. Default value: *1*.
GroupId	Long	No	The ID of the asset group.

Parameter	Type	Required	Description
Ip	String	No	The IP address of the server.
Port	String	No	The port number.
Extend	String	No	Indicates whether fuzzy match is enabled to search for port numbers. Valid values: • *1*: indicates that fuzzy match is enabled. • *0*: indicates that fuzzy match is disabled.
ProcName	String	No	The name of the process.
Mark	String	No	The IP address or instance name of the server. Note Fuzzy match is supported.
TagIdListString	String	No	The server tag ID.
Uuid	String	No	The universally unique identifier (UUID) of the server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
Count	Integer	The number of records returned on the current page.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
PropertyPorts	Array	The information about the listening port. For more information, see the following descriptions.
BindIp	String	The IP address bound to the port.
Create	String	The time when the port was enabled.
InstanceName	String	The instance name of the server.
Ip	String	The IP address of the server.

Parameter	Type	Description
Port	String	The port number.
ProcName	String	The name of the process.
Proto	String	The network protocol, such as TCP and UDP.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyPortDetail
&Uuid=inet-f6ac9a93-0818-4052-90e2-d24f18ee198b
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":1,
  "PageSize":20,
  "RequestId":"D85484BB-4DC2-44EC-AD67-0B3765EC9213",
  "CurrentPage":1,
  "PropertyPorts":[
    {
      "InstanceName":"****",
      "Uuid":"inet-f6ac9a93-0818-4052-90e2-d24f18ee198b",
      "Proto":"tcp",
      "Create":1514373168000,
      "Ip":"x.x.x.x",
      "Port":"22",
      "ProcName":"sshd",
      "BindIp":"0.0.0.0"
    }
  ],
  "Count":1
}
```

2.16.4.3.19. DescribePropertyPortDiff

Description

You can call this operation to query listening port changes.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribePropertyPortDiff*.
PageSize	Integer	No	The number of records to return on each page. Default value: *20*.
CurrentPage	Integer	No	The number of the page to return. Default value: *1*.
DiffStatus	String	No	The type of the listening port change. Valid values: • *start*: indicates that the listening port is enabled. • *stop*: indicates that the listening port is disabled.
Ip	String	No	The IP address of the server.
Port	String	No	The port number.
Extend	String	No	Indicates whether fuzzy match is enabled to search for port numbers. Valid values: • *1*: indicates that fuzzy match is enabled. • *0*: indicates that fuzzy match is disabled.
ProcName	String	No	The name of the process.
Mark	String	No	The IP address or instance name of the server. Note Fuzzy match is supported.

Parameter	Type	Required	Description
TagIdListString	String	No	The server tag ID.
Uuid	String	No	The universally unique identifier (UUID) of the server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
PropertyPortDiffs	Array	The listening port changes. For more information, see the following descriptions.
BindIp	String	The IP address bound to the port.
Create	String	The time when the port was enabled.
DiffKeyList	String	The port fields that have been changed, including Proto, ProcName, and BindIp.
DiffStatus	String	The type of the listening port change. Valid values: • *start*: indicates that the listening port is enabled. • *stop*: indicates that the listening port is disabled.
InstanceName	String	The instance name of the server.
Ip	String	The IP address of the server.
ProcName	String	The name of the process.
Port	String	The port number.
Proto	String	The network protocol, such as TCP and UDP.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyPortDiff
&Uuid=inet-f6ac9a93-0818-4052-90e2-d24f18ee198b
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":1,
  "PageSize":20,
  "RequestId":"AFC431E3-F8E3-4652-91CB-9FF4053F282A",
  "CurrentPage":1,
  "PropertyPortDiffs":[
    {
      "InstanceName":"****",
      "Uuid":"inet-f6ac9a93-0818-4052-90e2-d24f18ee198b",
      "Proto":"tcp",
      "Create":1514366856000,
      "Ip":"x.x.x.x",
      "Port":"22",
      "ProcName":"sshd",
      "DiffKeyList":"proto,procName,bindIp",
      "DiffStatus":"stop",
      "BindIp":"0.0.0.0"
    }
  ]
}
```

2.16.4.3.20. DescribePropertyProcItem

Description

You can call this operation to obtain a list of server processes.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribePropertyProcItem*.

Name	Type	Required	Description
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
Name	String	No	The process name.
User	String	No	The user who started the process.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of returned records.
Count	Integer	The number of records on the current page.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
PropertyProcItems	Array	The list of server processes. For more information, see the following parameter descriptions.
Count	Integer	The number of servers on which the process is running.
Name	String	The process name.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyProcItem
&Name=init
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "PropertyProcItems":[
  {
   "Count":2,
   "Name":"init"
  }
 ],
 "PageSize":20,
 "RequestId":"8BE95FB1-66B7-4509-AF82-3AA67368A5D8",
 "CurrentPage":1,
 "Count":1
}
```


2.16.4.3.21. DescribePropertyProcDetail

Description

You can call this operation to query server process details.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribePropertyProcDetail*.
PageSize	Integer	No	The number of records to return on each page. Default value: *20*.
CurrentPage	Integer	No	The number of the page to return. Default value: *1*.
GroupId	Long	No	The ID of the asset group.
Ip	String	No	The IP address of the server.
Name	String	No	The name of the process.

Parameter	Type	Required	Description
Extend	String	No	Indicates whether fuzzy match is enabled to search for process names. Valid values: • *1*: indicates that fuzzy match is enabled. • *0*: indicates that fuzzy match is disabled.
User	String	No	The user who started the process.
Mark	String	No	The IP address or instance name of the server. Note Fuzzy match is supported.
Cmdline	String	No	The process parameter.
TagIdListString	String	No	The server tag ID.
Uuid	String	No	The universally unique identifier (UUID) of the server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
Count	Integer	The number of records returned on the current page.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
PropertyProcs	Array	The details of the server process. For more information, see the following descriptions.
Cmdline	String	The process parameter.
Create	String	The time when the information was reported.
EuidName	String	The permissions that the process has to access resources and files.
InstanceName	String	The instance name of the server.

Parameter	Type	Description
Md5	String	The MD5 value of the executable file.
Name	String	The name of the process.
Path	String	The path of the process.
Pid	String	The ID of the process.
ProcName	String	The name of the process.
Pname	String	The name of the parent process.
StartTime	String	The time when the process was started.
User	String	The user who started the process.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyProcDetail
&Uuid=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "PropertyProcs":[
    {
      "InstanceName":"****",
      "Path":"/sbin/init",
      "Pname":"N/A",
      "Uuid":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818",
      "User":"root",
      "Create":1514373133000,
      "StartTime":"2017-12-26 22:34:45",
      "Pid":"1",
      "EuidName":"root",
      "Cmdline":"/sbin/init",
      "Name":"init",
      "Md5":"70023aaf3f480d198d3b078d8c39****"
    }
  ],
  "TotalCount":1,
  "PageSize":20,
  "RequestId":"AB20A6D4-43EB-44E2-AD64-E03EAC1C14D9",
  "CurrentPage":1,
  "Count":1
}
```


2.16.4.3.22. DescribePropertyProcDiff

Description

You can call this operation to query process changes of a server.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribePropertyProcDiff*.
PageSize	Integer	No	The number of records to return on each page. Default value: *20*.

Parameter	Type	Required	Description
CurrentPage	Integer	No	The number of the page to return. Default value: *1*.
DiffStatus	String	No	The type of the process change. Valid values: • *start*: indicates that the process is started. • *stop*: indicates that the process is stopped.
Ip	String	No	The IP address of the server.
Name	String	No	The name of the process.
User	String	No	The user who started the process.
Mark	String	No	The IP address or instance name of the server. **Note** Fuzzy match is supported.
Uuid	String	No	The universally unique identifier (UUID) of the server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
PropertyProcDiffs	Array	The server process changes. For more information, see the following descriptions.
Cmdline	String	The process parameter.
Create	String	The time when the information was reported.
DiffKeyList	String	The names of the fields that have been changed.
DiffStatus	String	The type of the process change.

Parameter	Type	Description
EuidName	String	The permissions that the process has to access resources and files.
InstanceName	String	The instance name of the server.
Ip	String	The IP address of the server.
Md5	String	The MD5 value of the executable file.
Name	String	The name of the process.
Path	String	The path of the process.
Pid	String	The ID of the process.
Pname	String	The name of the parent process.
StartTime	String	The time when the process was started.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyProcDiff
&Uuid=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":1,
  "PageSize":20,
  "RequestId":"D0951162-E933-4E2B-BDE2-B8FD806CEF9F",
  "CurrentPage":1,
  "PropertyProcDiffs":[
    {
      "Pname":"N/A",
      "Ip":"x.x.x.x",
      "StartTime":"2017-12-26 22:34:45",
      "Pid":"1",
      "DiffKeyList":"startTime,path,user,pid,pname,md5,uid,cmdline,euidName",
      "DiffStatus":"start",
      "Name":"init",
      "InstanceName":"****",
      "Uuid":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818",
      "Create":1514366744000,
      "Cmdline":"/sbin/init",
      "Euidname":"root",
      "Md5":"70023aaf3f480d198d3b078d8c39****"
    },
  ]
}
```


2.16.4.3.23. DescribePropertySoftwareItem

Description

You can call this operation to query servers that have been installed with the specified application.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribePropertySoftwareItem*.

Name	Type	Required	Description
PageSize	Integer	No	The maximum number of records displayed on a page. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
Name	String	No	The name of the application.
Path	String	No	The application installation path.
SoftwareVersion	String	No	The version of the application.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The number of returned records.
Count	Integer	The number of records on the current page.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
PropertySoftwareItems	Array	A list of servers that have been installed with the application. For more information, see the following parameter descriptions.
Count	Integer	The number of servers that have been installed with the application.
Name	String	The name of the application.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertySoftwareItem
&Name=spice-vdagent
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "PropertySoftwareItems":[
  {
   "count":2,
   "Name":"spice-vdagent"
  }
 ],
 "PageSize":20,
 "RequestId":"0F2A3DEA-A5B3-4C2A-8BFC-4724A205E28B",
 "CurrentPage":1,
 "count": 1,
}
```

2.16.4.3.24. DescribePropertySoftwareDetail

Description

You can call this operation to query the details of software installed on a server.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribePropertySoftwareDetail*.
PageSize	Integer	No	The number of records to return on each page. Default value: *20*.
CurrentPage	Integer	No	The number of the page to return. Default value: *1*.
Ip	String	No	The IP address of the server.
Name	String	No	The name of the software.

Parameter	Type	Required	Description
Extend	String	No	Indicates whether fuzzy match is enabled to search for software names.. Valid values: • *1*: indicates that fuzzy match is enabled. • *0*: indicates that fuzzy match is disabled.
Path	String	No	The installation path of the software.
Remark	String	No	The IP address or instance name of the server. Note Fuzzy match is supported.
SoftwareVersion	String	No	The version of the software.
Uuid	String	No	The universally unique identifier (UUID) of the server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
Count	Integer	The number of records returned on the current page.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
PropertySoftwares	Array	The details of software installed on the server. For more information, see the following descriptions.
Create	String	The time when the information was reported.
InstallTime	String	The time when the software was installed.
InstanceName	String	The instance name of the server.
Ip	String	The IP address of the server.
Path	String	The installation path of the software.

Parameter	Type	Description
Version	String	The version of the software.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertySoftwareDetail
&Uuid=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":1,
  "PropertySoftwares":[
    {
      "InstanceName":"****",
      "Path":"/usr/libexec/gvfs-gphoto2-volume-monitor",
      "Uuid":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818",
      "InstallTime":"2016-06-29 06:55:22",
      "Version":"1.4.3",
      "Create":1514172615000,
      "Ip":"x.x.x.x"
    }
  ],
  "PageSize":20,
  "RequestId":"31409246-AB88-4B36-A2B8-16D21BA9E170",
  "CurrentPage":1,
  "Count":1
}
```

2.16.4.3.25. DescribePropertySoftwareDiff

Description

You can call this operation to query changes of applications that have been installed on servers.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribePropertySoftwareDiff*.
PageSize	Integer	No	The maximum number of records displayed on a page. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
DiffStatus	String	No	The type of the application changes. Valid values: • *create*: indicates an installation. • *delete*: indicates an uninstallation. • *modified*: indicates a modification.
Ip	String	No	The IP address of the server.
Name	String	No	The name of the application.
Path	String	No	The path where the application is installed.
SoftwareVersion	String	No	The version of the application.
Mark	String	No	The IP address or instance name of the server. Note Fuzzy match is supported.
Uuid	String	No	The UUID of the server.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The number of returned records.
CurrentPage	Integer	The current page number.

Name	Type	Description
PageSize	Integer	The maximum number of records displayed on a page.
PropertySoftwareDiffs	Array	The application changes. For more information, see the following parameter descriptions.
Create	String	The time when the application change was reported.
DiffKeyList	String	The name of the fields that have been changed.
DiffStatus	String	The type of the changes.
InstanceName	String	The instance name of the server.
Ip	String	The IP address of the server.
Name	String	The name of the application.
Path	String	The path where the application is installed.
Version	String	The version of the application.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertySoftwareDiff
&Uuid=inet-f6ac9a93-0818-4052-90e2-d24f18ee198b
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1398,
 "PageSize":2,
 "RequestId":"3A0814BA-1A5D-43DC-A6E9-3B52EDD3700E",
 "CurrentPage":1,
 "PropertySoftwareDiffs":[
  {
   "Path":"/etc/ghostscript",
   "Uuid":"inet-f6ac9a93-0818-4052-90e2-d24f18ee198b",
   "Version":"8.70",
   "Create":1514172428000,
   "DiffKeyList":"version,path",
   "DiffStatus":"create",
   "Name":"ghostscript"
  },
  {
   "Path":"/usr/sbin/brctl",
   "Uuid":"inet-f6ac9a93-0818-4052-90e2-d24f18ee198b",
   "Version":"1.2",
   "Create":1514172428000,
   "DiffKeyList":"version,path",
   "DiffStatus":"create",
   "Name":"bridge-utils"
  }
 ]
}
```


2.16.4.3.26. DescribePropertyUserItem

Description

You can call this operation to query user account information.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribePropertyUserItem*.

Name	Type	Required	Description
PageSize	Integer	No	The maximum number of records displayed on a page. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
User	String	No	The username of the account.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The number of returned records.
Count	Integer	The number of records on the current page.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
PropertyUserItems	Array	The returned user account information. For more information, see the following parameter descriptions.
Count	Integer	The number of servers under the account.
Name	String	The username of the account.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyUserItem
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":2,
 "PropertyUserItems":[
  {
   "User":"abrt",
   "Count": 2
  },
  {
   "User":"adm",
   "Count": 2
  }
 ],
 "PageSize":20,
 "RequestId":"E80981C2-AD12-4C60-9976-6927C1FE449B",
 "CurrentPage":1,
 "Count": 2
}
```


2.16.4.3.27. DescribePropertyUserDetail

Description

You can call this operation to query user account details.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribePropertyUserDetail*.
PageSize	Integer	No	The number of records to return on each page. Default value: *20*.
CurrentPage	Integer	No	The number of the page to return. Default value: *1*.
GroupId	Long	No	The ID of the asset group.
Ip	String	No	The IP address of the server.

Parameter	Type	Required	Description
IsRoot	String	No	Indicates whether the user account is a root account. Valid values: • *1*: indicates yes. • *0*: indicates no.
User	String	No	The name of the user account.
Extend	String	No	Indicates whether fuzzy match is enabled to search for user accounts. Valid values: • *1*: indicates that fuzzy match is enabled. • *0*: indicates that fuzzy match is disabled.
Mark	String	No	The IP address or instance name of the server. Note Fuzzy match is supported.
TagIdListString	String	No	The server tag ID.
Uuid	String	No	The universally unique identifier (UUID) of the server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
Count	Integer	The number of records returned on the current page.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
PropertyUsers	Array	The details of the user account. For more information, see the following descriptions.
AccountsExpirationDate	String	The time when the user account expires.
Create	String	The time when the information was reported.

Parameter	Type	Description
GroupName	String	The information about the user group.
InstanceName	String	The instance name of the server.
Ip	String	The IP address of the server.
IsRoot	String	Indicates whether the user account is a root account.
LastLoginIp	String	The last IP address that is used by the user account to log on to the server.
LastLoginTime	String	The last logon time of the user account.
PasswordExpirationDate	String	The time when the password of the user account expires.
User	String	The name of the user account.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyUserDetail
&Uuid=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":66,
  "PageSize":2,
  "RequestId":"2EEAE2A6-1662-471C-A5E5-8A6190B01AFF",
  "CurrentPage":1,
  "Count":1,
  "PropertyUsers":[
    {
      "GroupName":[
        "root"
      ],
      "InstanceName":"****",
      "IsRoot":"1",
      "LastLoginTime":"2017-12-27 10:22:25",
      "Uuid":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818",
      "User":"root",
      "LastLoginIp":"192.168.x.x",
      "Create":1514373155000,
      "Ip":"x.x.x.x",
      "AccountsExpirationDate":"never",
      "PasswordExpirationDate":"never"
    }
  ]
}
```


2.16.4.3.28. DescribePropertyUserDiff

Description

You can call this operation to query user account changes.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribePropertyUserDiff*.

Parameter	Type	Required	Description
PageSize	Integer	No	The number of records to return on each page. Default value: *20*.
CurrentPage	Integer	No	The number of the page to return. Default value: *1*.
DiffStatus	String	No	The type of the user account change. Valid values: • *create*: indicates that a new account has been added. • *delete*: indicates that an account has been deleted. • *modified*: indicates that an account has been modified.
IsRoot	String	No	Indicates whether the user account is a root account. Valid values: • *1*: indicates yes. • *0*: indicates no.
User	String	No	The name of the user account.
Mark	String	No	The IP address or instance name of the server. Note Fuzzy match is supported.
Uuid	String	No	The universally unique identifier (UUID) of the server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
PropertyUserDiffs	Array	The user account changes. For more information, see the following descriptions.

Parameter	Type	Description
AccountsExpirationDate	String	The time when the user account expires.
Create	String	The time when the information was reported.
DiffKeyList	String	The names of the fields that have been changed.
DiffStatus	String	The type of the user account change.
GroupName	String	The information about the user group.
InstanceName	String	The instance name of the server.
Ip	String	The IP address of the server.
IsRoot	String	Indicates whether the user account is a root account.
PasswordExpirationDate	String	The time when the password of the user account expires.
User	String	The name of the user account.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribePropertyUserDiff
&Uuid=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":1,
  "PageSize":20,
  "RequestId":"20903EB6-E695-44A4-85C2-B9DFE4376F1F",
  "CurrentPage":1,
  "PropertyUserDiffs":[
    {
      "GroupName":[
        "root"
      ],
      "InstanceName":"****",
      "IsRoot":"0",
      "User":"****",
      "Uuid":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818",
      "Create":1514020942000,
      "Ip":"x.x.x.x",
      "AccountsExpirationDate":"never",
      "DiffKeyList":"isRoot,groupName,accountsExpirationDate,passwordExpirationDate",
      "DiffStatus":"create",
      "PasswordExpirationDate":"never"
    }
  ]
}
```


2.16.4.3.29. PushAllTask

Description

You can call this operation to perform a quick security check on specified servers.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *PushAllTask*.
Uuids	String	No	The universally unique identifier (UUID) of the server. Separate multiple UUIDs with commas (,).

Parameter	Type	Required	Description
Tasks	String	No	The type of the security check task. Valid values: • *OVAL_ENTITY*: indicates all security check tasks. • *CMS*: indicates a check for CMS vulnerabilities. • *SYSVUL*: indicates a check for system software vulnerabilities. • *HEALTH_CHECK*: indicates a baseline check. • *WEBSHELL*: indicates a check for webshells. • *PROC_SNAPSHOT*: indicates a check on process data. • *PORT_SNAPSHOT*: indicates a check on port data. • *ACCOUNT_SNAPSHOT*: indicates a check on account data. • *SOFTWARE_SNAPSHOT*: indicates a check on application data.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
PushTaskRsp	Struct	The task delivery result. For more information, see the following descriptions.
PushTaskResultList	Array	The tasks that fail to be delivered. For more information, see the following descriptions.
GroupId	String	The ID of the asset group.
InstanceId	String	The instance ID of the server.
InstanceName	String	The instance name of the server.
Ip	String	The IP address of the server.
Message	String	The details of the task delivery result.
Online	String	Indicates whether the Server Guard client is online.
OsVersion	String	The version of the operating system.
Region	String	The region where the server resides.

Parameter	Type	Description
Success	String	The task delivery result.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=PushAllTask
&Tasks=OVAL_ENTITY
&Uuids=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5****
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"8A773295-DB9C-423D-979E-C0E8B9F88FEA",
  "PushTaskRsp":{
    "PushTaskResultList":[
      {
        "InstanceName":"****",
        "Uuid":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5****",
        "Message":"{\"code\":\"clinent_offline\",\"message\":\"The client is offline\",\"success\":fal
se}",
        "InstanceId":"i-25l6r****",
        "Ip":"x.x.x.x",
        "OsVersion":"linux",
        "Region":"cn-****-a01",
        "Online":false,
        "Success":false,
        "GroupId":336
      }
    ]
  }
}
```

2.16.4.3.30. DescribeTopRiskyAssets

Description

You can call this operation to query top N vulnerable servers.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeTopRiskyAssets*.
PageSize	Integer	No	The number of records to return, that is, the top N vulnerable servers.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
TopRiskyAssets	Array	The top N vulnerable servers. For more information, see the following descriptions.
HcCount	String	The number of at-risk items detected in the baseline check.
Ip	String	The IP address of the server.
Uuid	String	The universally unique identifier (UUID) of the server.
VulCount	String	The number of detected vulnerabilities.
WarningCount	String	The number of detected security events.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeTopRiskyAssets
&PageSize=1
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount": 1,
  "RequestId": "5D8D4058-2EE3-4599-9951-BDAA3340AD4D",
  "TopRiskyAssets": [
    {
      "Ip": "192.168.x.x",
      "Uuid": "inet-dsljaoe-jjdsklaj****",
      "VulCount": 2,
      "HcCount": 1,
      "WarningCount": 2
    }
  ]
}
```

2.16.4.3.31. UnbindAegis

Description

You can call this operation to disable Server Guard for a specified server.

Note After this operation, Server Guard is not able to detect any security events on this server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *UnbindAegis*.
Uuids	String	Yes	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=UnbindAegis
&Uuids=6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac,6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"8BFB5273-6582-446A-9E0B-BAC0A1A468EA"
}
```

2.16.4.3.32. UninstallAegis

Description

You can call this operation to uninstall the Server Guard client from a specified server.

> **Note** After the client is uninstalled, Server Guard is not able to detect the security events on this server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *UninstallAegis*.
Uuids	String	Yes	The UUID of the server. Separate multiple UUIDs with commas (,).
Reason	String	No	The reason for uninstalling the client.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=UninstallAegis
&Reason=Suspend the feature
&Uuids=6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac,6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"8BFB5273-6582-446A-9E0B-BAC0A1A468EA"
}
```

2.16.4.4. Vulnerability management operations

2.16.4.4.1. DescribeTarget

Description

You can call this operation to query the servers that are checked for the specified type of risks in vulnerability management.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeTarget*.
Type	String	No	The type of the risks. For example, *vul* represents vulnerabilities.
Config	String	No	The type of the vulnerabilities in JSON format. For example, {"vulType":"cve"} represents Linux software vulnerabilities.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The number of returned records.
Targets	Array	A list of servers that are checked for the specified type of risks. For more information, see the following parameter descriptions.

Name	Type	Description
TargetType	String	Valid values: • *groupId*: indicates the ID of an asset group. • *uuid*: indicates the UUID of a server.
Target	String	The asset group ID or server UUID.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeTarget
&Config={"vulType":"cve"}
&Type=vul
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "TotalCount":2,
  "RequestId":"1FF54D56-47ED-47FB-B4DB-2BDF3857D526",
  "Targets":[
    {
      "Target":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818",
      "TargetType":"uuid"
    },
    {
      "Target":"336",
      "TargetType":"groupId"
    }
  ]
}
```

2.16.4.4.2. ModifyVulTarget

Description

You can call this operation to modify the servers for detecting a specified type of vulnerability in the vulnerability management settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyVulTarget*.
Config	String	No	The vulnerability type information, in JSON format. For example, `{"vulType":"cve"}` indicates Linux software vulnerabilities.
Target	String	No	The specified server, in JSON format. For more information, see the sample request.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyVulTarget
&Config={"vulType":"cve"}
&Target={"target":"inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818","targetType":"uuid","flag":"add"}
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"1FF54D56-47ED-47FB-B4DB-2BDF3857D526"
}
```

2.16.4.4.3. DescribeVulTargetStatistics

Description

You can call this operation to query the information about target hosts for which vulnerability detection is enabled in the vulnerability management configuration.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVulTargetStatistics*.
Type	String	No	The vulnerability type.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
TotalCount	Integer	The total number of returned records.
TargetStats	Array	The list of target hosts for which vulnerability detection is enabled. For more information, see the following parameter descriptions.
VulType	String	The vulnerability type.
Targets	Array	The information about target hosts. For more information, see the following parameter descriptions.
Flag	String	Indicates whether vulnerability detection is enabled.
TargetType	String	The type of the Target parameter value. Valid values: • *groupId*: indicates an asset group ID. • *uuid*: indicates a host asset UUID.
Target	String	The asset group ID or host asset UUID.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulTargetStatistics
&Type=cve
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "TargetStats":[
  {
   "VulType":"cve","Targets":[]
  },
 "PageSize":10,
 "RequestId":"89DD84B4-B592-476C-A6C0-51D56B3E8EAC",
 "CurrentPage":1
}
```

2.16.4.4.4. DescribeTargetConfig

Description

You can call this operation to query the vulnerability scanning configuration information of a specified server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeTargetConfig*.
Type	String	No	The type of the vulnerability.
Uuid	String	No	The UUID of the server.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of the returned records.
TargetConfigs	Array	The list of vulnerability scanning configuration information. For more information, see the following parameter descriptions.

Name	Type	Description
Type	String	The type of the vulnerability.
Config	String	Whether vulnerability scanning is enabled. Valid values: on and off.
OverAllConfig	String	Whether global vulnerability scanning is enabled. Valid values: on and off. Note The global vulnerability scanning configuration overrides the vulnerability scanning configuration for a single server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeTargetConfig
&Type=cve
&Uuid=inet-00f20b1a-e2dd-408b-b38e-6a6e1ed5d818
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "RequestId":"092094BF-910F-4CE6-BE93-C3989B607977",
 "TargetConfigs":[
  {
   "Config":"off",
   "Type":"cve",
   "OverAllConfig":"off"
  }
 ]
}
```

2.16.4.4.5. ModifyTargetConfig

Description

You can call this operation to modify the vulnerability scanning configuration for a specified server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyTargetConfig*.
Type	String	No	The type of the vulnerability.
Uuid	String	No	The UUID of the server.
Config	String	No	The vulnerability scanning configuration. Valid values: • *on*: indicates enabled. • *off*: indicates disabled.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyTargetConfig
&Config=on
&Type=cms
&Uuid=46ef7c05-0c53-486c-b446-ef6ff972551c
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"092094BF-910F-4CE6-BE93-C3989B607977"
}
```

2.16.4.4.6. DescribeVulConfig

Description

You can call this operation to query the global scanning configuration for each vulnerability type.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVulConfig*.
Type	String	No	The type of the vulnerability.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of returned records.
TargetConfigs	Array	The list of global vulnerability scanning configurations. For more information, see the following parameter descriptions.
Type	String	The type of the vulnerability.
Config	String	The global scanning configuration for the vulnerability type. Valid values: on and off.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulConfig
&Type=cve
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "RequestId":"A8E09216-31DF-45B6-A76B-E3F053752C07",
 "TargetConfigs":[
  {
   "Config":"off",
   "Type":"cve"
  }
}
```


2.16.4.4.7. ModifyVulConfig

Description

You can call this operation to modify the global vulnerability scanning configuration.

> **Note** The global vulnerability scanning configuration overrides the vulnerability scanning configuration for a single server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyVulConfig*.
Type	String	No	The type of the vulnerability.
Config	String	No	The vulnerability scanning configuration. Valid values: • *on*: indicates enabled. • *off*: indicates disabled.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyVulConfig
&Config=on
&Type=cms
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"A8E09216-31DF-45B6-A76B-E3F053752C07"
}
```

2.16.4.4.8. DescribeAutoDelConfig

Description

You can call this operation to query the number of days that an invalid vulnerability is kept for before it is automatically deleted in the vulnerability management settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeAutoDelConfig*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Days	Integer	The number of days that an invalid vulnerability is kept for.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeAutoDelConfig
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"E3785090-CFF4-4C53-82E4-08F902586053",
 "Days":7
}
```

2.16.4.4.9. ModifyAutoDelConfig

Description

You can call this operation to modify the number of days that an invalid vulnerability is kept for before it is automatically deleted in the vulnerability management settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyAutoDelConfig*.
Days	Integer	No	The number of days that an invalid vulnerability is kept for.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyAutoDelConfig
&Days=7
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"E3785090-CFF4-4C53-82E4-08F902586053"
}
```

2.16.4.4.10. DescribeVulLevel

Description

You can call this operation to query the vulnerability severities that require attention.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVulLevel*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
ConcernLevels	List	The list of vulnerability severities that require attention.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulLevel
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"7935CB7A-D1B7-4EE6-93D0-FF3D040CF19B",
 "ConcernLevels":["high","medium"]
}
```

2.16.4.4.11. ModifyVulLevel

Description

You can call this operation to change the vulnerability severities that require attention.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyVulLevel*.
ConcernLevels	String	No	The vulnerability severities that require attention. Separate multiple severities with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyVulLevel
&ConcernLevel=high,medium
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"7935CB7A-D1B7-4EE6-93D0-FF3D040CF19B"
}
```

2.16.4.4.12. CreateVulWhitelist

Description

You can call this operation to add a specified vulnerability to the whitelist. Server Guard does not report the vulnerabilities on the whitelist.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateVulWhitelist*.

Name	Type	Required	Description
Reason	String	No	The reason for adding the vulnerability to the whitelist.
Whitelist	String	No	The vulnerability to be whitelisted, in JSON format. For more information, see the sample request.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=CreateVulWhitelist
&Reason=The vulnerability is not harmful.
&Whitelist=[{"name":"oval:com.redhat.rhsa:def:20173263","type":"cve","aliasName":"RHSA-2017:3263:
curl security update"}]
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"E3785090-CFF4-4C53-82E4-08F902586053"
}
```

2.16.4.4.13. DescribeVulWhitelist

Description

You can call this operation to obtain the whitelist of vulnerabilities.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVulWhitelist*.

Name	Type	Required	Description
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
TotalCount	Integer	The total number of returned records.
VulWhitelists	Array	The vulnerability whitelist. For more information, see the following parameter descriptions.
AliasName	String	The alias of the vulnerability.
Name	String	The name of the vulnerability.
Reason	String	The reason for adding the vulnerability to the whitelist.
Type	String	The vulnerability type.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulWhitelist
&CurrentPage=1
&PageSize=20
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "VulWhitelists":[
  {
   "Name":"oval:com.redhat.rhsa:def:20173263",
   "AliasName":"RHSA-2017:3263: curl security update",
   "Type":"cve",
   "Reason":"Not fixed at present"
  }
 ],
 "PageSize":3,
 "RequestId":"74F97EF7-B543-43FD-A4E9-18456731F9C5",
 "CurrentPage":1
}
```


2.16.4.4.14. DeleteVulWhitelist

Description

You can call this operation to delete a specified vulnerability from the vulnerability whitelist. After this operation, Server Guard re-detects and reports the vulnerability.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DeleteVulWhitelist*.
Whitelist	String	No	The vulnerability to be deleted from the whitelist, in JSON format. For more information, see the sample request.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DeleteVulWhitelist
&Whitelist=[{"name":"oval:com.redhat.rhsa:def:20173263","type":"cve","aliasName":"RHSA-2017:3263:
curl security update"}]
&<Common request parameters>
```

- Sample response (JSON format)

```
{
 "RequestId":"E3785090-CFF4-4C53-82E4-08F902586053"
}
```

2.16.4.4.15. DescribeGroupedVul

Description

You can call this operation to query information about the specified vulnerability group. The vulnerability management feature can display detected vulnerability records by group. A vulnerability group contains all servers with a specific vulnerability detected by Server Guard.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeGroupedVul*.
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
Dealed	String	No	Indicates whether the vulnerability has been handled. Valid values: • *Y*: indicates that the vulnerability has been handled. • *N*: indicates that the vulnerability has not been handled.

Name	Type	Required	Description
Direction	String	No	The sorting mode of vulnerabilities in the vulnerability group. Valid values: • *asc*: indicates sorting in ascending order. • *desc*: indicates sorting in descending order.
LastTsEnd	Long	No	The end time of the last detection of the vulnerability.
LastTsStart	Long	No	The start time of the last detection of the vulnerability.
Level	String	No	The severity of the vulnerability. Valid values: • *serious*: critical • *high*: important • *medium*: moderate • *low*: low
Name	String	No	The name of the vulnerability.
Necessity	String	No	The necessity for fixing the vulnerability. Valid values: • *asap*: indicates that the vulnerability must be fixed as soon as possible. • *later*: indicates that the vulnerability can be fixed later. • *nntf*: indicates that the vulnerability can be ignored.
OrderBy	String	No	The field based on which the vulnerabilities in the vulnerability group are sorted. You can specify other request parameters for sorting order.
PatchId	Long	No	The ID of the patch used to fix the vulnerability.
Product	String	No	The product where the vulnerability exists.

Name	Type	Required	Description
StatusList	String	No	The status of the vulnerability. Valid values: • *1*: indicates that the vulnerability has not been fixed. • *2*: indicates that the vulnerability fix failed. • *3*: indicates that the server has failed to be rolled back to the version before the vulnerability fix. • *4*: indicates that the vulnerability is being fixed. • *5*: indicates that the server is being rolled back to the version before the vulnerability fix. • *6*: indicates that the vulnerability fix is being verified. • *7*: indicates that the vulnerability has been fixed successfully. • *8*: indicates that the vulnerability has been fixed successfully, and that the server is waiting for restart. • *9*: indicates that the server has been rolled back to the version before the vulnerability fix. • *10*: indicates that the vulnerability has been ignored. • *11*: indicates that the server has been rolled back to the version before the vulnerability fix, and that the server is waiting for restart. • *12*: indicates that the vulnerability does not exist. • *20*: indicates that the vulnerability is invalid. Note The statuses are specified in a single parameter, separated with commas (,).
Type	String	No	The type of the vulnerability.
Uuids	String	No	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
TotalCount	Integer	The total number of returned records.
GroupedVulItems	Array	The information about the vulnerability group. For more information, see the following parameter descriptions.
AliasName	String	The alias of the vulnerability.
AsapCount	Integer	The number of assets to be fixed as soon as possible.
Count	Integer	The total number of vulnerabilities.
GmtLast	Long	The last time when the vulnerability was detected.
HandledCount	Integer	The total number of vulnerabilities handled.
Level	String	The severity of the vulnerability.
Name	String	The name of the vulnerability.
PendingCount	Integer	The number of vulnerabilities that have not been handled.
Product	String	The product affected by the vulnerability.
Status	Integer	The status of the vulnerability.
TotalCount	Integer	The total number of vulnerabilities.
Type	String	The type of the vulnerability.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeGroupedVul
&CurrentPage=1
&Dealed=y
&Direction=asc
&LastTsEnd=1517414400000
&LastTsStart=1517414500000
&Level=high
&Name=oval:com.redhat.rhsa:def:20170817
&Necessity=asap
&OrderBy=name
&PageSize=20
&PatchId=27001
&Product=redhat
&SourceIp=
&StatusList=1,2
&Type=cve
&Uuids=46ef7c05-0c53-486c-b446-ef6ff972551c,b688bf9f-1fd9-42c8-bb34-28697f562dc5
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "GroupedVulItems":[
  {
   "Name":"oval:com.redhat.rhsa:def:20170817",
   "Status":7,
   "Count":0,
   "TotalCount":1,
   "PendingCount":0,
   "AliasName":"RHSA-2017:0817: kernel security, bug fix, and enhancement update",
   "AsapCount":0,
   "Type":"cve",
   "GmtLast":1513695612000,
   "Level":"high",
   "HandledCount":1
  },
 ],
 "TotalCount":1,
 "PageSize":10,
 "RequestId":"6FCF95BE-7A78-4AD8-811C-BF12FC34AC34",
 "CurrentPage":1
}
```


2.16.4.4.16. DescribeVulList

Description

You can call this operation to obtain the vulnerability list of the specified host asset.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVulList*.
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.

Name	Type	Required	Description
Dealed	String	No	Indicates whether the vulnerability has been handled. Valid values: • *Y*: indicates that the vulnerability has been handled. • *N*: indicates that the vulnerability has not been handled.
Level	String	No	The severity of the vulnerability. Valid values: • *serious*: critical • *high*: important • *medium*: moderate • *low*: low
Name	String	No	The name of the vulnerability.
Necessity	String	No	The necessity for fixing the vulnerability. Valid values: • *asap*: indicates that the vulnerability must be fixed as soon as possible. • *later*: indicates that the vulnerability can be fixed later. • *nntf*: indicates that the vulnerability can be ignored.
Type	String	No	The type of the vulnerability.

Name	Type	Required	Description
StatusList	String	No	The status of the vulnerability. Valid values: • *1*: indicates that the vulnerability has not been fixed. • *2*: indicates that the vulnerability fix failed. • *3*: indicates that the host has failed to be rolled back to the version before the vulnerability fix. • *4*: indicates that the vulnerability is being fixed. • *5*: indicates that the host is being rolled back to the version before the vulnerability fix. • *6*: indicates that the vulnerability fix is being verified. • *7*: indicates that the vulnerability has been fixed successfully. • *8*: indicates that the vulnerability has been fixed successfully, and that the host is waiting for restart. • *9*: indicates that the host has been rolled back to the version before the vulnerability fix. • *10*: indicates that the vulnerability has been ignored. • *11*: indicates that the host has been rolled back to the version before the vulnerability fix, and that the host is waiting for restart. • *12*: indicates that the vulnerability does not exist. • *20*: indicates that the vulnerability is invalid. Note Note: The statuses are specified in a single parameter, separated with commas (,).
Uuids	String	No	The UUID of the host asset. Separate multiple host asset UUIDs with commas (,).

Response parameters

Name	Type	Description

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
TotalCount	Integer	The total number of records returned from the query.
VulRecords	Array	The list of vulnerabilities. For more information, see the following parameter descriptions.
AliasName	String	The alias of the vulnerability.
ExtendContent	String	The extended information of the vulnerability.
ExtendContentJson	String	The extended information of the vulnerability (JSON format).
FirstTs	Long	The first time when the vulnerability was detected.
ModifyTs	Long	The last time when the vulnerability was updated.
LastTs	Long	The last time when the vulnerability was detected.
Level	String	The severity of the vulnerability.
Name	String	The name of the vulnerability.
Necessity	String	The necessity for fixing the vulnerability. Valid values: • *asap*: indicates that the vulnerability must be fixed as soon as possible. • *later*: indicates that the vulnerability can be fixed later. • *nntf*: indicates that the vulnerability can be ignored.
PrimaryId	Long	The ID of the primary key.
Product	String	The product affected by the vulnerability.
RecordId	Long	The ID of the vulnerability record.
Related	String	The CVE ID of the vulnerability.
RepairTs	Long	The time when the vulnerability was fixed.

Name	Type	Description
ResultCode	String	The code of the vulnerability handling result.
ResultMessage	String	The message of the vulnerability handling result.
RiskDesc	String	The risk description of the vulnerability.
RiskLevel	Integer	The risk level of the vulnerability.
Status	Integer	The status of the vulnerability. Valid values: • *1*: indicates that the vulnerability is to be handled. • *2*: indicates that the vulnerability has been ignored. • *3*: indicates that the vulnerability has been confirmed. • *8*: indicates that the vulnerability has been marked as a false positive. • *16*: indicates that the vulnerability is being handled. • *32*: indicates that the vulnerability has been handled.
Tag	String	The tag of the vulnerability.
Type	String	The type of the vulnerability.
Uuid	String	The UUID of the host asset.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulList
&CurrentPage=1
&Dealed=n
&Level=serious
&Name=RHSA-2017:1100: nss and nss-util security update
&Necessity=asap
&PageSize=20
&StatusList=1
&Type=cve
&Uuids=f293ade2-e5b1-4cc0-99a6-cc993a4158cc
&<Common request parameters>
```

- Sample responses (JSON format)


```
{
 "TotalCount":1,
 "PageSize":20,
 "RequestId":"2E35F7F7-DA6D-46A5-BA9D-8751BDAE7710",
 "CurrentPage":1,
 "VulRecords":[
  {
   "Uuid":"b688bf9f-1fd9-42c8-bb34-28697f562dc5",
   "Necessity":"nntf",
   "ModifyTs":1512949391000,
   "Type":"cve",
   "FirstTs":1499321694000,
   "Related":"CVE-2016-1248",
   "ExtendContentJson":{"Necessity":{"Cvss_factor":"6.8","Total_score":"6.799999965526585","Status":"n
ormal","Enviroment_factor":"1.0","Time_factor":"0.9999999949303802","Assets_factor":"1","Gmt_create"
:"20171210","Is_calc":"1"},"Os":"centos","cveList":["CVE-2016-1248"],"RpmEntityList":[{"Name":"vim-mini
mal","Version":"7.4.160","FullVersion":"7.4.160-1.el7","MatchDetail":"vim-minimal version less than 2:7.4
.160-1.el7_3.1","UpdateCmd":"yum update vim-minimal","Path":"/etc/virc"}],"OsRelease":"7"},
   "Name":"oval:com.redhat.rhsa:def:20162972",
   "Status":1,
   "LastTs":1512949391000,
   "AliasName":"RHSA-2016:2972: vim security update (Moderate)",
   "Tag":"oval",
   "PrimaryId":281156,
   "Level":"high"
  }
 ]
}
```


2.16.4.4.17. DescribeVulDetails

Description

You can call this operation to query detailed information about a vulnerability.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVulDetails*.
Type	Integer	Yes	The type of the vulnerability.
Name	String	Yes	The name of the vulnerability.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Cves	Array	The vulnerability details. For more information, see the following parameter descriptions.
Classify	String	The vulnerability type code.
Classifys	Array	The detailed vulnerability information. For more information, see the following parameter descriptions.
Classify	String	The vulnerability type code.
Description	String	The description of the vulnerability type.
DemoVideoUrl	String	The URL of the vulnerability video demo.
CnvdId	String	The CNVD ID.
Complexity	String	The complexity.
Content	String	The vulnerability details.
ExtendContentJson	String	The additional information about the vulnerability (JSON format).
CveId	String	The CVE ID.
CvssScore	String	The CVSS score.
CvssVector	String	The CVSS score string.
OtherId	String	The ID of the vulnerability.
Poc	String	The proof of concept (POC) method.
PocCreateTime	Long	The time when the POC method was created.

Name	Type	Description
PocDisclosureTime	Long	The time when the POC method was revealed.
Service	String	The products that are affected by the vulnerability.
Reference	String	The corresponding reference.
ReleaseTime	Long	The time when the vulnerability was revealed.
Solution	String	The solution for fixing the vulnerability.
Summary	String	The vulnerability summary.
Title	String	The title of the vulnerability.
Vendor	String	The vendors that are affected by the vulnerability.
VulLevel	String	The severity level of the vulnerability.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulDetails
&Name=oval:com.redhat.rhsa:def:20170036
&Type=cve
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "Cves": [{
  "CvssVector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H",
  "OtherId": "CVE-2016-7117",
  "Classifys": [],
  "Vendor": "Linux",
  "CvssScore": "10.0",
  "CnvdId": "CNVD-2016-09362",
  "Reference": "http://www.securityfocus.com/bid/93304",
  "Solution": "<p>The vendor has released a patch to fix this vulnerability. Download the patch from: \
n<br  />https://bugzilla.redhat.com/show_bug.cgi?id=1382268</p>\n",
  "CveId": "CVE-2016-7117",
  "ReleaseTime": 1476028800000,
  "VulLevel": "serious",
  "Title": "The use-after-free vulnerability in __sys_recvmmsg function in the Linux kernel",
  "Summary": "The Linux kernel is released by the Linux Foundation of the United States for Linux ope
rating systems. The use-after-free vulnerability is found in the net/socket.c file in \n\nLinux kernel 4.
5.2 and earlier versions. It allows remote attackers to execute arbitrary code."
 }],
 "RequestId": "70DEE6B7-A167-4B5D-ADAA-3631443D5190"
}
```


2.16.4.4.18. DescribeVulNumStatistics

Description

You can call this operation to query vulnerability statistics.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVulNumStatistics*.
StartTs	Long	No	The start time for statistics collection.
EndTs	Long	No	The end time for statistics collection.
Uuids	String	No	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CmsDealedTotalNum	Integer	The number of CMS vulnerabilities handled.
CmsNum	Integer	The number of CMS vulnerabilities.
CveNum	Integer	The number of CVE vulnerabilities.
EmgNum	Integer	The number of other vulnerabilities.
SysNum	Integer	The number of Windows OS vulnerabilities.
VulAsapSum	Integer	The number of vulnerabilities that need to be handled as soon as possible.
VulDealedTotalNum	Integer	The total number of vulnerabilities handled.
VulSeriousTotal	Integer	The total number of critical vulnerabilities.
VulHighTotal	Integer	The total number of important vulnerabilities.
VulMediumTotal	Integer	The total number of moderate vulnerabilities.
VulLowTotal	Integer	The total number of low vulnerabilities.
VulLaterSum	Integer	The number of vulnerabilities that can be handled later.
VulNntfSum	Integer	The number of vulnerabilities that do not need to be fixed temporarily.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulNumStatistics
&EndTs=1514736000000
&StartTs=1514736000000
&Uuids=46ef7c05-0c53-486c-b446-ef6ff972551c
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "VulHighTotal":0,
  "CveNum":1,
  "VulMediumTotal":0,
  "EmgNum":0,
  "VulLowTotal":0,
  "VulNntfSum":1,
  "VulAsapSum":0,
  "SysNum":0,
  "VulDealedTotalNum":1,
  "RequestId":"093C121C-2981-4E69-8309-CD1BDD8C872A",
  "CmsNum":0,
  "VulSeriousTotal":0,
  "CmsDealedTotalNum":0,
  "VulLaterSum":0
}
```


2.16.4.4.19. DescribeVulLevelStatistics

Description

You can call this operation to obtain the statistics on vulnerabilities by vulnerability severity.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVulLevelStatistics*.
StartTs	Long	No	The start time of the time frame specified for query.
EndTs	Long	No	The end time of the time frame specified for query.
Uuids	String	No	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of returned records.
LevelStatistics	Array	The vulnerability statistics. For more information, see the following parameter descriptions.
CmsDealedTotalNum	Integer	The number of handled CMS vulnerabilities.
CmsNum	Integer	The number of CMS vulnerabilities.
CveNum	Integer	The number of CVE vulnerabilities.
EmgNum	Integer	The number of other vulnerabilities.
Level	String	The severity of the vulnerability.
SysNum	Integer	The number of Windows vulnerabilities.
VulAsapSum	Integer	The number of high-priority vulnerabilities.
VulDealedTotalNum	Integer	The total number of handled vulnerabilities.
VulSeriousTotal	Integer	The total number of critical-risk vulnerabilities.
VulHighTotal	Integer	The total number of important-risk vulnerabilities.
VulMediumTotal	Integer	The total number of moderate-risk vulnerabilities.
VulLowTotal	Integer	The total number of low-risk vulnerabilities.
VulLaterSum	Integer	The number of medium-priority vulnerabilities.
VulNntfSum	Integer	The number of low-priority vulnerabilities.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulLevelStatistics
&EndTs=1514736000000
&StartTs=1514736000000
&Uuids=46ef7c05-0c53-486c-b446-ef6ff972551c,b688bf9f-1fd9-42c8-bb34-28697f562dc5
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":0,
 "LevelStatistics":[
  {
   "VulHighTotal":0,
   "CveNum":0,
   "VulMediumTotal":0,
   "EmgNum":0,
   "VulLowTotal":0,
   "VulNntfSum":0,
   "VulAsapSum":0,
   "SysNum":0,
   "VulDealedTotalNum":0,
   "CmsNum":0,
   "Level":"high",
   "VulSeriousTotal":0,
   "CmsDealedTotalNum":0,
   "VulLaterSum":0
  },
  {
   "VulHighTotal":0,
   "CveNum":0,
   "VulMediumTotal":0,
   "EmgNum":0,
   "VulLowTotal":0,
   "VulNntfSum":0,
   "VulAsapSum":0,
   "SysNum":0,
   "VulDealedTotalNum":0,
   "CmsNum":0,
   "Level":"low",
   "VulSeriousTotal":0,
   "CmsDealedTotalNum":0,
   "VulLaterSum":0
  }
 ],
 "RequestId":"9B062D3F-AD5A-4D3E-9A7A-45CAC2713FC0"
}
```


2.16.4.4.20. DescribeVulMachineList

Description

You can call this operation to query the vulnerability statistics of a specified server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVulMachineList*.
StartTs	Long	No	The start time of the time frame during which the statistics were collected.
EndTs	Long	No	The end time of the time frame during which the statistics were collected.
Uuids	String	No	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of the returned records.
MachineStatistics	Array	The vulnerability statistics. For more information, see the following parameter descriptions.
CmsDealedTotalNum	Integer	The number of CMS vulnerabilities that have been handled.
CmsNum	Integer	The number of CMS vulnerabilities.
CveNum	Integer	The number of CVE vulnerabilities.
EmgNum	Integer	The number of other vulnerabilities.
SysNum	Integer	The number of Windows vulnerabilities.
VulAsapSum	Integer	The number of high-priority vulnerabilities.
VulDealedTotalNum	Integer	The total number of vulnerabilities that have been handled.
VulSeriousTotal	Integer	The total number of critical-risk vulnerabilities.
VulHighTotal	Integer	The total number of important-risk vulnerabilities.

Name	Type	Description
VulMediumTotal	Integer	The total number of moderate-risk vulnerabilities.
VulLowTotal	Integer	The total number of low-risk vulnerabilities.
VulLaterSum	Integer	The number of medium-priority vulnerabilities.
VulNntfSum	Integer	The number of low-priority vulnerabilities.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulMachineList
&EndTs=1514736000000
&StartTs=1514736000000
&Uuids=46ef7c05-0c53-486c-b446-ef6ff972551c
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":0,
 "MachineStatistics":[
  {
   "Uuid":"577f9886-bf66-4c3c-88ac-28c938cb527b",
   "VulHighTotal":0,
   "CveNum":1,
   "VulMediumTotal":0,
   "EmgNum":0,
   "VulLowTotal":0,
   "VulNntfSum":0,
   "VulAsapSum":0,
   "SysNum":0,
   "VulDealedTotalNum":0,
   "CmsNum":0,
   "VulSeriousTotal":0,
   "CmsDealedTotalNum":0,
   "VulLaterSum":0
  }
 ],
 "RequestId":"A3F8BE63-9BA1-450D-BB5D-CE9205E6645D"
}
```


2.16.4.4.21. OperateVul

Description

You can call this operation to handle detected vulnerabilities.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *OperateVul*.
Info	String	No	The vulnerability information, in JSON format. For more information, see the sample request.

Name	Type	Required	Description
OperateType	String	No	The type of the operation. Valid values: • *vul_fix*: indicates an operation to fix the vulnerability. • *vul_verify*: indicates an operation to verify the vulnerability fix. • *vul_rebooted*: indicates an operation to verify the vulnerability fix after the server is restarted. • *vul_rollback*: indicates an operation to undo the vulnerability fix. • *vul_ignore*: indicates an operation to ignore the vulnerability. • *vul_undo_ignore*: indicates an operation to unignore the vulnerability. • *vul_delete*: indicates an operation to delete the vulnerability record.
Reason	String	No	The reason why the vulnerability is ignored if the OperateType parameter is set to vul_ignore.
Type	String	No	The type of the vulnerability.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=OperateVul
&Info=[{"name":"oval:com.redhat.rhsa:def:20171100","uuid":"e49fb179-bbe7-4b6c-ab65-e106fb58d235"
,"tag":"oval"}]
&OperateType=vul_ignore
&Reason=Postpone the fix
&Type=cve
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"A3F8BE63-9BA1-450D-BB5D-CE9205E6645D"
}
```

2.16.4.4.22. ModifyBatchIgnoreVul

Description

You can call this operation to ignore multiple vulnerabilities.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyBatchIgnoreVul*.
Info	String	No	The vulnerabilities to be ignored, in JSON format. For more information, see the sample request.
Reason	String	No	The reason for ignoring the vulnerabilities.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyBatchIgnoreVul
&Info=[{"name":"oval:com.redhat.rhsa:def:20162972","type":"cve","aliasName":"RHSA-2016:2972: vim s
ecurity update (Moderate)"}]
&Reason=Postpone handling
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"E3785090-CFF4-4C53-82E4-08F902586053"
}
```

2.16.4.4.23. DeleteVulBatch

Description

You can call this operation to delete a specified batch of vulnerabilities.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteVulBatch*.
BatchName	String	No	The name of the vulnerability batch.
Resource	String	No	The scenario of the vulnerability batch.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DeleteVulBatch
&BatchName=Vulnerabilities managed by network security team
&Resource=vulnerability
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"E3785090-CFF4-4C53-82E4-08F902586053"
}
```

2.16.4.4.24. ExportVul

Description

You can call this operation to export vulnerability records that match the specified criteria.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ExportVul*.
AliasName	String	No	The alias of the vulnerability.
BatchName	String	No	The name of the vulnerability fix batch.
Dealed	String	No	Indicates whether the vulnerability has been handled. Valid values: • *Y*: indicates that the vulnerability has been handled. • *N*: indicates that the vulnerability has not been handled.
Level	String	No	The severity of the vulnerability.
Name	String	No	The name of the vulnerability.
Necessity	String	No	The priority of the vulnerability. Valid values: • *asap*: indicates that the vulnerability must be fixed as soon as possible. • *later*: indicates that the vulnerability can be fixed later. • *nntf*: indicates that the vulnerability can be ignored.
Resource	String	No	The source of the vulnerability fixing batch.

Name	Type	Required	Description
StatusList	String	No	The status of the vulnerability. Valid values: • *1*: indicates that the vulnerability is pending. • *2*: indicates that the vulnerability has been ignored. • *3*: indicates that the vulnerability has been confirmed. • *8*: indicates that the vulnerability has been marked as a false positive. • *16*: indicates that the vulnerability is being handled. • *32*: indicates that the vulnerability has been handled. You can specify multiple statuses and separate them with commas (,).
Type	String	No	The type of the vulnerability.
Uuids	String	No	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CurrentCount	Integer	The number of records that have been exported.
ExportStatus	String	The status of the export task. Valid values: • *init*: indicates that the export task is being initialized. • *pending*: indicates that the export task is pending for summarization. • *exporting*: indicates that the export task is being executed. • *success*: indicates that the export task has been completed. • *fail*: indicates that the export task has failed.
Message	String	The status description or failure information of the export task.
FileName	String	The name of the exported file.
Id	Integer	The ID of the export task.

Name	Type	Description
Link	String	The download link of the exported file.
Progress	Integer	The export progress.
TotalCount	Integer	The total number of records that have been exported.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ExportVul
for example, RHSA-2016:2972: vim security update (Moderate), and trigger another vulnerability scan.
&BatchName=Security group test
&Dealed=y
&Level=low
&Name=oval:com.redhat.rhsa:def:20162972
&Necessity=later
&Resource=vulnerability
&StatusList=1
&Type=cve
&Uuids=46ef7c05-0c53-486c-b446-ef6ff972551c
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "FileName":"cve_20180303",
 "RequestId":"3B3C79B1-617E-4081-903B-86EA4AC0213F",
 "Id":36
}
```

2.16.4.4.25. DescribeVulExportInfo

Description

You can call this operation to query a vulnerability record export task.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeVulExportInfo*.
ExportId	Long	No	The ID of the vulnerability record export task.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentCount	Integer	The number of records that have been exported.
ExportStatus	String	The status of the export task. Valid values: • *init*: indicates that the export task is being initialized. • *pending*: indicates that the export task is pending. • *exporting*: indicates that the export task is being executed. • *success*: indicates that the export task has been completed. • *fail*: indicates that the export task has failed.
Message	String	The status description or failure information of the export task.
FileName	String	The name of the exported file.
Id	Integer	The ID of the export task.
Link	String	The download link of the exported file.
Progress	Integer	The export progress.
TotalCount	Integer	The total number of records that have been exported.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeVulExportInfo
&ExportId=10
&<Common request parameters>
```

- Sample response (JSON format)

```
{
 "Status":"success",
 "Link":"http://jiangzhi.oss-cn-shanghai.example.com/export/sys_20171124_1511510709277.zip?Expire
s=1511514309&OSSAccessKeyId=<yourAccessKeyId>&Signature=xxxx%xxxx%3D",
 "TotalCount":2,
 "Message":"success",
 "FileName":"sys_20171124",
 "RequestId":"9C689776-0F8B-4290-8C11-D9242A86C75B",
 "CurrentCount":1,
 "Id":17,
 "Progress":100
}
```

2.16.4.5. Baseline check operations

2.16.4.5.1. DescribeStrategy

Description

You can call this operation to obtain a list of baseline check policies.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeStrategy*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Count	Integer	The total number of the returned records.

Name	Type	Description
Strategies	Array	The list of baseline check policies. For more information, see the following parameter descriptions.
CycleDays	Integer	The cycle of policy execution.
CycleStartTime	Integer	The start time of policy execution. Valid values: • *0*: indicates the period from 00:00 to 06:00. • *6*: indicates the period from 06:00 to 12:00. • *12*: indicates the period from 12:00 to 18:00. • *18*: indicates the period from 18:00 to 24:00.
EcsCount	Integer	The number of hosts using the policy.
Id	Integer	The ID of the policy.
Name	String	The name of the policy.
RiskCount	Integer	The number of at-risk items contained in the policy.
Type	Integer	The policy type. Valid values: • *1*: indicates a system default policy. • *2*: indicates a custom policy.
ConfigTargets	Array	The information about asset groups using the policy. For more information, see the following parameter descriptions.
Flag	String	A flag that indicates whether the policy applies to the specified asset group. Valid values: • *add*: indicates the whitelist mode, that is, the policy applies to the asset group. • *del*: indicates the blacklist mode, that is, the policy does not apply to the asset group. Note Generally, the blacklist mode is used for system default policies, and the whitelist mode is used for custom policies.
TargetType	String	The return value is fixed to groupId, which indicates that the value of the Target parameter is an asset group ID.
Target	String	The ID of the asset group.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeStrategy
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "Count": 2,
  "RequestId": "4F914046-4358-4BA9-BE42-83AA1FD1FF52",
  "Strategies": [
    {
      "Name": "test",
      "RiskCount": 2,
      "CycleDays": 3,
      "Type": 2,
      "CycleStartTime": 6,
      "ConfigTargets": [
        {
          "Target": "4361221",
          "Flag": "add",
          "TargetType": "groupId"
        }
      ],
      "Id": 15161,
      "EcsCount": 0
    },
    {
      "Name": "Default policy",
      "RiskCount": 14,
      "CycleDays": 1,
      "Type": 1,
      "CycleStartTime": 0,
      "ConfigTargets": [
        {
          "Target": "none",
          "Flag": "del",
          "TargetType": "flag_item"
        }
      ],
      "Id": 20,
      "EcsCount": 48
    }
  ]
}
```


2.16.4.5.2. DescribeStratetyDetail

Description

You can call this operation to query the details of a specified baseline check policy.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeStratetyDetail*.
Id	String	No	The ID of the baseline check policy.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Strategy	Array	The details of the baseline check policy. For more information, see the following parameter descriptions.
CycleDays	Integer	The cycle of policy execution.
CycleStartTime	Integer	The start time of policy execution. Valid values: • *0*: indicates the period from 00:00 to 06:00. • *6*: indicates the period from 06:00 to 12:00. • *12*: indicates the period from 12:00 to 18:00. • *18*: indicates the period from 18:00 to 24:00.
Id	Integer	The ID of the policy.
Name	String	The name of the policy.
Type	Integer	The type of the policy. Valid values: • *1*: indicates a system default policy. • *2*: indicates a custom policy.
RiskTypeWhiteListQueryResultList	Array	The risk information contained in the policy. For more information, see the following parameter descriptions.
Alias	String	The name of the risk category.
On	Boolean	Indicates whether to check for risks of the specified category.
TypeName	String	The code of the risk category.

Name	Type	Description
SubTypes	Array	The list of risk subcategories. For more information, see the following parameter descriptions.
Alias	String	The name of the risk subcategory.
TypeName	String	The code of the risk subcategory.
On	Boolean	Indicates whether to check for risks of the specified subcategory.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeStratetyDetail
&Id=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
    "RequestId": "99F17C4B-2E23-4B41-BBEB-C03963B06EB4",
    "Strategy": {
  "Name": "Yunwu testing",
        "CycleDays": 1,
        "CycleStartTime": 18,
        "Type": 2,
        "Id": 12,
        "RiskTypeWhiteListQueryResultList": [
          {
            "On": false,
            "Alias": "Compliance with Security Standards",
            "TypeName": "cis",
            "SubTypes": [
              {
                "On": true,
                "Alias": "Memcached",
                "TypeName": "memcached-check"
              },
              {
                "On": true,
                "Alias": "CentOS 7",
                "TypeName": "centos7"
              },
              {
                "On": false,
                "Alias": "Tomcat 7",
                "TypeName": "tomcat7"
              },
              {
                "On": false,
                "Alias": "MongoDB",
                "TypeName": "mongodb-check"
              }
            ]
          }
  ]
 }
}
```

2.16.4.5.3. ModifyStrategy

Description

You can call this operation to modify the basic information of a baseline check policy.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyStrategy*.
CycleDays	String	No	The baseline check cycle.
CycleStartTime	String	No	The time when the baseline check starts. Valid values: • *0*: starts at 00:00 and ends at 06:00. • *6*: starts at 06:00 and ends at 12:00. • *12*: starts at 12:00 and ends at 18:00. • *18*: starts at 18:00 and ends at 24:00.
Id	String	No	The ID of the baseline check policy. Note If this parameter is set to null, a baseline check policy is added.
Name	String	No	The name of the baseline check policy.
RiskSubTypeName	String	No	The sub-risk types in the baseline check policy. Separate multiple sub-risk types with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Result	Struct	The returned information. For more information, see the following parameter descriptions.
StrategyId	Integer	The ID of the baseline check policy.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyStrategy
&CycleDays=1
&CycleStartTime=8
&Id=52
&Name=Web server
&RiskSubTypeName=redis_check,linux_password
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"161F1BEE-5268-4935-9763-C39A2F7F65DD",
 "Result":2
  "StrategyId":52
 }
}
```

2.16.4.5.4. DeleteStrategy

Description

You can call this operation to delete a specified baseline check policy.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteStrategy*.
Id	String	No	The ID of the baseline check policy.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DeleteStrategy
&Id=123456
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "43F670F3-AB40-4E91-BC7D-C57468834F67"
}
```

2.16.4.5.5. DescribeStrategyTarget

Description

You can call this operation to query the information about asset groups to which a specified baseline check policy applies.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeStrategyTarget*.
Config	String	No	The policy configuration information. The baseline check policy ID is specified in JSON format, for example, `{"strategyId":15161}`.
Type	String	No	The configuration type. Set the value to *hc_strategy*.
Target	String	No	The ID of the asset group to which the baseline check policy applies.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Count	Integer	The total number of returned records.

Name	Type	Description
StrategyTargets	Array	The information about asset groups to which the policy applies. For more information, see the following parameter descriptions.
Flag	String	Indicates whether the policy applies to the specified asset group. Valid values: • *add*: indicates the whitelist mode, that is, the policy applies to the asset group. • *del*: indicates the blacklist mode, that is, the policy does not apply to the asset group. Note Generally, the blacklist mode is used for system default policies, and the whitelist mode is used for custom policies.
TargetType	String	The return value is fixed to groupId, indicating that the value of the Target parameter is the ID of the asset group.
Target	String	The asset group ID.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeStrategyTarget
&Config={"strategyId":15161}
&Type=hc_strategy
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
      "Count": 1,
      "StrategyTargets":[
        {
          "Flag": "del",
          "Target": "281801",
          "TargetType": "groupId"
        }
      ]
 "requestId": "B44F545D-15CF-4A57-B8BF-4340D15D0507"
}
```


2.16.4.5.6. ModifyStrategyTarget

Description

You can call this operation to modify the information about the asset groups that a specified baseline check policy applies to.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyStrategyTarget*.
Config	String	No	The policy configuration information. The baseline check policy ID is specified in JSON format, for example, `{"strategyId":15161}`.
Type	String	No	The configuration type. Set the value to *hc_strategy*.
Target	String	No	The information about asset groups that the baseline check policy applies to. For more information, see the sample request.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyStrategyTarget
&Type=hc_strategy
&Config={"strategyId":36071}
&Target=[{"targetType":"groupId","target":"1111","flag":"add"}]
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId": "B44F545D-15CF-4A57-B8BF-4340D15D0507"
}
```

2.16.4.5.7. DescribeUuidConfig

Description

You can call this operation to check whether baseline check is enabled for a specified server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeUuidConfig*.
Uuid	String	No	The UUID of the server.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Data	Struct	The baseline check configuration. For more information, see the following parameter descriptions.

Name	Type	Description
Flag	String	Indicates whether baseline check is enabled. Valid values: • *add*: indicates enabled. • *del*: indicates disabled.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeUuidConfig
&uuid=4bc19998-e100-4b04-ab11-1e677418d311
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
   "Data": {
      "Flag": "del"
   },
   "RequestId": "A89978FE-BC35-427E-A4B1-7AEEAE741CC2",
}
```

2.16.4.5.8. ModifyMachineConfig

Description

You can call this operation to configure whether to apply a specified baseline check policy to a specified server.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyMachineConfig*.
Type	String	No	The configuration type. Set the value to *hc_switch*, indicating the baseline check policy switch.

Name	Type	Required	Description
Target	String	No	The specified server, in JSON format. For more information, see the sample request.
Config	String	No	The policy configuration information. The baseline check policy ID is specified in JSON format, for example, `{"strategyId":15161}`.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyMachineConfig
&target={"targetType":"uuid","target":"2738e842-7d46-42f7-acb4-e6796b051ddc","ip":"x.x.x.x","flag":"del"}
&type=hc_switch
&config={"strategyId":15161}
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "A89978FE-BC35-427E-A4B1-7AEEAE741CC2",
}
```

2.16.4.5.9. DescribeUserSetting

Description

You can call this operation to query the number of days an invalid risk is kept for before it is automatically deleted in baseline check.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeUserSetting*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
InvalidWarningKeepDays	Integer	The number of days that an invalid risk is kept for.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeUserSetting
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "InvalidWarningKeepDays":90,
 "RequestId":"0A079FE2-0D1B-4A4D-A4EF-D02B5DDE12A7"
}
```

2.16.4.5.10. CreateUserSetting

Description

You can call this operation to specify the number of days an invalid risk is kept for before it is automatically deleted in baseline check.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateUserSetting*.

Name	Type	Required	Description
InvalidWarningKeepDays	Integer	No	The number of days an invalid risk is kept for. Valid values: • *7*: indicates that the invalid risk item is to be deleted in seven days. • *30*: indicates that the invalid risk item is to be deleted in 30 days. • *90*: indicates that the invalid risk item is to be deleted in 90 days.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=CreateUserSetting
&InvalidWarningKeepDays=90
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "43F670F3-AB40-4E91-BC7D-C57468834F67",
}
```

2.16.4.5.11. DescribeRiskWhiteList

Description

You can call this operation to obtain the whitelist of risk items that are exempt from the baseline check.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeRiskWhiteList*.

Name	Type	Required	Description
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
RiskName	String	No	The name of the risk item. This parameter supports fuzzy match.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of returned records.
Count	Integer	The number of records on the current page.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
WhiteLists	Array	The risk item whitelist. For more information, see the following parameter descriptions.
Reason	String	The reason for adding the risk item to the whitelist.
RiskId	Long	The ID of the risk item.
RiskName	String	The name of the risk item.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeRiskWhiteList
&RiskName=SSH logon baseline check
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "PageSize":20,
 "RequestId":"B452E97A-7DFA-44FC-915D-5D590A702846",
 "CurrentPage":1,
 "WhiteLists":[
  {
   "RiskName":"SSH logon baseline check",
   "RiskId":1
  }
 ],
 "Count":1
}
```

2.16.4.5.12. BatchDeleteWhiteList

Description

You can call this operation to delete multiple risks from the whitelist for baseline check.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *BatchDeleteWhiteList*.
RiskIdList	String	No	The ID of the risk to be deleted from the whitelist. Separate multiple IDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=BatchDeleteWhiteList
&RiskIdList=1,2,3
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"E3785090-CFF4-4C53-82E4-08F902586053"
}
```

2.16.4.5.13. CreateUserWhiteList

Description

You can call this operation to add a specified risk to the baseline check whitelist. After this operation, the risk is not reported during baseline check.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateUserWhiteList*.
RiskIdList	String	No	The ID of the risk to be added to the whitelist. Separate multiple IDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=CreateUserWhiteList
&RiskIdList=1,2,3
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"E3785090-CFF4-4C53-82E4-08F902586053"
}
```

2.16.4.5.14. DescribeStratety

Description

You can call this operation to query the execution details of a specified baseline check policy.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeStratety*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Strategies	Array	The list of baseline check policies. For more information, see the following parameter descriptions.
CycleDays	Integer	The execution cycle of the policy.
CycleStartTime	Integer	The start time of policy execution.
EcsCount	Integer	The number of hosts to which the policy applies.
ExecStatus	Integer	The current execution status of the policy. Valid values: • *1*: indicates that the policy has been executed. • *2*: indicates that the policy is being executed.
Id	Integer	The ID of the policy.
Name	String	The name of the policy.

Name	Type	Description
ProcessRate	Integer	The progress of policy execution. Unit: percentage.
RiskCount	Integer	The number of risk items contained in the policy.
ConfigTargets	Array	The asset group to which the policy applies. For more information, see the following parameter descriptions.
Flag	String	Indicates whether the policy applies to the specified asset group. Valid values: • *add*: indicates the whitelist mode, that is, the policy applies to the asset group. • *del*: indicates the blacklist mode, that is, the policy does not apply to the asset group. Note Generally, the blacklist mode is used for system default policies, and the whitelist mode is used for custom policies.
TargetType	String	The return value is fixed to groupId, indicating that the value of the Target parameter is the ID of the asset group.
Target	String	The asset group ID.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeStratety
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
    "requestId": "751BEDD8-A16F-49CE-A3C4-605849645D79",
  "Strategies": [
      {
        "Name": "Threat Detection Service No. 12345",
        "RiskCount": 4,
        "CycleDays": 1,
        "CycleStartTime": 6,
        "Type": 2,
        "ProcessRate": 0,
        "ConfigTargets": [
          {
            "Flag": "add",
            "Target": "5078483",
            "TargetType": "groupId"
          }
        ],
        "Id": 36071,
        "ExecStatus": 1,
        "EcsCount": 2
      }
  ]
}
```


2.16.4.5.15. DescribeStrategyExecDetail

Description

You can call this operation to query the execution details of a baseline check policy.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeStrategyExecDetail*.
StrategyId	Integer	No	The ID of the baseline check policy.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
EndTime	String	The time when the baseline check was complete.
FailCount	Integer	The number of servers that failed to pass the check.
FailedEcsList	Array	A list of servers that failed to pass the check. For more information, see the following parameter descriptions.
Ip	String	The IP address of the server.
InstanceName	String	The instance name of the server.
IntranetIp	String	The private IP address of the server.
Reason	String	The reason that causes the baseline check failure.
InProcessCount	Integer	The number of servers that are being checked.
percent	String	The baseline check progress in percentage.
Source	String	The baseline check mode: automatic or manual.
StartTime	String	The time when the baseline check started.
SuccessCount	Integer	The number of servers that have passed the check.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeStrategyExecDetail
&StrategyId=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
    "requestId": "751BEDD8-A16F-49CE-A3C4-605849645D79",
     "Source": "Schedule",
     "InProcessCount": 0,
     "SuccessCount": 1,
     "Percent": 100,
     "EndTime": "2018-04-08 12:15:20",
     "FailedEcsList": [],
     "StartTime": "2018-04-08 12:15:10",
     "FailCount": 0,
}
```


2.16.4.5.16. DescribeRiskType

Description

You can call this operation to query all types of risks detected in baseline check and view the number of risks that have been detected by a baseline check policy or on the specified servers for a specific risk type.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeRiskType*.
StrategyId	Long	No	The ID of the baseline check policy.
Uuids	String	No	The UUID of the server. Multiple UUIDs are separated with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Count	Integer	The number of risk types.
RiskTypes	Array	A list of risk types. For more information, see the following parameter descriptions.
Alias	String	The name of the risk type.
TypeName	String	The code of the risk type.

Name	Type	Description
WarnCount	String	The number of risks that have been detected.
SubTypes	Array	A list of sub-risk types. For more information, see the following parameter descriptions.
Alias	String	The name of the sub-risk type.
TypeName	String	The code of the sub-risk type.
WarnCount	String	The number of risks that have been detected.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeRiskType
&StrategyId=10
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"11D3993A-02B8-4FD9-9116-922BCDE53A80",
 "RiskTypes":[
  {
   "TypeName":"system",
   "SubTypes":[
    {
     "TypeName":"group_policy",
     "Alias":"Group policy",
     "WarnCount":0
    },
    {
     "TypeName":"baseline",
     "Alias":"Baseline policy",
     "WarnCount":0
    },
    {
     "TypeName":"register",
     "Alias":"Registry",
     "WarnCount":0
    }
   ],
   "Alias":"System",
   "WarnCount":0
  }
 ],
 "count": 1,
}
```


2.16.4.5.17. Describesummary

Description

You can call this operation to query the risks detected in baseline check by risk type.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *Describesummary*.

Name	Type	Required	Description
PageSize	Integer	No	The number of records displayed on a page. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
Dealed	String	No	Indicates whether the risk has been handled. Valid values: • *Y*: indicates that the risk has been handled. • *N*: indicates that the risk has not been handled.
RiskLevels	String	No	The risk level. Separate multiple risk levels with commas (,).
RiskName	String	No	The name of the risk. Note Fuzzy match is supported.
StatusList	String	No	The status of the risk. Valid values: • *1*: indicates that the risk is pending. • *2*: indicates that the risk has been ignored. • *3*: indicates that the risk has been confirmed. • *8*: indicates that the risk has been marked as a false positive. • *16*: indicates that the risk is being handled. • *32*: indicates that the risk has been handled. You can specify multiple statuses and separate them with commas (,).
StrategyId	Long	No	The ID of the baseline check policy.
TypeNames	String	No	The type of the risk. Separate multiple risk types with commas (,).
SubTypeNames	String	No	The type of the sub-risk. Separate multiple sub-risk types with commas (,).
Uuids	String	No	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The number of returned records.
Count	Integer	The number of returned risk records.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
WarningSummarys	Array	A list of risks. For more information, see the following parameter descriptions.
LastFoundTime	String	The latest time when the risk was detected.
Level	String	The risk level.
PendingCount	Integer	The number of pending risks.
RiskDetail	String	The risk details.
RiskId	Long	The ID of the risk.
RiskName	String	The name of the risk.
TypeAlias	String	The type of the risk.
SubTypeAlias	String	The type of the sub-risk.
TotalCount	Integer	The total number of risks.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=Describesummary
&CurrentPage=20
&Dealed=Y
&PageSize=10
&StrategyId=1
&Uuid=2738e842-7d46-42f7-acb4-e6796b051ddc
&<Common request parameters>
```

- Sample responses (JSON format)


```
{
 "TotalCount":1,
 "PageSize":20,
 "RequestId":"38AAFEEE-F52F-4B2E-9F28-FC4A35F8D432",
 "CurrentPage":1,
 "count": 1,
 "WarningSummarys":[
  {
   "RiskId":1,
   "LastFoundTime":"2018-04-08 16:51:26",
   "RiskDetail":"The SSH logon security policy checks the following configurations: \n1. Checks whether the logon port is the default port 22\n2 and whether the root account is allowed\n3. Checks whether t he SSH V1 protocol is used\n4. Checks whether the RSH protocol is used\n5. Checks whether authenti cation-based logon is performed\n Solution: \n Edit /etc/ssh/sshd_config\n1. Port (not 22)\n2. Permit RootLogin (no)\n3. Protocol (2)\n4. IgnoreRhosts (yes)\n5. e) HostbasedAuthentication (no)
   "Level":"low",
   "TypeAlias":"System",
   "SubTypeAlias":"Baseline check policy",
   "RiskName":"SSH logon baseline check"
  }
 ]
}
```


2.16.4.5.18. OperateWarning

Description

You can call this operation to handle the risk alert records detected during the baseline check.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *OperateWarning*.
RiskWarningIds	String	No	The risk alert record ID. Separate multiple risk alert record IDs with commas (,).

Name	Type	Required	Description
OperateType	String	No	The type of the operation. Valid values: • *verify*: indicates an operation to verify the risk alert. • *ignore*: indicates an operation to ignore the risk alert. • *cancelIgnore*: indicates an operation to cancel the ignore operation on the risk alert. • *delete*: indicates an operation to delete the risk alert record.
Reason	String	No	The reason why the risk alert record is ignored if the OperateType parameter is set to ignore.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=OperateWarning
&OperateType=verify
&RiskWarningIds=22,45
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"38AAFEEE-F52F-4B2E-9F28-FC4A35F8D432"
}
```

2.16.4.5.19. ExportWarning

Description

You can call this operation to export risks that match the specified criteria from baseline check.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ExportWarning*.
IsSummaryExport	String	No	Indicates whether to export the summary page. Valid values: • *1*: exports the summary page. • *0*: does not export the summary page.
Dealed	String	No	Indicates whether the risk has been handled. Valid values: • *Y*: indicates that the risk has been handled. • *N*: indicates that the risk has not been handled.
RiskLevels	String	No	The risk level. Multiple risk levels are separated with commas (,).
RiskName	String	No	The name of the risk. Note Fuzzy match is supported.
StrategyId	Integer	No	The ID of the baseline check policy.
TypeNames	String	No	The risk type.
SubTypeNames	String	No	The sub-risk type.
Uuids	String	No	The UUID of the server. Multiple UUIDs are separated with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
FileName	String	The name of the exported file.
Id	Integer	The ID of the export task.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ExportWarning
&Dealed=n
&RiskLevels=serious,high,medium,low
&RiskName=Weak FTP password
&StrategyId=15161
&SubTypeNames=centos7
&TypeNames=cis
&Uuids=6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
    "FileName": "health_check_export_20180306",
    "RequestId": "F2F08DED-C788-430F-91F2-11991818BE2D",
    "Id": 16719
}
```

2.16.4.5.20. DescribeExportInfo

Description

You can call this operation to query the export task information, including the export progress and the download link of the exported file.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeExportInfo*.
ExportId	Long	No	The ID of the export task.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Parameter	Type	Description
CurrentCount	Integer	The number of records that have been exported.
FileName	String	The name of the exported file.
Id	Integer	The ID of the export task.
GmtCreate	Long	The time when the export task was created.
Link	String	The download link of the exported file.
Progress	Integer	The export progress.
TotalCount	Integer	The total number of records that have been exported.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeExportInfo
&ExportId=1
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "Link": "http://hc-export.oss-cn-shanghai.example.com/export_hc/health_check_export_20180303_1
520065303578.zip?Expires=1520670103&OSSAccessKeyId=<yourAccessKeyId>&Signature=xxxx%xxxx%3
D",
  "TotalCount": 82,
  "FileName": "health_check_export_20180303",
  "RequestId": "00F89798-3370-4C20-8506-B2BC3970EC5A",
  "CurrentCount": 82,
  "Id": 16678,
  "GmtCreate": 1520065302000,
  "Progress": 100
}
```

2.16.4.6. Unusual logon operations

2.16.4.6.1. DescribeBaseConfigs

Description

You can call this operation to query the logon security settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeBaseConfigs*.
Type	String	Yes	The type of the logon security configuration record. Valid values: • *login_common_location*: indicates an approved logon location. • *login_common_ip*: indicates an approved logon IP address. • *login_common_time*: indicates an approved logon time period. • *login_common_account*: indicates an approved logon account.
Target	String	No	The specified server. **Note** You must specify this parameter to query the logon security settings of a specified server. For more information about the format, see the sample request.
PageSize	Integer	No	The maximum number of records to be displayed on each page. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CurrentPage	Integer	The current page number.

Name	Type	Description
PageSize	Integer	The maximum number of records displayed on a page.
TotalCount	Integer	The total number of the returned records.
BaseConfigs	Array	The logon security settings. For more information, see the following parameter descriptions.
Account	String	The approved logon account.
EndTime	String	The end time of the approved logon time period.
Ip	String	The approved logon IP address.
Location	String	The approved logon location.
StartTime	String	The start time of the approved logon time period.
TotalCount	Integer	The total number of servers.
UuidCount	Integer	The number of servers to which the specified configuration record applies.
TargetList	Array	The information about servers to which the specified configuration record applies. For more information, see the following parameter descriptions.
TargetType	String	The type of the Target parameter value. Valid values: • *groupId*: indicates an asset group ID. • *uuid*: indicates a server UUID.
Target	String	The asset group ID or server UUID.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeBaseConfigs
&CurrentPage=1
&PageSize=20
&Target=[{"targetType":"uuid","target":"6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac"}]
&Type=login_common_location
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "BaseConfigs": [{
  "totalCount": 9,
  "location": "United States",
  "uuidCount": 1,
  "targetList": [{
   "target": "6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac",
   "targetType": "uuid"
  }]
 }],
 "TotalCount": 1,
 "PageSize": 5,
 "RequestId": "485ABE58-4E27-4416-997C-F8F3B8748EB6",
 "CurrentPage": 1
}
```


2.16.4.6.2. ModifyBaseConfig

Description

You can call this operation to modify logon security settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyBaseConfig*.
Type	String	Yes	The type of the logon security settings. Valid values: • *login_common_location*: indicates approved logon locations. • *login_common_ip*: indicates approved logon IP addresses. • *login_common_time*: indicates approved logon time periods. • *login_common_account*: indicates approved logon accounts.

Name	Type	Required	Description
Target	String	No	The target server. Note You must set this parameter when you need to query the logon security settings for a server. For more information about the format, see the following sample request.
Config	String	No	The logon security settings. The formats for all the settings are as follows: • Approved logon locations: `{"location":"Ganzhou City"}` • Approved logon IP addresses: `{"ip":"x.x.x.x"}` • Approved logon time periods: `{"startTime":"16:18","endTime":"16:18"}` • Approved logon accounts: `{"account":"dbaadmin"}`

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyBaseConfig
&Config={"startTime":"16:18","endTime":"16:18"}
&Target=[{"targetType":"uuid","target":"0c797eb1-e6b9-4b5a-8917-a7e6cbbb4b2e","flag":"add"},{"targetType":"uuid","target":"1759b0ea-6dd7-438b-b60d-c90179bd9ebc","flag":"del"}]
&Type=login_common_location
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"BB8F5902-BD50-49AB-B124-18E9CA92BB99"
}
```

2.16.4.6.3. DeleteBaseConfig

Description

You can call this operation to delete a logon security setting, such as an approved logon location or IP address.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DeleteBaseConfig*.
Config	String	Yes	The logon security setting. The formats of the logon security settings and examples are as follows: • Approved logon location: `{"location":"Ganzhou City"}` • Approved logon IP address: `{"ip":"x.x.x.x"}` • Approved logon time range: `{"startTime":"16:18","endTime":"16:18"}` • Approved logon account: `{"account":"dbaa****"}`
Type	String	Yes	The type of the logon security setting. Valid values: • *login_common_location*: indicates an approved logon location. • *login_common_ip*: indicates an approved logon IP address. • *login_common_time*: indicates an approved logon time range. • *login_common_account*: indicates an approved logon account.

Parameter	Type	Required	Description
Target	String	No	The target server. Note You must set this parameter if you want to delete a logon security setting for a server. For more information about the format, see the following sample request.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DeleteBaseConfig
&Config={"location":"Ganzhou City"}
&Target=[{"targetType":"uuid","target":"6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac"}]
&Type=login_common_location
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"E3785090-CFF4-4C53-82E4-08F902586053"
}
```

2.16.4.6.4. DescribeSwitchConfigs

Description

You can call this operation to query the logon security configuration records in the logon security settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeSwitchConfigs*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Count	Integer	The total number of returned records.
ConfigList	Array	The statuses of the logon security configuration items. For more information, see the following parameter descriptions.
Item	String	The logon security configuration items. Valid values: • *login_common_location*: indicates an approved logon location. • *login_common_ip*: indicates an approved logon IP address. • *login_common_time*: indicates an approved logon time range. • *login_common_account*: indicates an approved logon account.
Status	Integer	The status of the configuration item. Valid values: • *1*: indicates enabled. • *0*: indicates disabled.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeSwitchConfigs
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "Count":3,
 "RequestId":"3F2C126D-870B-4AE4-8604-58BDECF873F4",
 "ConfigList":[
  {
   "Status":1,
   "Item":"login_common_ip"
  },
  {
   "Status":0,
   "Item":"login_common_account"
  },
  {
   "Status":0,"Item":"login_common_time"
  }
 ]
}
```


2.16.4.6.5. ModifySwitchConfig

Description

You can call this operation to modify the setting about whether to enable a logon security configuration record to identify a valid logon to a server in the logon security settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifySwitchConfig*.
Item	String	Yes	The logon security configuration items. Valid values: • *login_common_location*: indicates an approved logon location. • *login_common_ip*: indicates an approved logon IP address. • *login_common_time*: indicates an approved logon time range. • *login_common_account*: indicates an approved logon account.

Name	Type	Required	Description
Status	Integer	Yes	The status of the logon security configuration switch. Valid values: • *1*: indicates enabled. • *0*: indicates disabled.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Count	Integer	The total number of returned records.
ConfigList	Array	The status of the logon security configuration switch. For more information, see the following parameter descriptions.
Item	String	The logon security configuration items. Valid values: • *login_common_location*: indicates an approved logon location. • *login_common_ip*: indicates an approved logon IP address. • *login_common_time*: indicates an approved logon time range. • *login_common_account*: indicates an approved logon account.
Status	Integer	The status of the logon security configuration switch. Valid values: • *1*: indicates enabled. • *0*: indicates disabled.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifySwitchConfig
&Item=login_common_location
&Status=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"3F2C126D-870B-4AE4-8604-58BDECF873F4"
}
```

2.16.4.6.6. DescribeConfigTarget

Description

You can call this operation to query the information about servers to which a specified logon security configuration record applies.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeConfigTarget*.
Type	String	Yes	The logon security configuration record used to identify a valid logon to a server. Valid values: • *login_common_location*: indicates an approved logon location. • *login_common_ip*: indicates an approved logon IP address. • *login_common_time*: indicates an approved logon time range. • *login_common_account*: indicates an approved logon account.
Target	String	No	The specified server. **Note** You need to specify this parameter to query the logon security configuration records of a specified server. For more information about the format, see the sample request.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Count	Integer	The total number of returned records.

Name	Type	Description
TargetList	Array	The information about server to which the specified configuration record applies. For more information, see the following parameter descriptions.
TargetType	String	The type of the Target parameter value. Valid values: • *groupId*: indicates an asset group ID. • *uuid*: indicates a server UUID.
Target	String	The asset group ID or server UUID.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeConfigTarget
&Config={"uuidCount":1,"location":"Ganzhou"}
&Target=[{"targetType":"uuid","target":"6dbdbfe7-06fa-4d9a-8268-ce2dc6d673ac"}]
&Type=login_common_location
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "TargetList": [{
   "Target": "inet-e53455ec-a134-4d46-9ff5-c4f3a5fe0f02",
   "TargetType": "uuid"
  }, {
   "Target": "inet-25f4ef74-29c7-49fd-85cc-b4543a2489a8",
   "TargetType": "uuid"
  }
 "Count": 2,
 "RequestId": "B8064EA4-9472-4D03-B7D1-6684DB5CD0BE",
}
```

2.16.4.7. Webshell detection operations

2.16.4.7.1. DescribeWebPath

Description

You can call this operation to query the Web directories defined in webshell settings.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeWebPath*.
PageSize	Integer	No	The number of records to return on each page. Default value: *20*.
CurrentPage	Integer	No	The number of the page to return. Default value: *1*.
Type	String	No	The type of the settings. Set this parameter to *web_path* to specify the Web directory settings.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The number of returned records.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
Count	Integer	The number of Web directories.
ConfigList	Array	The Web directories. For more information, see the following descriptions.
WebPath	String	The path of the Web directory.
TargetList	Array	The servers that the Web directory has been applied to. For more information, see the following descriptions.
TargetType	String	This parameter always returns a value of uuid, which means that the Target parameter returns the universally unique identifier (UUID) of the server.
Target	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeWebPath
&<Common request parameters>
```

- Sample response (JSON format)

```
{
 "TotalCount":1,
 "PageSize":5,
 "RequestId":"7B6AD7C9-0F8D-4126-B8AA-6DC308B0B534",
 "CurrentPage":1,
 "Count":1,
 "ConfigList":[
  {
   "TargetList":[
    {
     "Target":"inet-f6ac9a93-0818-4052-90e2-d24f18ee198b",
     "TargetType":"uuid"
    }
   ],
   "WebPath":"/usr/local/tomcat/webroot18"
  }
 ]
}
```

2.16.4.7.2. ModifyWebPath

Description

You can call this operation to modify the Web directory in webshell settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyWebPath*.

Name	Type	Required	Description
Type	String	No	The configuration type. Set the value to *web_path*, indicating the web directory configuration.
Config	String	No	The Web directory configuration, in JSON format. For more information, see the sample request.
Target	String	No	The list of target servers to which the Web directory configuration applies, in JSON format. For more information, see the sample request.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=ModifyWebPath
&Type=web_path
&Config={"webPath":"/test"}
&Target={"targetType":"uuid","target":"0c797eb1-e6b9-4b5a-8917-a7e6cbbb4b2e","flag":"add"}
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"7B6AD7C9-0F8D-4126-B8AA-6DC308B0B534"
}
```

2.16.4.7.3. DescribeCategoryCount

Description

You can call this operation to query the number of webshells detected by Server Guard.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeCategoryCount*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Webshell	Integer	The number of webshells.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeCategoryCount
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "43F670F3-AB40-4E91-BC7D-C57468834F67",
  "Webshell": 2
}
```

2.16.4.7.4. DescribeWebshell

Description

You can call this operation to query records of webshell files that have been detected by Server Guard, including the detection time and webshell file path.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeWebshell*.

Parameter	Type	Required	Description
GroupId	Integer	No	The ID of the asset group.
Mark	String	No	The IP address or instance name of the server.
Tag	Integer	No	The server tag ID.
Dealed	String	No	The status of the webshell event. Valid values: • *n*: indicates that the event is pending. • *y*: indicates that the event has been handled.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
WebshellList	Array	The webshell events. For more information, see the following descriptions.
Os	String	The operating system of the server.
InstanceName	String	The instance name of the server.
GroupId	Long	The ID of the asset group.
Ip	String	The IP address of the server. Note The public IP address of the server is displayed preferentially. If no public IP address is assigned to the server, the private IP address of the server is displayed.
Uuid	String	The universally unique identifier (UUID) of the server.
FoundTime	String	The time when the webshell file was detected.
InstanceId	String	The instance ID of the server.
TrojanType	String	The type of the webshell file.
FirstFoundTime	String	The time when the webshell file was detected for the first time.
TrojanSize	Long	The size of the webshell file.

Parameter	Type	Description
Domain	String	The domain name associated with the server.
TrojanPath	String	The path of the webshell file.
Region	String	The region where the server resides.
Status	Integer	The status of the webshell event. Valid values: • *1*: indicates that the event is pending. • *2*: indicates that the event has been ignored. • *3*: indicates that the event has been confirmed. • *8*: indicates that the event has been labeled as a false positive. • *16*: indicates that the event is being handled. • *32*: indicates that the event has been handled.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeWebshell
&Dealed=n
&GroupId=1
&Remark=xx.xx.xx.xx
&Tag=11
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "WebshellList": [{
    "Uuid": "aa46dbe9-d35d-4b77-a4d9-10bc6b1b****",
    "FoundTime": "2018-02-27 03:23:18",
    "Ip": "xx.xx.xx.xx",
    "FirstFoundTime": "2017-12-24 03:36:03",
    "Domain": "",
    "TrojanType": "Webshell",
    "InstanceId": "i-bp15xtqydmbujgep****",
    "TrojanPath": "c:/zhb/wamp/wamp/www/My.php",
    "GroupId": 3259405,
    "Os": "windows",
    "Status": 1,
    "Region": "cn-hangzhou-dg-a01",
    "TrojanSize": 0,
    "InstanceName": "win08****"
  }, {
    "Uuid": "aa46dbe9-d35d-4b77-a4d9-10bc6b1bb610",
    "FoundTime": "2017-12-25 03:53:22",
    "Ip": "x.x.x.x",
    "FirstFoundTime": "2017-12-24 03:36:01",
    "Domain": "",
    "TrojanType": "Webshell",
    "InstanceId": "i-bp15xtqydmbujgepdbev",
    "TrojanPath": "c:/zhb/wamp/../wamp/wamp/www/abc/My.php",
    "GroupId": 3259405,
    "Os": "windows",
    "Status": 9,
    "Region": "cn-hangzhou-dg-a01",
    "TrojanSize": 0,
    "InstanceName": "win08-zhb"
  }],
  "RequestId": "E4B254AE-5CB1-4810-8B51-A08DF5697F25"
}
```


2.16.4.7.5. OperateTrojan

Description

You can call this operation to handle detected webshells.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *OperateTrojan*.
Info	String	No	The webshell information, in JSON format. For more information, see the sample request.
OperateType	String	No	The type of the operation. Valid values: • *isolate*: indicates an operation to quarantine the file. • *trust*: indicates an operation to trust the file. • *untrust*: indicates an operation to cancel trusting the file. • *restore*: indicates an operation to restore the file.
Type	Integer	No	The type of the trojan. Set the value to *1*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
FailedCount	Integer	The number of failed operations.
SuccessCount	Integer	The number of successful operations.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=OperateTrojan
&Info=[{"uuid":"97988c2b-de9d-4159-90ab-7cc73561c64c","filePath":"/home/test/Z02.php","webshellId"
:""}]
&OperateType=trust
&Type=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "43F670F3-AB40-4E91-BC7D-C57468834F67",
  "FailedCount": 0,
  "SuccessCount": 1
}
```

2.16.4.7.6. DescribeQuaraFile

Description

You can call this operation to obtain the list of quarantined files.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeQuaraFile*.
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query result. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of returned records.
CurrentPage	Integer	The current page number.

Name	Type	Description
PageSize	Integer	The maximum number of records displayed on a page.
QuaraFiles	Array	The list of quarantined files. For more information, see the following parameter descriptions.
EventName	String	The name of the unusual event.
EventType	String	The type of the unusual event.
FileStatus	String	The status of the quarantined file. Valid values: • *quaraFailed*("0"): indicates that the file failed to be quarantined. • *rollbackFailed*("1"): indicates that the file failed to be rolled back to a previous version. • *quaraDone*("2"): indicates that the file has been quarantined. • *rollbackDone*("3"): indicates that the file has been rolled back to a previous version. • *quaraing*("4"): indicates that the file is being quarantined. • *rollbacking*("5"): indicates that the file is being rolled back to a previous version.
Md5	String	The MD5 value of the file.
Online	Boolean	Indicates whether the Server Guard agent on the server is online.
Path	String	The file path.
Tag	String	The unique identifier of the unusual event.
Uuid	String	The UUID of the server.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeQuaraFile
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "TotalCount":1,
  "PageSize":20,
  "RequestId":"0C7FAD74-83FA-4671-9250-A5F2A64F437A",
  "CurrentPage":1,
  "QuaraFiles":[
    {
      "Path":"/bin/ping",
      "Uuid":"9b0c4d55-2f1f-4766-a90a-2c9d8a0b7642",
      "FileStatus":"quaraDone",
      "EventType":"Parent class of cloud scanning events (test ping)",
      "EventName":"Sub-class of cloud scanning events (test ping)",
      "Tag":"1d791175ad0bffd973b039248d6086e0",
      "Online":false,
      "Md5":"1421d9ad2b0031483f396154d48161f1"
    }
  ]
}
```


2.16.4.7.7. RollbackQuaraFile

Description

You can call this operation to restore a specified quarantined file.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *RollbackQuaraFile*.
EventName	String	No	The name of the unusual event.
EventType	String	No	The type of the unusual event.
Tag	String	No	The GUID of the unusual event.
Uuid	String	No	The UUID of the server.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=RollbackQuaraFile
&EventName=DDoS trojan
&EventType=Malicious process
&Tag=a50f96f958fbd59f68e4bca4d90679d6
&Uuid=00f11fcb-1a9a-4fd5-a48a-e0e5bd12a6a4
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"0C7FAD74-83FA-4671-9250-A5F2A64F437A",
}
```

2.16.4.8. Server exception detection operations

2.16.4.8.1. DescribeSuspEventTypes

Description

You can call this operation to query the unusual event types.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeSuspEventTypes*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Name	Type	Description
TotalCount	Integer	The total number of returned records.
EventTypes	Array	The list of unusual event types. For more information, see the following parameter descriptions.
AliseEventType	String	The name of the unusual event type.
EventType	String	The identifier of the unusual event type.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeSuspEventTypes
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "TotalCount":1,
 "RequestId":"66BE7091-BC00-4943-8A0D-B3DCE90AD7B5",
 "EventTypes":[
  {
   "EventType":"Suspicious process",
   "AliseEventType":"Suspicious process"
  }
 ]
}
```

2.16.4.8.2. DescribeSuspTrendStatistics

Description

You can call this operation to query the chart data on different types of unusual server events on each day.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeSuspTrendStatistics*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Interval	Integer	The time length of the the time frame specified for query.
StartTime	Integer	The start time of the time frame specified for query.
SuspiciousItems	List	The statistics on numbers of different types of suspicious events.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeSuspTrendStatistics
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"66BE7091-BC00-4943-8A0D-B3DCE90AD7B5",
 "Start":-28800000,
 "Interval":86400000,
 "SuspiciousItems":[ ]
}
```

2.16.4.8.3. OperateSuspiciousEvent

Description

You can call this operation to handle detected unusual events.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *OperateSuspiciousEvent*.
Data	String	No	The unusual event to be handled, in JSON format. For more information, see the sample request.
OperateType	String	No	The type of the operation. Valid values: • *deal*: indicates an operation to handle the unusual event. • *confirm*: indicates an operation to mark the unusual event as handled. • *mark_misinformation*: indicates an operation to mark the unusual event as false positive. • *unmark_misinformation*: indicates an operation to remove the false positive mark of the unusual event. • *ignore*: indicates an operation to ignore the unusual event.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=OperateSuspiciousEvent
&OperateType=ignore
&Data={"uuid":"97988c2b-de9d-4159-90ab-7cc73561c64c","tag":"f87eb0ee5934f6f65343ec601ce71c2f","eventType":"Malicious processes (malware checking)","eventName":"DDoS Trojan},{"uuid":"97988c2b-de9d-4159-90ab-7cc73561c64c","tag":"95347a77b8c0d6dae99a23ab69aa90f4","eventType":"Malicious processes (malware checking)","eventName":"GateDDoS Trojan"}
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"654A6FD8-B55D-4D6B-AAFF-4122503D108B"
}
```

2.16.4.8.4. OperateLoginLog

Description

You can call this operation to label a detected unusual logon event as handled.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *OperateLoginLog*.
Ids	String	Yes	The ID of the unusual logon log. Separate multiple log IDs with commas (,).
OperateType	String	Yes	The type of the operation. Set the value to *confirm*, indicating that the event has been handled.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=OperateLoginLog
&Ids=2006434
&OperateType=confirm
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"BE391ABB-6B7C-4C41-9F6C-862C1DEE3905"
}
```

2.16.4.8.5. CreateSuspiciousExport

Description

You can call this operation to export the information about unusual events on servers based on search conditions.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateSuspiciousExport*.
Dealed	String	No	Indicates whether the unusual event has been handled. Valid values: • *Y*: indicates that the event has been handled. • *N*: indicates that the event has not been handled.
EventNameRemark	String	No	The name of the event. Fuzzy matching is supported.
EventType	String	No	The name of the event type. Valid values: • *Unusual logon* • *Suspicious process* • *Suspicious account* • *Sensitive file tampering* • *Suspicious network connection* • *Unusual event* • *Suspicious file* • *Malicious process*
GroupId	String	No	The ID of the asset group.

Name	Type	Required	Description
Level	String	No	The risk level of the event. Valid values: • *Critical*: indicates a critical-risk event. • *Important*: indicates an important-risk event. • *Moderate*: indicates a moderate-risk event. • *low*: indicates a low-risk event. You can specify multiple event levels and separate them with commas (,).
Remark	String	No	The name or IP address of the server. Fuzzy matching is supported.
StatusList	String	No	The handling status of the event. Valid values: • *1*: indicates that the event is to be handled. • *2*: indicates that the event has been ignored. • *3*: indicates that the event has been confirmed. • *8*: indicates that the event has been labeled as a false positive. • *16*: indicates that the event is being handled. • *32*: indicates that the event has been handled. You can specify multiple statuses and separate them with commas (,).
Tag	String	No	The tag of the server.
Uuids	String	No	The UUID of the server. Separate multiple UUIDs with commas (,).

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
FileName	String	The name of the exported file.
Id	Long	The ID of the export task.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=CreateSuspiciousExport
&Remark=23
&EventType=Suspicious process
&Level=serious,high,medium,low
&Dealed=n
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
   "RequestId": "43F670F3-AB40-4E91-BC7D-C57468834F67",
   "FileName": "suspicious_20180408",
   "Id": 387
}
```

2.16.4.8.6. DescribeSuspiciousExportInfo

Description

You can call this operation to query an unusual event export task.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeSuspiciousExportInfo*.
ExportId	Long	No	The ID of the export task.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentCount	Integer	The number of records that have been exported.

Parameter	Type	Description
ExportStatus	String	The status of the export task. Valid values: • *init*: indicates that the export task is being initialized. • *pending*: indicates that the export task is pending. • *exporting*: indicates that the export task is being executed. • *success*: indicates that the export task has been completed. • *fail*: indicates that the export task has failed.
Message	String	The status description or failure information of the export task.
FileName	String	The name of the exported file.
Id	Integer	The ID of the export task.
GmtCreate	Long	The time when the export task was created.
Link	String	The download link of the exported file.
Progress	Integer	The export progress.
TotalCount	Integer	The total number of records that have been exported.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://aegis.[ RegionId].example.com/?Action=DescribeSuspiciousExportInfo
&ExportId=1
&<Common request parameters>
```

- Sample response (JSON format)

```
{
 "TotalCount":30,
 "GmtCreate":1518071546000,
 "Progress":100,
 "Message":"success",
 "RequestId":"654A6FD8-B55D-4D6B-AAFF-4122503D108B",
 "FileName":"suspicious_20180208",
 "ExportStatus":"success",
 "CurrentCount":30,
 "Id":11,
 "Link":"http://suspicious-export.oss-cn-shanghai.example.com/export/suspicious_20180208_1518071
576098.zip?Expires=1518075176&OSSAccessKeyId=<yourAccessKeyId>&Signature=xxxx%xxxx%3D"
}
```


2.16.4.8.7. DescribeVirusInfo

Description

You can call this operation to upload the MD5 values of files and use Alibaba Cloud Antivirus to determine whether the files are malicious programs.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeVirusInfo*.
Md5	String	Yes	The MD5 value of the file.
Lang	String	No	The language attribute of the file, such as *zh*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Name	Type	Description
Data	Boolean	Indicates whether the file is malicious. Valid values: • True: Indicates that the file is malicious. • False: Indicates that the file is not malicious.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].aliyuncs.com/?Action= DescribeVirusInfo
&Md5=6f6628d923f9018b28acc5f905e03244
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId": "A2423F39-3272-4491-804E-D0EBDE3E894D",
 "Data": true
}
```

2.16.4.9. Server log retrieval operations

2.16.4.9.1. CreateLogQuery

Description

You can call this operation to create or save server log search conditions.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateLogQuery*.
Conditions	String	No	The log search condition.
QueryDetail	String	No	The log search sub-conditions.
QueryName	String	No	The saved search name.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=CreateLogQuery
&Conditions=aegis-log-login@warn_port:22
&QueryDetail=[[{"itemForm":{},"d":{"name":"Logons","id":"aegis-log-login","fields":[{"name":"ip","type"
:"string","desc":"IP address","text":"IP(IP address)"}]]
&QueryName=test
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"415AE1FC-3C11-4AA9-A06F-DE13D3430366"
}
```

2.16.4.9.2. DescribeLogQuery

Description

You can call this operation to query the saved server log search conditions.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeLogQuery*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
ListTotal	Integer	The total number of returned records.

Name	Type	Description
QueryItems	Array	The details of log search conditions. For more information, see the following parameter descriptions.
Conditions	String	The log search conditions.
QueryDetail	String	The log search sub-conditions.
QueryName	String	The name of the log search task.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeLogQuery
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"65802B9B-4D30-40F0-8691-F126652DBEBE",
 "ListTotal":1,
 "QueryItems":[
  {
   "QueryDetail":"[[{\"itemForm\":{},\"d\":{\"name\":\"Account snapshot\",\"id\":\"aegis-snapshot-host\",\"fields\":[{\"name\":\"ip\",\"type\":\"string\",\"desc\":\"IP address\"},{\"name\":\"uuid\",\"type\":\"string\",\"desc\":\"Client ID\"},{\"name\":\"perm\",\"type\":\"string\",\"desc\":\"Root permission availability\"},{\"name\":\"home_dir\",\"type\":\"string\",\"desc\":\"Home directory\"},{\"name\":\"warn_time\",\"type\":\"string\",\"desc\":\"Password expiration reminder time\"},{\"name\":\"groups\",\"type\":\"array\",\"desc\":\"User group\"},{\"name\":\"login_ip\",\"type\":\"string\",\"desc\":\"Last logon IP\"},{\"name\":\"last_chg\",\"type\":\"string\",\"desc\":\"Last password change time\"},{\"name\":\"shell\",\"type\":\"string\",\"desc\":\"Linux shell command\"},{\"name\":\"domain\",\"type\":\"string\",\"desc\":\"Windows domain\"},{\"name\":\"tty\",\"type\":\"string\",\"desc\":\"Logon terminal\"},{\"name\":\"account_expire\",\"type\":\"string\",\"desc\":\"Account expiration time\"},{\"name\":\"passwd_expire\",\"type\":\"string\",\"desc\":\"Password expiration time\"},{\"name\":\"last_logon\",\"type\":\"string\",\"desc\":\"Last logon time\"},{\"name\":\"user\",\"type\":\"string\",\"desc\":\"User\"},{\"name\":\"status\",\"type\":\"string\",\"desc\":\"User status: 0-disabled, 1-enabled\"}]},\"searchFields\":[{\"name\":\"ip\",\"type\":\"string\",\"desc\":\"IP address\"},{\"name\":\"uuid\",\"type\":\"string\",\"desc\":\"Client ID\"},{\"name\":\"perm\",\"type\":\"string\",\"desc\":\"Root permission availability\"},{\"name\":\"home_dir\",\"type\":\"string\",\"desc\":\"Home directory\"},{\"name\":\"warn_time\",\"type\":\"string\",\"desc\":\"Password expiration reminder time\"},{\"name\":\"groups\",\"type\":\"array\",\"desc\":\"User group\"},{\"name\":\"login_ip\",\"type\":\"string\",\"desc\":\"Last logon IP\"},{\"name\":\"last_chg\",\"type\":\"string\",\"desc\":\"Last password change time\"},{\"name\":\"shell\",\"type\":\"string\",\"desc\":\"Linux shell command\"},{\"name\":\"domain\",\"type\":\"string\",\"desc\":\"Windows domain\"},{\"name\":\"tty\",\"type\":\"string\",\"desc\":\"Logon terminal\"},{\"name\":\"account_expire\",\"type\":\"string\",\"desc\":\"Account expiration time\"},{\"name\":\"passwd_expire\",\"type\":\"string\",\"desc\":\"Password expiration time\"},{\"name\":\"last_logon\",\"type\":\"string\",\"desc\":\"Last logon time\"},{\"name\":\"user\",\"type\":\"string\",\"desc\":\"User\"},{\"name\":\"status\",\"type\":\"string\",\"desc\":\"User status: 0-disabled, 1-enabled\"}],\"f\":{\"name\":\"ip\",\"type\":\"string\",\"desc\":\"IP address\"},\"searchLimit\":[{\"name\":\"Including\",\"value\":\":\"}],\"l\":\":\",\"kw\":\"string\"}]]",
   "Conditions":"aegis-snapshot-host@ip:string",
   "QueryName":"aa"
  }

 ]
}
```


2.16.4.9.3. DeleteLogQuery

Description

You can call this operation to delete the saved server log search conditions.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteLogQuery*.
QueryName	String	No	The name of the saved search.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DeleteLogQuery
&QueryName=test
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"415AE1FC-3C11-4AA9-A06F-DE13D3430366"
}
```

2.16.4.9.4. DescribeFilterFields

Description

You can call this operation to query the filter fields of a specified server log search condition.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeFilterFields*.
Query	String	No	The log search condition.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Total	String	The total number of search conditions.
LogFilterList	Array	The filter field information. For more information, see the following parameter descriptions.
Fields	String	The filter fields.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeFilterFields
&Query=aegis-log-login@warn_port:22
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "LogFilterList":[
  {
   "Fields":"IP;IP address,UUID;Client ID","fieldsName":"default"
  }
 ],
 "Total":"20",
 "RequestID":"883e1e3d-4443-4206-871c-6c0625c01332"
}
```

2.16.4.9.5. DescribeHistogram

Description

You can call this operation to obtain the statistics on server logs generated within a specified time frame.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeHistogram*.
Query	String	Yes	The log query conditions.
EndTime	String	Yes	The end time of the time frame specified for query.
StartTime	String	Yes	The start time of the time frame specified for query.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Categories	String	The timeline information.
Items	Array	The log quantity statistics. For more information, see the following parameter descriptions.
Data	List	The number of logs.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeHistogram
&EndTime=2018-03-03 17:41:03
&Query=aegis-log-login@warn_port:22
&StartTime=2018-03-02 17:41:03
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"82D245FB-7A5D-4155-B59F-5B084CE93B6B",
 "Categories":[
  "1519983663000,1519984800000",
  "1519984800000,1519986600000",
  "1519986600000,1519988400000",
  "1519988400000,1519990200000",
  "1519990200000,1519992000000",
  "1519992000000,1519993800000",
  "1519993800000,1519995600000"
 ],
 "Items":[
  {
   "Data":[
    0,
    0,
    0,
    0,
    0,
    0,
    0
   ]
  }
 ]
}
```


2.16.4.9.6. DescribeLogInfo

Description

You can call this operation to query the server log fields based on specified query conditions.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeLogInfo*.

Name	Type	Required	Description
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query result. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
Query	String	Yes	The log query conditions.
EndTime	String	Yes	The end time of the query.
StartTime	String	Yes	The start time of the query.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The total number of returned records.
LogInfoItems	Array	The information about server log fields. For more information, see the following parameter descriptions.
Id	String	The ID of the log source.
Name	String	The name of the log source.
Fields	Array	The list of server log fields. For more information, see the following parameter descriptions.
Name	String	The ID of the log field.
Desc	String	The name of the log field.
Type	String	The type of the log field.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeLogInfo
&CurrentPage=1
&EndTime=2018-03-03 17:41:03
&PageSize=20
&Query=aegis-log-login@warn_port:22
&StartTime=2018-03-02 17:41:03
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "TotalCount":1,
  "RequestId":"3A7CFB73-C24C-4711-B7D9-2BE74EBFFE78",
  "LogInfoItems":[
    {
      "Fields":[
        {
          "Desc":"IP address",
          "Type":"string",
          "Name":"ip"
        },
        {
          "Desc":"Client number",
          "Type":"string",
          "Name":"uuid"
        },
        {
          "Desc":"Logon source IP address",
          "Type":"string",
          "Name":"warn_ip"
        },
        {
          "Desc":"Logon port",
          "Type":"string",
          "Name":"warn_port"
        },
        {
          "Desc":"Logon username",
          "Type":"string",
          "Name":"warn_user"
        },
```

```
            {
                "Desc":"Logon type",
                "Type":"string",
                "Name":"warn_type"
            },
            {
                "Desc":"Logon count",
                "Type":"string",
                "Name":"warn_count"
            }
        ],
        "Id":"aegis-log-login",
        "Name":"Logon serial number"
    },
  ]
}
```


2.16.4.9.7. DescribeLogItems

Description

You can call this operation to query the server log details that are returned by a query.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeLogItems*.
PageSize	Integer	No	The number of records displayed on a page. Default value: *20*.
CurrentPage	Integer	No	The current page number. Default value: *1*.
Query	String	No	The log query criterion.
AccountSnapshotOffset	Integer	No	The offset of the account snapshot log.
CrackOffset	Integer	No	The offset of the brute force password cracking log.

Name	Type	Required	Description
LoginOffset	Integer	No	The offset of the logon log.
NetworkOffset	Integer	No	The offset of the network connection log.
PortSnapshotOffset	Integer	No	The offset of the listening port snapshot log.
ProcessOffset	Integer	No	The offset of the process startup log.
ProcessSnapshotOffset	Integer	No	The offset of the process snapshot log.
EndTime	String	Yes	The end time of the time frame specified for query.
StartTime	String	Yes	The start time of the time frame specified for query.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
TotalCount	Integer	The number of returned records.
CurrentPage	Integer	The current page number.
SetPageSize	Integer	The maximum number of records displayed on a page.
AccountSnapshotOffset	Integer	The offset of the account snapshot log.
AccountSnapshotTotalCount	Integer	The total number of account snapshot log entries.
CrackOffset	Integer	The offset of the brute force password cracking log.
CrackTotalCount	Integer	The total number of brute force password cracking log entries.
LoginTotalCount	Integer	The total number of logon log entries.
NetworkOffset	Integer	The offset of the network connection log.
NetworkTotalCount	Integer	The total number of network connection log entries.
PortSnapshotOffset	Integer	The offset of the listening port snapshot log.

Name	Type	Description
PortSnapshotTotalCount	Integer	The total number of listening port snapshot log entries.
ProcessOffset	Integer	The offset of the process startup log.
ProcessTotalCount	Integer	The total number of process startup log entries.
ProcessSnapshotOffset	Integer	The offset of the process snapshot log.
ProcessSnapshotTotalCount	Integer	The total number of process snapshot log entries.
LogsList	Array	A list of host log details. For more information, see the following parameter descriptions.
LogSourceID	String	The ID of the log source.
LogSource	String	The name of the log source.
MLogTime	String	The time when the log entry was created.
MContents	Array	A list of host log entries. For more information, see the following parameter descriptions.
MKey	String	The log entry.
MValue	String	The value of the log entry.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://aegis.[ RegionId].example.com/?Action=DescribeLogItems
&CurrentPage=1
&PageSize=100
&AccountSnapshotOffset=1000
&CrackOffset=1000
&EndTime=2018-03-05 11:46:07
&LoginOffset=1000
&NetworkOffset=1000
&PortSnapshotOffset=1000
&ProcessOffset=1000
&ProcessSnapshotOffset=1000
&Query=aegis-log-login@warn_port:22
&StartTime=2018-03-02 17:41:03
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"BE391ABB-6B7C-4C41-9F6C-862C1DEE3905",
 "PageSize":100,
 "AccountSnapshotTotalCount":0,
 "LogsList":[],
 "CrackOffset":0,
 "ProcessOffset":0,
 "NetworkOffset":0,
 "ProcessSnapshotOffset":0,
 "LoginTotalCount":0,
 "CurrentPage":1,
 "PortSnapshotOffset":0,
 "NetworkTotalCount":0,
 "AccountSnapshotOffset":0,
 "CrackTotalCount":0,
 "PortSnapshotTotalCount":0,
 "ProcessSnapshotTotalCount":0,
 "ProcessTotalCount":0
}
```

2.16.5. Anti-DDoS

2.16.5.1. List of operations

This topic introduces all the Apsara Stack Security Anti-DDoS operations that you can call. For more information, see the corresponding operation description.

Operation	Description
CheckIpSegment	Checks whether a CIDR block to be added for monitoring is valid.
DescribeRegionName	Queries the regions of the CIDR blocks where traffic data collection and analysis is performed.
CreateIpSegment	Adds a specified CIDR block to be monitored.
DescribeIpSegment	Obtains a list of CIDR blocks under traffic monitoring.
DeleteIpSegment	Deletes a CIDR block whose traffic is collected and monitored based on the CIDR block record ID.
ModifyIpSegment	Modifies a monitored CIDR block with a specified record ID.
CreateDdosPolicy	Adds an anti-DDoS policy for a specified IP address or CIDR block.
DescribeDdosPolicies	Queries the configured DDoS protection policies.
DeleteDdosPolicy	Deletes an anti-DDoS policy for a specified CIDR block.
ModifyDdosPolicy	Modifies a specified anti-DDoS policy.
DescribeBlockSwitchs	Queries the status of the traffic block switch in anti-DDoS.
ModifyBlockSwitchs	Changes the status of the block switch in DDoS settings.
DescribeDdosEvents	Obtains the list of DDoS events that meet the specified search criteria.
DescribeFlowAnalysisResult	Queries the analysis result of the traffic sent to an IP address.
DescribeFlowDetails	Queries the detailed traffic information for a specified IP address.
CancelCleanStatus	Disables DDoS traffic scrubbing for a specified IP address.
CreateWhiteList	Adds a whitelist of trusted IP addresses that are exempt from traffic security monitoring.
DescribeWhiteList	Queries the IP addresses that have been added to a whitelist.
DeleteWhiteList	Deletes multiple risks from the whitelist for baseline check.
DescribeConsoleDdosPolicies	Obtains the records of anti-DDoS policies, including the system default policies.

2.16.5.2. Make API requests

2.16.5.2.1. Request structure

Apsara Stack Security API is based on Remote Procedure Call (RPC). This topic describes the structure of the API requests.

Description

You can send an HTTP request to call an API operation. The URL of the request must be in the following format:

```
http://endpoint/?Action=xx&parameters
```

Where:

- `endpoint`: the endpoint used to call a cloud service. The endpoint for the Anti-DDoS service is `ddosprivate.[ RegionId].example.com`.
- `Action`: the operation that you want to perform.

  For example, you can set this parameter to DescribeFeatures to query the deployed Apsara Stack Security features.
- `parameters`: the request parameters. Request parameters include common request parameters and custom request parameters. Request parameters must be separated with ampersands (&).
  - Common request parameters include information such as the API version and authentication information.
  - For more information about the custom request parameters, see the corresponding operation description.

Example

Call the DescribeFeatures operation to query the deployed Apsara Stack Security features.

```
https://yundunprivate.[ RegionId].example.com/?Action=DescribeFeatures&AccessKeyId=key-test&Format=JSON&SecureTransport=true&SignatureMethod=HMAC-SHA1&SignatureNonce=15215528852396&SignatureVersion=1.0&SourceIp=1xxxx6&Timestamp=2018-03-02Txxxxxxx&Version=2018-01-16&Signature=xxxx%xxxx%3D
```

API requests are presented in the following easy-to-read format in this document:

```
https://yundunprivate.[ RegionId].example.com/?Action=DescribeFeatures
&Format=JSON
&Version=2018-01-16
&Signature=xxxx%xxxx%3D
&SignatureMethod=HMAC-SHA1
&SignatureNonce=15215528852396
&SignatureVersion=1.0
&AccessKeyId=key-test
&Timestamp=2012-06-01T12:00:00Z
```

2.16.5.2.2. Signature mechanism

Apsara Stack Security authenticates each access request. You need to include a signature for the submitted HTTP or HTTPS request.

API authorization

To ensure the security of your account, we recommend that you use a Resource Access Management (RAM) user to call API operations. Before using a RAM user to call an API operation, you must grant the RAM user the corresponding permission to call the API by creating an authorization policy and attaching the policy to the RAM user.

API signature

To ensure secure calls to the API, Alibaba Cloud authenticates each API request through the signature. When you manually make an API request, you need to use AccessKey Secret to calculate the signature, that is, the hash-based message authentication code (HMAC) value, based on the encoded and sorted request string. For more information, see the definition in RFC 2104.

This topic uses the raw access parameters in the following table to describe how to create an API signature.

Parameter	Description
Access point	`http://yundunprivate.[ RegionId].example.com/?`
API-specific parameters	`Action=DescribeFeatures`

Parameter	Description
Common parameters (excluding the Signature parameter)	&Timestamp=2016-02-23T12:46:24Z &Format=JSON &AccessKeyId=<yourAccessKeyId> &SignatureMethod=HMAC-SHA1 &SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf &Version=2018-01-16 &SignatureVersion=1.0
AccessKey secret	<yourAccessKeySecret>

1. Use the request parameters to construct a canonicalized query string.

   > **Note** The request parameters include common request parameters (excluding the Signature parameter) and API-specific parameters.

   i. Sort the parameters.

   Sort the request parameters in alphabetical order.

   ii. Encode the parameters.

   Use UTF-8 to URL-encode the parameter names and values. The encoding rules are as follows:

   - Letters, digits, hyphens (-), underscores (_), periods (.), and tildes (~) are not encoded.
   - Other characters are encoded in the %XY format, where XY is the hexadecimal representation of the character in ASCII. For example, the double quotation mark (") is encoded as %22.
   - Extended UTF-8 characters are encoded in the %XY%ZA... format.
   - Note that a space is encoded as %20, instead of a plus sign (+).

   iii. Connect the encoded parameter names and values with equal signs (=).

   iv. Then, sort the parameter name and value pairs connected by equal signs in alphabetical order, and connect them with ampersands (&) to produce the canonicalized query string.

2. Use the canonicalized query string to construct the string for signature calculation based on the following rules:

   ```
   StringToSign=HTTPMethod + “&” + percentEncode( “/” ) + ” &” +
   percentEncode(CanonicalizedQueryString)
   ```

3. Calculate the HMAC value of the StringToSign string according to the definition in RFC 2104.

   > **Note** The key used for signature calculation is your AccessKey secret adding the ampersand (&) (ASCII 38). Secure Hash Algorithm 1 (SHA1) is used as the hash algorithm.

4. Encode the preceding HMAC value into a string based on Base64 encoding rules to obtain the

signature value.

```
LEW8N4y7Uasop******
```

5. Set the Signature parameter in the request parameters to this signature value to sign the request.

2.16.5.2.3. Common request parameters

The following table describes the common request parameters that are used to indicate information such as the API version and authentication information.

Name	Type	Required	Description
Version	String	Yes	The API version in the format of YYYY-MM-DD. Set the value to *2018-01-16*.
AccessKeyId	String	Yes	The key ID that Alibaba Cloud assigns to a user for service access.
Signature	String	Yes	The signature string.
SignatureMethod	String	Yes	The signature method. Set the value to *HMAC-SHA1*.
Timestamp	String	Yes	The timestamp of the request. Follow the ISO 8601 standard to specify the date and use the offset from Coordinated Universal Time (UTC) to specify the time zone. The format is `YYYY-MM-DDThh:mm:ssZ`. For example, 2014-05-26T12:00:00Z indicates 20:00:00 on May 26, 2014, Beijing time.
SignatureVersion	String	Yes	The signature algorithm version. Set the value to *1.0*.
SignatureNonce	String	Yes	The unique random number used to prevent network replay attacks. You must use different random numbers for different requests.
ResourceOwnerAccount	String	No	The owner account of the resource to be accessed through this API request, that is, the logon username.

Name	Type	Required	Description
Format	String	No	The format of the response. Set the value to *JSON or XML*. Note Default value: XML.

2.16.5.2.4. Response structure

Apsara Stack Security API responses support both the XML and JSON formats. The system always returns a unique identification code RequestId each time you send a request to call an operation, no matter whether the call is successful or not.

Sample responses (XML format)

```
<? xml version="1.0" encoding="UTF-8"? >
<! -- The root node of the result -->
<Operation name+Response>
   <! -- Returned request ID -->
   <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
   <! -- Returned data -->
</Operation name+Response>
```

Sample responses (JSON format)

```
{
"RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
/* Returned data */
}
```

2.16.5.3. APIs

2.16.5.3.1. CheckIpSegment

Description

You can call this operation to check whether a CIDR block to be added for monitoring is valid. If a success result is returned through this API, the CIDR block specified in the request can be added.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CheckIpSegment*.
IpSegmentName	String	Yes	The CIDR block to be checked, in x.x.x.x/x format. For example, 172.21.23.222/24.
InfoType	String	No	The CIDR block information type. For example, a value of distribution indicates the region information.
InfoName	String	No	The information describing the CIDR block based on the value of the InfoType parameter. For example, if the InfoType parameter is set to distribution, you can set the InfoName parameter to DXJF, indicating that the CIDR block belongs to the region where the Daxing IDC is located.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://ddosprivate.[ RegionId].example.com/?Action=CheckIpSegment
&IpSegmentName=192.1.1.1/24
&InfoType=distribution
&InfoName=DXJF
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"71064826-726F-4ADA-B879-05D8055476FB"
}
```

2.16.5.3.2. DescribeRegionName

Description

You can call this operation to query the regions of the CIDR blocks where traffic data collection and analysis is performed.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeRegionName*.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
RegionNameList	Array	A list of regions. For more information, see the following parameter descriptions.
Id	Integer	The ID of the region.
Description	String	The region of the CIDR block.
CodeType	String	The type of the CIDR block information. For example, distribution indicates the region information.
Code	String	This parameter is used with the CodeType parameter to specify the code of the corresponding information. For example, if the CodeType parameter is set to distribution and the Code parameter is set to DXJF, this indicates that the CIDR block belongs to the region where the Daxing data center is located.
CodeName	String	This parameter is used with the CodeType parameter to specify the name of the corresponding information.
GmtCreate	String	The time when the CIDR block was created.
GmtModified	String	The latest time when the CIDR block was modified.
Seq	Integer	The sequence number of the region record.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://ddosprivate.[ RegionId].example.com/?Action=DescribeRegionName
&<Common request parameters>
```

- Sample responses (JSON format)


```
{
 "RegionNameList":[
  {
   "GmtCreate":1463367238000,
   "Description":"Hybrid cloud data center list",
   "CodeName":"Daxing data center",
   "GmtModified":1463367238000,
   "CodeType":"distribution",
   "Id":17,
   "Code":"am1",
   "Seq":1
  },
  {
   "GmtCreate":1463367238000,
   "Description":"Hybrid cloud data center list",
   "CodeName":"Not specified",
   "GmtModified":1463367238000,
   "CodeType":"distribution",
   "Id":32,
   "Code":"UNKNOWN",
   "Seq":4
  },
  {
   "GmtCreate":1485069049000,
   "Description": "Data center list",
   "CodeName":"Beijing data center",
   "GmtModified":1485069049000,
   "CodeType":"distribution",
   "Id":50,
   "RegionId": "cn-beijing-btc-a01",
   "Seq":2
  },
  {
```

```
  "GmtCreate":1485069106000,
  "Description": "Data center list",
  "CodeName":"Hangzhou data center",
  "GmtModified":1485069104000,
  "CodeType":"distribution",
  "Id":51,
  "Code":"cn-hangzhou-dg-a01",
  "Seq":3
 },
 {
  "GmtCreate":1463367238000,
  "Description":"Hybrid cloud data center list",
  "CodeName":"Daxing data center",
  "GmtModified":1463367238000,
  "CodeType":"distribution",
  "Id":52,
  "Code":"DD_DXJF",
  "Seq":1
 }
],
 "RequestId":"26738B34-6680-4BD7-BBF8-EF8DE53D52F6"
}
```


2.16.5.3.3. CreateIpSegment

Description

You can call this operation to add a specified CIDR block to be monitored.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *CreateIpSegment*.
IpSegmentName	String	Yes	The CIDR block to be added for monitoring, in x.x.x.x/x format. For example, 172.21.23.222/24.
InfoType	String	No	The CIDR block information type. For example, a value of distribution indicates the region information.

Name	Type	Required	Description
InfoName	String	No	The information describing the CIDR block based on the value of the InfoType parameter. For example, if the InfoType parameter is set to distribution, you can set the InfoName parameter to DXJF, indicating that the CIDR block belongs to the region where the Daxing data center is located.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://ddosprivate.[ RegionId].example.com/?Action=CreateIpSegment
&IpSegmentName=172.21.13.222/24
&InfoType=distribution
&InfoName=DXJF
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"6C91B447-DAA5-40DB-B818-E10820D99DEC"
}
```

2.16.5.3.4. DescribeIpSegment

Description

You can call this operation to query Classless Inter-Domain Routing (CIDR) blocks under traffic monitoring.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeIpSegment*.
CurrentPage	Integer	No	The number of the page to return.
PageSize	Integer	No	The number of records to return on each page.
InfoType	String	No	The type of the CIDR block information. For example, a value of distribution indicates the region information.
Distribution	String	No	The ID of the region. For example, a value of DXJF indicates the region where the Daxing IDC is located.
IpSegment	String	No	The CIDR block, in x.x.x.x/x format.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
TotalCount	Integer	The total number of returned pages.
IpSegmentList	Array	The CIDR blocks for traffic collection. For more information, see the following descriptions.
GmtCreate	Long	The time when the CIDR block for traffic collection was created.
GmtModified	Long	The time when the CIDR block for traffic collection was last modified.
Id	Integer	The ID of the CIDR block for traffic collection.
RegionName	String	The region name of the CIDR block.
InfoType	String	The type of the CIDR block information. For example, a value of distribution indicates the region information.

Parameter	Type	Description
InfoName	String	The information describing the CIDR block based on the value of the InfoType parameter. For example, if the value of the InfoType parameter is distribution, the value of the InfoName parameter can be DXJF, indicating that the CIDR block belongs to the region where the Daxing IDC is located.
IpExpressions	String	The CIDR block for traffic collection, in x.x.x.x/x format.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=DescribeIpSegment
&CurrentPage=1
&Distribution=DXJF
&InfoType=distribution
&IpSegment=x.x.x.x/x
&PageSize=20
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TotalCount":1,
  "PageSize":20,
  "RequestId":"AC51224B-3730-4C6B-B444-2307C7F73E84",
  "IpSegmentList":[
    {
      "IpExpressions":"192.168.x.x/24",
      "GmtCreate":1520565939000,
      "RegionName":"Daxing IDC",
      "GmtModified":1520565939000,
      "InfoName":"****",
      "Id":9,
      "InfoType":"distribution1"
    }
  ],
  "CurrentPage":1
}
```


2.16.5.3.5. DeleteIpSegment

Description

You can call this operation to delete a CIDR block whose traffic is collected and monitored based on the CIDR block record ID.

> **Note** You must obtain the record ID of the monitored CIDR block to be deleted before calling this operation.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteIpSegment*.
IpId	String	Yes	The record ID of the monitored CIDR block to be deleted.

Response parameters

Name	Type	Description

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://ddosprivate.[ RegionId].example.com/?Action=DeleteIpSegment
&IpId=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"9C40FE9D-EE39-4162-8E94-7C0A32F276D8"
}
```

2.16.5.3.6. ModifyIpSegment

Description

You can call this operation to modify a monitored Classless Inter-Domain Routing (CIDR) block with a specified record ID.

Note You must know the record ID of the monitored CIDR block to be modified before calling this operation.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *ModifyIpSegment*.
IpId	Integer	Yes	The record ID of the monitored CIDR block to be modified.
InfoName	String	Yes	The region to which the CIDR block belongs. For example, a value of DXJF indicates that the CIDR block belongs to the region where the Daxing IDC is located.

Parameter	Type	Required	Description
IpSegmentName	String	Yes	The CIDR block, in x.x.x.x/x format.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=ModifyIpSegment
&InfoName=****
&InfoType=distribution
&IpId=11
&IpSegmentName=192.168.x.x/24
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"5FFE58AA-355B-4E0E-A742-0BB5554BA959"
}
```

2.16.5.3.7. CreateDdosPolicy

Description

You can call this operation to add an anti-DDoS policy for a specified IP address or Classless Inter-Domain Routing (CIDR) block.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *CreateDdosPolicy*.

Parameter	Type	Required	Description
ExternalServiceIP	String	Yes	The IP address or CIDR block to which the anti-DDoS policy applies, in x.x.x.x or x.x.x.x/x format.
FlowRate	Integer	Yes	The traffic rate threshold. Unit: Mbit/s. Note The value of this parameter must be greater than 0.
HttpRate	Integer	Yes	The HTTP request rate threshold. Unit: queries per second (QPS). Note The value of this parameter must be greater than 50.
PackageRate	Integer	Yes	The packet rate threshold. Unit: packets per second (PPS). Note The value of this parameter must be greater than 0.
UserId	Long	No	The user ID of the request sender. The parameter is automatically set by the system.
UserName	String	Yes	The username of the request sender. The parameter is automatically set by the system.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=CreateDdosPolicy
&ExternalServiceIP=192.168.x.x/32
&FlowRate=1
&HttpRate=60
&PackageRate=1
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"CA179B61-DD6D-4FE3-A410-CC16AC705DF4"
}
```

2.16.5.3.8. DescribeDdosPolicies

Description

You can call this operation to query the configured DDoS protection policies.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeDdosPolicies*.
CurrentPage	Integer	No	The current page number.
PageSize	Integer	No	The maximum number of records displayed on a page.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
TotalCount	Integer	The total number of pages returned.

Name	Type	Description
DdosPolicies	Array	A list of DDoS protection policies. For more information, see the following parameter descriptions.
Code	String	The region code of the CIDR block that the DDoS protection policy is applied to.
CodeName	String	The region name of the CIDR block that the DDoS protection policy is applied to.
DepartmentName	String	The department of the user AliUID that created the DDoS protection policy.
ExternalServiceIP	String	The IP address or CIDR block that the DDoS protection policy is applied to.
FlowRate	Integer	The bandwidth threshold. Unit: Mbit/s.
HttpRate	Integer	The HTTP request threshold. Unit: QPS.
PackageRate	Integer	The packet threshold. Unit: PPS.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://ddosprivate.[ RegionId].example.com/?Action=DescribeDdosPolicies
&CurrentPage=1
&PageSize=10
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "TotalCount":1,
  "PageSize": 10,
  "RequestId": "179E1AA9-1BC2-4A66-9E4B-1640EDDE7D1C",
  "CurrentPage": 1,
  "DdosPolicies": [
    {
      "PackageRate": 200,
      "HttpRate": 0,
      "CodeName":"Daxing data center",
      "ExternalServiceIP": "x.x.x.x/x",
      "DepartmentName": "Department 1",
      "Code": "DD_DXJF",
      "FlowRate": 900,
      "AliUid": 0
    }
  ]
}
```


2.16.5.3.9. DeleteDdosPolicy

Description

You can call this operation to delete an anti-DDoS policy for a specified Classless Inter-Domain Routing (CIDR) block.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DeleteDdosPolicy*.
RegionCode	String	Yes	The ID of the region. For example, cn-hangzhou-env6-d01.
ExternalServiceIP	String	Yes	The IP address or CIDR block to which the anti-DDoS policy applies, in x.x.x.x or x.x.x.x/x format.

Parameter	Type	Required	Description
FlowRate	Integer	No	The traffic rate threshold. Unit: Mbit/s. Note The value of this parameter must be greater than 0.
HttpRate	Integer	No	The HTTP request rate threshold. Unit: queries per second (QPS). Note The value of this parameter must be greater than 50.
PackageRate	Integer	No	The packet rate threshold. Unit: packets per second (PPS). Note The value of this parameter must be greater than 0.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=DeleteDdosPolicy
&ExternalServiceIP=192.168.x.x/24
&RegionCode=cn-****-env6-d01
&FlowRate=55
&HttpRate=55
&PackageRate=55
&<Common request parameters>
```

- Sample response (JSON format)

```
{
   "RequestId":"8C9B8735-18BA-451B-AE9D-1428554CA360"
}
```

2.16.5.3.10. ModifyDdosPolicy

Description

You can call this operation to modify a specified anti-DDoS policy.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *ModifyDdosPolicy*.
Distribution	String	Yes	The ID of the region. For example, a value of DXJF indicates the region where the Daxing IDC is located.
ExternalServiceIP	String	Yes	The IP address or Classless Inter-Domain Routing (CIDR) block to which the anti-DDoS policy applies, in x.x.x.x or x.x.x.x/x format.
FlowRate	Integer	Yes	The traffic rate threshold. Unit: Mbit/s. Note The value of this parameter must be greater than 0.
HttpRate	Integer	Yes	The HTTP request rate threshold. Unit: queries per second (QPS). Note The value of this parameter must be greater than 50.
PackageRate	Integer	Yes	The packet rate threshold. Unit: packets per second (PPS). Note The value of this parameter must be greater than 0.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=ModifyDdosPolicy
&Distribution=****
&ExternalServiceIP=192.168.x.x/32
&FlowRate=1
&HttpRate=60
&PackageRate=1
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"CA179B61-DD6D-4FE3-A410-CC16AC705DF4"
}
```

2.16.5.3.11. DescribeBlockSwitchs

Description

You can call this operation to query the status of the traffic block switch in anti-DDoS.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DescribeBlockSwitchs*.
CurrentPage	Integer	No	The current page number.
PageSize	Integer	No	The maximum number of records displayed on a page.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
CurrentPage	Integer	The current page number.
PageSize	Integer	The maximum number of records displayed on a page.
TotalCount	Integer	The total number of pages returned.
BlockSwitchs	Array	The traffic block switch information. For more information, see the following parameter descriptions.
Code	String	The code of the block switch, which uniquely identifies a block switch.
Description	String	The brief description of the block switch.
Id	Integer	The ID of the block switch.
Mode	Integer	The status of the block switch. Valid values: • *0*: indicates disabled. • *1*: indicates enabled.
ModeName	String	The status name of the block switch. Valid values: • *Disabled* • *Enabled*
Name	String	The name of the block switch.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://ddosprivate.[ RegionId].example.com/?Action=DescribeBlockSwitchs
&CurrentPage=1
&PageSize=20
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "PageSize": 10,
 "RequestId":"95F2F4C8-7623-48B7-A976-30B48F3A25EB",
 "CurrentPage":1,
 "BlockSwitchs":[
  {
   "Description": "test",
   "Mode":0,
   "ModeName":"Disabled",
   "id": 1,
   "Code":"UPGRADE_SWITCH",
   "Name":"Upgrade channel switch"
  },
  {
   "Description":"Automatic upgrade switch",
   "Mode":1,
   "ModeName":"Enabled",
   "Id":2,
   "Code":"AUTO_UPGRADE_SWITH",
   "Name":"Automatic upgrade switch"
  }
 ]
}
```


2.16.5.3.12. ModifyBlockSwitchs

Description

You can call this operation to change the status of the block switch in DDoS settings.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *ModifyBlockSwitch*.
Id	Integer	Yes	The ID of the block switch.
Mode	Integer	Yes	The status of the block switch. Valid values: • *0*: indicates disabled. • *1*: indicates enabled.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://ddosprivate.[ RegionId].example.com/?Action=ModifyBlockSwitch
&Id=1
&Mode=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"B7FA97F0-082D-4611-A3C4-867011E2A106"
}
```

2.16.5.3.13. DescribeDdosEvents

Description

You can call this operation to query distributed denial of service (DDoS) events that meet the specified search criteria.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeDdosEvents*.
CurrentPage	Integer	No	The number of the page to return.
PageSize	Integer	No	The number of records to return on each page.
StartRow	Integer	No	The sequence number of the first record to return on the current page.

Parameter	Type	Required	Description
Distribution	String	No	The ID of the region. For example, a value of DXJF indicates the region where the Daxing IDC is located.
VmIP	String	No	The IP address of the victim server.
StartDay	Long	No	The beginning of the time range where data is queried.
EndDay	Long	No	The end of the time range where data is queried.
SearchReason	String	No	The reason why the DDoS event is triggered. Valid values: *bps*, *pps*, and *qps*. You can query events triggered by multiple reasons. For example, you can enter "bps,pps" to query the DDoS events that are triggered when the traffic rate threshold or the packet transmission rate threshold is exceeded.
SelectStatus	String	No	The status of the DDoS event. Valid values: • *Scrubbing* • *Scrubbing completed*

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
TotalCount	Integer	The total number of returned pages.
DdosEvents	Array	The DDoS events. For more information, see the following descriptions.
Id	Long	The ID of the event.
GmtCreate	Long	The time when the event was created.
GmtModified	Long	The time when the event was updated.
Aliuid	Long	The AliUid of the asset owner.

Parameter	Type	Description
AttackType	String	The type of the attack. Note In the current version, only the value of *defence* is supported.
Caller	String	The name of the system that calls the operation. Note Currently, the fixed value is *beaver_dj*, indicating Network Traffic Monitoring System.
Category	Integer	The number of the security event category.
CategoryName	String	The name of the security event category.
VmIp	String	The IP address of the victim server.
Code	String	The scrubbing status of the event. Valid values: • *Scrubbing* • *Scrubbing completed*
Bps	Long	The traffic rate threshold. Unit: Mbit/s.
Pps	Long	The packet rate threshold. Unit: packets per second (PPS).
Qps	Long	The HTTP request rate threshold. Unit: queries per second (QPS).
Conn	Integer	The threshold of concurrent connections. Note This response parameter has been deprecated.
NewConn	Integer	The threshold of new connections. Note This response parameter has been deprecated.
Reason	String	The reason why the event was reported.
Distribution	String	The ID of the region.
DistributionDisplay	String	The name of the region.

Parameter	Type	Description
IsFinished	Boolean	Indicates whether the attack has finished. Valid values: • *true*: indicates that the attack has finished. • *false*: indicates that the attack has not finished.
OccurrenceTime	Long	The time when the event occurred.
EndTime	Long	The time when the attack finished.
LocationAdd	String	The location where the event was added. Note This response parameter is invalid in Apsara Stack.
LocationDel	String	The location where the event was canceled. Note This response parameter is invalid in Apsara Stack.
Status	Integer	The status of the IP address where the DDoS event occurred. Valid values: • *0*: indicates that the IP address has not expired. • *1*: indicates that the IP address has expired.
Successful	Integer	Indicates whether the attack succeeds. Valid values: • *0*: indicates that the attack has failed. • *1*: indicates that the attack succeeded.
NeedIgnore	Integer	Indicates whether you need to ignore the event. Valid values: • *0*: indicates that you do not need to ignore the event. • *1*: indicates that the event has been reported repeatedly and you need to ignore the event.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=DescribeDdosEvents
&CurrentPage=1
&Distribution=DXJF
$StartDay=1381079107176
$EndDay=1481079107176
&PageSize=10
&<Common request parameters>
```

- Sample response (JSON format)

```
{
 "TotalCount":1,
 "RequestId":"AD525B06-F5F7-4319-94F4-45154D5B0750",
 "DdosEvents":[
  {
   "NewConn":0,
   "Status":0,
   "LocationDel":"nulllocal",
   "Category":21,
   "Bps":5,
   "EndTime":1573233588000,
   "Zone":"default",
   "GmtModified":1484372333000,
   "AttackType":"0",
   "Conn":0,
   "Code":"Scrubbing",
   "DistributionDisplay":"Daxing IDC",
   "Reason":"bps",
   "OccurrenceTime":1473233588000,
   "GmtCreate":1484369068000,
   "Pps":450,
   "Caller":"beaver_dj",
   "Qps":0,
   "Distribution":"am1",
   "LocationAdd":"local",
   "CategoryName":"DDOS_DEFENSE",
   "Id":3,
   "IsFinished":false,
   "NeedIgnore":0
  }
 ],
 "CurrentPage":1
}
```


2.16.5.3.14. DescribeFlowAnalysisResult

Description

You can call this operation to query the analysis result of the traffic sent to an IP address.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeFlowAnalysisResult*.
Distribution	String	Yes	The ID of the region. For example, a value of DXJF indicates the region where the Daxing IDC is located.
VmIP	String	Yes	The IP address of the victim server.
StartDate	Long	Yes	The beginning of the time range where traffic is analyzed.
SearchReason	String	No	The reason why the distributed denial of service (DDoS) event is triggered. Valid values: *bps*, *pps*, and *qps*. You can query events triggered by multiple reasons. For example, you can enter "bps,pps" to query the DDoS events that are triggered when the traffic rate threshold or the packet transmission rate threshold is exceeded.
SelectStatus	String	No	The status of the DDoS event. Valid values: • *Scrubbing* • *Scrubbing completed*

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TopAttackers	Array	The analysis on the top 10 attackers. For more information, see the following descriptions.
Ip	String	The IP address of the attacker.
Count	Float	The percentage of attacks launched to the IP address compared to the total attacks.

Parameter	Type	Description
TopProtocols	Array	The analysis on the composition of the attack traffic. For more information, see the following descriptions. Note The traffic composition analysis shows traffic of different protocols, including TCP, ICMP, and UDP.
Protocol	String	The protocol.
Count	Float	The percentage of the traffic of the specified protocol compared to the total amount of traffic.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=DescribeFlowAnalysisResult
&Distribution=DD_DXJF
&startDate=123123312000
&VmIp=x.x.x.x
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "TopAttackers":["Ip":"x.x.x.x","Count":"1.00"],
  "RequestId":"B2488F1F-930D-4906-AC76-61045B4F1EF2",
  "TopProtocols":["Protocol":"tcp","Count":"1.00"]
}
```

2.16.5.3.15. DescribeFlowDetails

Description

You can call this operation to query the detailed traffic information for a specified IP address.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeFlowDetails*.
Distribution	String	Yes	The ID of the region. For example, a value of DXJF indicates the region where the Daxing IDC is located.
VmIP	String	Yes	The IP address of the victim server.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
HttpStatusCode	Integer	The HTTP status code.
FlowDetail	Struct	The detailed traffic information. For more information, see the following descriptions.
AliUid	Long	The ID of the Alibaba Cloud account.
Distribution	String	The ID of the region.
DistributionDisplay	String	The name of the region.
ExternalServiceIp	String	The IP address or Classless Inter-Domain Routing (CIDR) block.
FlowRate	Integer	The flow rate. Unit: Mbit/s.
HttpRate	Integer	The HTTP request rate. Unit: queries per second (QPS).
PackageRate	Integer	The packet rate. Unit: packets per second (PPS).

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=DescribeFlowDetails
&Distribution=****
&VmIp=10.0.x.x
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"8491DBFD-48C0-4E11-B6FC-6F38921244A9",
  "FlowDetail":{
    "PackageRate":200,
    "HttpRate":0,
    "ExternalServiceIP":"10.0.x.x/32",
    "Distribution":"DXJF",
    "DistributionDisplay":"Daxing IDC",
    "FlowRate":900,
    "AliUid":0
  },
  "HttpStatusCode":200
}
```

2.16.5.3.16. CancelCleanStatus

Description

You can call this operation to disable DDoS traffic scrubbing for a specified IP address.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *CancelCleanStatus*.
Distribution	String	Yes	The ID of the region. For example, a value of DXJF indicates the region where the Daxing IDC is located.
VmIp	String	Yes	The IP address of the instance, in x.x.x.x format.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=CancelCleanStatus
&Distribution=DXJF
&SourceIp=10.0.x.x
&VmIp=172.16.x.x
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

2.16.5.3.17. CreateWhiteList

Description

You can call this operation to add a whitelist of trusted IP addresses that are exempt from traffic security monitoring.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *CreateWhiteList*.
Type	Integer	Yes	The type of the whitelist. Valid values: • *6*: indicates a server brute-force attack whitelist. • *12*: indicates a BWAF source IP address whitelist. • *15*: indicates an application attack whitelist.

Parameter	Type	Required	Description
Username	String	No	The username used to add the whitelist.
DestinationIp	String	No	The destination IP address. Note When you add a BWAF source IP address whitelist (that is, the Type parameter is set to 12), the DestinationIp parameter must be set to the default value 0.0.0.0.
SourceIpStr	String	No	The source IP address.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=CreateWhiteList
&Type=15
&DestinationIp=192.168.xx.xx
&SourceIpStr=192.168.xx.xx
&Username=test
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "RequestId":"208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

2.16.5.3.18. DescribeWhiteList

Description

You can call this operation to query the IP addresses that have been added to a whitelist.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeWhiteList*.
DestinationIp	String	No	The destination IP address.
SourceIpStr	String	No	The source IP address.
Type	Integer	No	The type of the whitelist. Valid values: • *6*: indicates a server brute-force attack whitelist. • *12*: indicates a BWAF source IP address whitelist. • *15*: indicates an application attack whitelist.
Username	String	No	The username.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
TotalCount	Integer	The total number of returned pages.
WhiteLists	List	The whitelist records. For more information, see the following descriptions.
SourceIp	String	The source IP address.
Id	Integer	The ID of the whitelist record.
Type	Integer	The type of the whitelist. Valid values: • *6*: indicates a server brute-force attack whitelist. • *12*: indicates a BWAF source IP address whitelist. • *15*: indicates an application attack whitelist.
Username	String	The username.

Parameter	Type	Description
DestinationIp	String	The destination IP address.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=DescribeWhiteList
&Type=15
&DestinationIp=172.16.xx.xx
&SourceIpStr=172.17.xx.xx
&Username=test
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "CurrentPage":1,
  "PageSize":20,
  "RequestId":"430A3687-B9EC-4F71-B472-EE24ED609863",
  "Success":true,
  "TotalCount":0,
  "WhiteLists":[{
    "DestinationIp":"172.16.xx.xx",
    "Id":6,
    "SourceIp":"172.17.xx.xx",
    "Type":15,
    "Username":"****"
  }]
}
```

2.16.5.3.19. DeleteWhiteList

Description

You can call this operation to delete a specified whitelist entry.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to *DeleteWhiteList*.
Id	Integer	Yes	The ID of the whitelist entry.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample requests

```
https://ddosprivate.[ RegionId].example.com/?Action=DeleteWhiteList
&Id=15
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
 "RequestId":"208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

2.16.5.3.20. DescribeConsoleDdosPolicies

Description

You can call this operation to obtain the records of anti-DDoS policies, including the system default policies.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to *DescribeConsoleDdosPolicies*.
AliUid	Long	Yes	The ID of the Alibaba Cloud account.

Parameter	Type	Required	Description
CurrentPage	Integer	No	The number of the page to return.
PageSize	Integer	No	The number of records to return on each page.
StartRow	Integer	No	The start row to return.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The number of the current page returned.
PageSize	Integer	The number of records returned on each page.
TotalCount	Integer	The total number of returned pages.
ThresholdList	List	The anti-DDoS policies. For more information, see the following descriptions.
DepartmentName	String	The department name of the current user.
ExternalServiceIP	String	The IP address or Classless Inter-Domain Routing (CIDR) block. Note A value of default is returned if the system default policy is used.
Code	String	The IDC ID corresponding to the CIDR block.
CodeName	Sting	The IDC name corresponding to the CIDR block.
FlowRate	Integer	The threshold for the traffic rate. Unit: Mbit/s.
HttpRate	Integer	The threshold for the HTTP request rate. Unit: queries per second (QPS).
PackageRate	Integer	The threshold for the packet rate. Unit: packets per second (PPS).
AliUid	Long	The Alibaba Cloud account ID corresponding to the policy.

Error codes

For more information about the error codes that this operation can return, see Error codes.

Examples

- Sample request

```
https://ddosprivate.[ RegionId].example.com/?Action=DescribeConsoleDdosPolicies
&AliUid=****
&CurrentPage=1
&PageSize=10
&SourceIp=xx.xx.xx.xx
&<Common request parameters>
```

- Sample response (JSON format)

```
{
  "CurrentPage":1,
  "HttpStatusCode":200,
  "PageSize":20,
  "RequestId":"7C3AC882-E5A8-4855-BE77-B6837B695EF1",
  "ThresholdList":[
    {
      "AliUid":151971404963****,
      "Code":"DD_DXJF",
      "CodeName":"DD_DXJF",
      "DepartmentName":"****Cloud",
      "ExternalServiceIP":"1.1.xx.xx/32",
      "FlowRate":1,
      "HttpRate":52,
      "PackageRate":1
    },
    {
      "AliUid":151971404963****,
      "Code":"DD_DXJF",
      "CodeName":"DD_DXJF",
      "DepartmentName":"****Cloud",
      "ExternalServiceIP":"2.2.xx.xx/32",
      "FlowRate":1,
      "HttpRate":51,
      "PackageRate":1
    },
    {
      "AliUid":-1,
      "Code":"DD_DXJF",
      "CodeName":"DD_DXJF",
      "ExternalServiceIP":"default",
      "FlowRate":900,
      "HttpRate":0,
      "PackageRate":200
    }
  ],
  "TotalCount":3
}
```


2.16.6. Error codes

Functional module	Error code	Error message	Description
Threat Detection Service	yd.error.sas. 1	The specified field has not been found in the metadata.	The error message returned because the field you queried does not exist in the metadata. Check the request and try again.
Threat Detection Service	yd.error.sas. 2	An error occurred while invoking the task engine. Try again later.	The error message returned because the system has failed to call the task engine. Try again later.
Threat Detection Service	yd.error.sas. 3	An error occurred while starting the task. Try again later.	The error message returned because the system has failed to start the task. Try again later.
Threat Detection Service	yd.error.sas. 4	An error occurred while stopping the task. Try again later.	The error message returned because the system has failed to stop the task. Try again later.
Threat Detection Service	yd.error.sas. 5	An error occurred while restarting the task. Try again later.	The error message returned because the system has failed to restart the task. Try again later.
Threat Detection Service	yd.error.sas. 6	An error occurred while obtaining the task status. Try again later.	The error message returned because the system has failed to obtain the task status. Try again later.
Threat Detection Service	yd.error.sas. 7	An error occurred while deleting the task. Try again later.	The error message returned because the system has failed to delete the task. Try again later.
Threat Detection Service	yd.error.sas. 8	The specified table does not contain metadata.	The error message returned because the table you queried has no metadata configured. Check the request and try again.

Functional module	Error code	Error message	Description
Threat Detection Service	yd.error.sas. 400	The specified asset is under protection. Uninstall the Server Guard client and try again.	The error message returned because the asset you want to delete is protected. Uninstall the Server Guard agent from the server and try again.
Threat Detection Service	yd.error.sas. 500	A system error has occurred.	The error message returned because a system error has occurred. Contact Alibaba Cloud technical support.
Threat Detection Service	yd.error.sas. 101	The parameter is invalid.	The error message returned because a parameter error has occurred. Check the request and try again.
Threat Detection Service	yd.error.sas. 103	Request failed.	The error message returned because the request has failed. Try again later.
Threat Detection Service	yd.error.sas. 502	You are not authorized to access the instance.	The error message returned because you are not authorized to operate on the server.
Threat Detection Service	yd.error.sas. 100	Request failed. Refresh the page and try again.	The error message returned because the requested service is not available now. Try again later.
Threat Detection Service	yd.error.sas. 501	The function is not available in the current version.	The error message returned because the version you are using does not support this feature.
Anti-DDoS	yd.error.ddos. 400	An error occurred while accessing the server. Try again later.	The error message returned because the system has failed to access the server. Check the request and try again.
Anti-DDoS	yd.error.ddos. 500	An error occurred on the server.	The error message returned because a server error has occurred. Contact Alibaba Cloud technical support.

Functional module	Error code	Error message	Description
Anti-DDoS	yd.error.ddos.UNKNOWN_EXCEPTION	An internal error occurred.	The error message returned because an unknown error has occurred. Contact Alibaba Cloud technical support.
Anti-DDoS	yd.error.ddos.REQUEST_TIMEOUT	The request has timed out.	The error message returned because the request has timed out. Try again later.
Anti-DDoS	yd.error.ddos.SERVER_FAILED	An operation error occurred.	The error message returned because the operation has failed. Contact Alibaba Cloud technical support.
Anti-DDoS	yd.error.ddos.NOT_AUTHORIZED	You are not authorized to perform this operation.	The error message returned because you are not authorized to perform the action. Check the account permission.
Anti-DDoS	yd.error.ddos.PARAMETER_INVALID	The specified parameter is invalid or missing.	The error message returned because the specified request parameter is invalid. Check the request parameter and try again.
Anti-DDoS	yd.error.ddos.IP_SEGMENT_INVALID	The specified CIDR block is invalid.	The error message returned because the specified CIDR block is invalid. Check the CIDR block specified in the request parameter.
Anti-DDoS	yd.error.ddos.IP_SEGMENT_REPEAT	One CIDR block cannot be used in different regions. Enter another CIDR block.	The error message returned because one CIDR block belongs to different regions. Check the CIDR block specified in the request parameter.
Anti-DDoS	yd.error.ddos.IP_SEGMENT_ALREADY	The specified CIDR block already exists.	The error message returned because the specified CIDR block already exists. Check the CIDR block specified in the request parameter.

Functional module	Error code	Error message	Description
Anti-DDoS	yd.error.ddos.IP_SEGMENT_MASK_LENGTH_ERR	The prefix length must be less than 24 bits.	The error message returned because the mask contains more than 24 characters. Check the CIDR block mask specified in the request parameter.
Anti-DDoS	yd.error.ddos.QUERY_REGION_LIST_ERR	An error occurred while obtaining the regions list.	The error message returned because the system has failed to read the list of regions. Try again later.
Anti-DDoS	yd.error.ddos.IP_SEGMENT_OPERATION_ERR	An error occurred while performing the operation on the CIDR block.	The error message returned because the system has failed to process the CIDR block. Try again later.
Anti-DDoS	yd.error.ddos.QUERY_IP_SEGMENT_ERR	An error occurred while obtaining the CIDR block.	The error message returned because the system has failed to read the CIDR block information. Try again later.
Anti-DDoS	yd.error.ddos.MODIFY_IP_SEGMENT_ERR	An error occurred while modifying the CIDR block.	The error message returned because the system has failed to modify the CIDR block information. Try again later.
Anti-DDoS	yd.error.ddos.IP_SEGMENT_TYPE_ERR	Check whether the type of the CIDR block (internal or external) is specified.	The error message returned because the CIDR block type is not specified. Check the CIDR block type and try again.
Anti-DDoS	yd.error.ddos.CANCEL_FLOW_CLEAN_ERR	An error occurred while canceling traffic scrubbing. Check the network connection to Beaver.	The error message returned because the system has failed to cancel traffic scrubbing. Check the network connection with Network Traffic Monitoring System and try again.

Functional module	Error code	Error message	Description
Anti-DDoS	yd.error.ddos.QUERY_FLOW_ANALYSIS_ERR	An error occurred while obtaining the traffic analysis result. Check the network connection to Beaver.	The error message returned because the system has failed to obtain the traffic analysis result. Check the network connection with Network Traffic Monitoring System and try again.
Anti-DDoS	yd.error.ddos.QUERY_BEAVER_URL_ERR	An error occurred while obtaining the Beaver URL.	The error message returned because the system has failed to obtain the URL of Network Traffic Monitoring System. Check the network connection with Network Traffic Monitoring System and try again.
Anti-DDoS	yd.error.ddos.SET_VALVE_INVALID"	The specified thresholds are invalid.	The error message returned because the threshold validation has failed. Check the thresholds and try again.
Anti-DDoS	yd.error.ddos.VALVE_DEFAULT_ALREADY	You cannot add the default threshold again.	The error message returned because the system has failed to add the default threshold, which can only be modified.
Anti-DDoS	yd.error.ddos.NOT_BELONG_BEAVER_IP_SEGMENT	Check whether the specified CIDR block belongs to the internal network of Beaver.	The error message returned because the CIDR block you entered is not in the internal CIDR block of Network Traffic Monitoring System. Check the CIDR block.
Anti-DDoS	yd.error.ddos.VALVE_DELETE_ERR	Do not delete the threshold.	The error message returned because the system has failed to delete the default threshold or the threshold of 128.0.0.0/1, which cannot be deleted.

Functional module	Error code	Error message	Description
Anti-DDoS	yd.error.ddos.QUERY_CODE_ERR	An error occurred while obtaining the product configuration.	The error message returned because the system has failed to read the dictionary. Try again later.
Anti-DDoS	yd.error.ddos.IS_OPENED	Enabled.	The error message returned because the specified switch has been turned on and cannot be turned on repeatedly.
Anti-DDoS	yd.error.ddos.IS_CLOSED	Disabled.	The error message returned because the specified switch has been turned off and cannot be turned off repeatedly.
Server Guard	yd.error.aqs.REQUEST_FAILED	Request failed. Try again later.	The error message returned because the request has failed. Try again later.
Common errors of Apsara Stack Security	yd.error.all. 10001	Authorization required.	The error message returned because you are not authorized to perform the action. Check the account permission.
Common errors of Apsara Stack Security	yd.error.all. 10002	A system error has occurred. Try again later.	The error message returned because a system error has occurred. Try again later.
Common errors of Apsara Stack Security	yd.error.all. 10003	The parameter is invalid.	The error message returned because the specified request parameter is invalid. Check the request parameter and try again.
Common errors of Apsara Stack Security	yd.error.all.other	A system error has occurred.	The error message returned because a system exception has occurred. Try again later.
Common errors of Apsara Stack Security	yd.error.all.ConsoleSystemError_1001	An internal error has occurred.	The error message returned because the system has failed to process your request. Try again later.

Functional module	Error code	Error message	Description
Common errors of Apsara Stack Security	yd.error.all.ConsoleSystemError_1007	The specified API is unavailable.	The error message returned because the API has been brought offline. Contact Alibaba Cloud technical support.
Common errors of Apsara Stack Security	yd.error.all.ConsoleSystemError_1008	An error occurred while verifying postOnly.	The error message returned because the validation has failed. Check the common request parameters and try again.
Common errors of Apsara Stack Security	yd.error.all.ConsoleSystemError_1009	csrfToken must not be empty.	The error message returned because the validation has failed. Check the common request parameters and try again.
Common errors of Apsara Stack Security	yd.error.all.ConsoleSystemError_1010	An error occurred while verifying csrfToken.	The error message returned because the validation has failed. Check the common request parameters and try again.
Common errors of Apsara Stack Security	yd.error.all.ConsoleSystemError_1011	The Region ID must not be empty.	The error message returned because RegionId is left blank. Check the RegionId parameter.
Common errors of Apsara Stack Security	yd.error.all.ConsoleSystemError_1012	The specified region ID format is invalid.	The error message returned because the format of RegionId is invalid. Check the RegionId parameter.
Common errors of Apsara Stack Security	yd.error.all.ConsoleSystemError_1013	The parameter is null.	The error message returned because the specified request parameter is invalid. Check the request parameter and try again.
Common errors of Apsara Stack Security	yd.error.all.ConsoleSystemError_1014	The specified parameter format is invalid.	The error message returned because the specified request parameter is invalid. Check the request parameter and try again.

Functional module	Error code	Error message	Description
Common errors of Apsara Stack Security	yd.error.all.ConsoleNeedLogin	You are not logged on.	The error message returned because you are not authorized to perform the action. Check the account permission.
Common errors of Apsara Stack Security	yd.error.all.InvalidApi	The API is invalid.	The error message returned because an API exception has occurred. Try again later.
Common errors of Apsara Stack Security	yd.error.all.InvalidParameter	The parameter is invalid.	The error message returned because the specified request parameter is invalid. Check the request parameter and try again.
Common errors of Apsara Stack Security	yd.error.all.InvalidResult	The return value is invalid.	The error message returned because the return value is invalid. Try again later.
Common errors of Apsara Stack Security	yd.error.all.PropertyConvertFailed	An error occurred during conversion.	The error message returned because property conversion has failed. Try again later.
Common errors of Apsara Stack Security	yd.error.all.NoPermission	Authorization required.	The error message returned because you are not authorized to perform the action. Check the account permission.
Common errors of Apsara Stack Security	yd.error.all.ServerError	A server error has occurred.	The error message returned because a server exception has occurred. Try again later or contact Alibaba Cloud technical support.
Common errors of Apsara Stack Security	yd.error.all.UnkownError	An internal error has occurred.	The error message returned because the system has failed to process your request. Try again later or contact Alibaba Cloud technical support.

2.17. Key Management Service (KMS)

2.17.1. API reference

2.17.1.1. Make API requests

2.17.1.1.1. Overview

Make API requests

You can call KMS APIs by sending HTTP POST and GET requests to the KMS API server address with the corresponding API request parameters included in the request. The system will then return the request processing results.

1. Request structure.
2. Common parameters.
3. Request signatures.
4. Responses.

2.17.1.1.2. Request structure

Endpoints

The endpoint of the KMS API is kms.example.com.

Protocols

In KMS, requests can be sent only through the HTTPS channel.

SSL V2 and SSL V3 are not supported. TLS V1.0 and later are supported.

Methods

HTTP method POST or GET requests are URL encoded with the parameter values required by the API that is being called.

Parameters

For each request, you must specify the Action parameter indicating the API you want to call (such as `CreateKey`), the common request parameters required by all APIs, and the parameters specific to the API being called.

Encoding

Requests and responses are encoded in UTF-8.

2.17.1.1.3. Common parameters

Common request parameters

Common request parameters must be included in the request of each operation.

Parameter	Type	Required	Description
Format	String	No	The format of the response. Valid values: JSON and XML. Default value: XML.
Version	String	Yes	The version number of the API. The format is YYYY-MM-DD. The current version is 2016-01-20.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Alibaba Cloud.
Signature	String	Yes	The signature string. For more information about how to calculate the signature value, see Request signatures.
SignatureMethod	String	Yes	The signature method. HMAC-SHA1 is supported.
Timestamp	String	Yes	The timestamp of the request. Specify the time in the ISO 8601 standard in the YYYY-MM-DDThh:mm:ssZ format. The time must be in UTC. For example, 20:00:00 (UTC+8) on December 1, 2015 must be written as 2015-12-01T12:00:00Z.
SignatureVersion	String	Yes	The algorithm version of the signature. The current version is 1.0.

Examples

```
https://kms.cn-hangzhou.example.com/?
Format=json
&Version=2016-01-20
&AccessKeyId=testid
&Signature=YlrFhyqDZQ1ThNYARrv3Ptaxqf****
&SignatureMethod=HMAC-SHA1
&Timestamp=2016-03-25T09:36:58Z
&SignatureVersion=1.0
```

Common response parameters

The system returns a unique identifier (RequestId) for each API request, regardless of whether the request is successful.

Examples

XML format

```
<KMS>
<RequestId>348d9445-e39a-4d80-907d-298cc6c94447</RequestId>
<!—Response-->
</KMS>
```

JSON format

```
{
"RequestId": "284b2b80-9b17-4546-a093-adfbae512a54"
}
```

2.17.1.1.4. Request signatures

KMS authenticates each access request. Therefore, a request must contain signature information whether submitted using HTTP or HTTPS. KMS performs symmetric encryption using the AccessKey ID and AccessKey Secret to verify the identity of a request sender. The AccessKey ID and AccessKey Secret are issued to visitors by Alibaba Cloud. The AccessKey ID indicates the identity of the visitor. The AccessKey Secret is used to encrypt signature strings and verify signature strings on the server. It must be kept strictly confidential.

Perform the following steps to sign an access request:

1. Use request parameters to construct the canonicalized query string.

i. Sort parameters. Sort all request parameters by name in alphabetic order. These parameters include common request parameters and customized API request parameters , but do not include the Signature parameter in the common request parameters.

> **Note** When you use the GET method to submit requests, specify these parameters in the request URI following the question mark (?) and connect the remaining parameters with ampersands (&).

ii. Encode parameters. The parameter names and values must be encoded using UTF-8. The URL encoding rules are described as follows:

- Uppercase letters (A to Z), lowercase letters (a to z), digits (0 to 9), hyphens (-), underscores (_), periods (.), and tildes (~) are not encoded.
- Other characters are encoded in the %XY format, where XY is the hexadecimal representation of the character in ASCII. For example, double quotation marks (") are encoded as %22.
- Extended UTF-8 characters are encoded in the %XY%ZA... format.
- A space is encoded as %20, instead of the plus sign (+).

> **Note** This encoding method is similar to but different from the application/x-www-form-urlencoded MIME encoding algorithm (such as the java.net.URLEncoder class provided by the Java standard library). You can encode the names and values following the method for the standard library, then replace the plus signs (+) in the encoded strings with %20, the asterisks (*) with %2A, and change %7E back to the tilde (~) to conform to the encoding rules described above. You can implement this algorithm by using the following percentEncode() method:

```
private static final String ENCODING = "UTF-8";

private static String percentEncode(String value) throws UnsupportedEncodingException {
  return value ! = null ? URLEncoder.encode(value, ENCODING).replace("+", "%20").replace(
"*", "%2A").replace("%7E", "~") : null;
}
```

iii. Connect the encoded parameter names and values with equal signs (=).

iv. Sort the equal sign-connected parameter pairs in alphabetical order, and connect them with ampersands (&) to produce a canonicalized query string.

2. Use the created canonicalized query string to construct a string for signature calculation based on the following rule:

```
StringToSign=
  HTTPMethod + “&” +
  percentEncode( “/” ) + ” &” +
   percentEncode(CanonicalizedQueryString)
```

- In the preceding example, HTTPMethod indicates that an HTTP-style request such as GET is submitted.
- percentEncode("/") is the encoded value (%2F) of a forward slash (/). The encoding follows the URL encoding rules described in the previous step. percentEncode (CanonicalizedQueryString) is the encoded string of the canonicalized query string. The encoding follows the URL encoding rules described in the preceding step.

3. Use the signature string to calculate the HMAC value of the signature as defined by RFC 2104.

   > **Note** The key used for signature calculation is your AccessKey Secret. *An ampersand (&,* ASCII: 38) is added to the end of the key. The SHA-1 hashing algorithm is used.

4. Encode the HMAC value into a string based on Base64 encoding rules to obtain the signature value.
5. Add the obtained signature value to the request as the Signature parameter to sign the request.

   > **Note** When the signature value is submitted to the KMS server as the final request parameter value, the value will be URL encoded like other parameters based on RFC 3986.

   Taking DescribeRegions as an example, the AccessKey ID*testid and*AccessKey Secret*testsecret*are used. The request URL before being signed is: `http://kms.example.com/?TimeStamp=2016-02-23T12:46:24Z&Format=XML&AccessKeyId=testid&Action=DescribeRegions&SignatureMethod=HMAC-SHA1&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&Version=2014-05-26&SignatureVersion=1.0`

   The corresponding StringToSign is:

   ```
   GET&%2F&AccessKeyId%3Dtestid%26Action%3DDescribeRegions%26Format%3DXML%26SignatureMethod%3DHMAC-SHA1%26SignatureNonce%3D3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf%26SignatureVersion%3D1.0%26TimeStamp%3D2016-02-23T12%253A46%253A24Z%26Version%3D2014-05-26
   ```

   Because AccessKey Secret is *testsecret,*the Key used for HMAC calculation is *testsecret&.*The calculated signature value is: *CT9X0VtwR86fNWSnsc6v8YGOju*****.

   Add the signature value to the URL request as the Signature parameter. The URL is: `http://kms.example.com/?SignatureVersion=1.0&Action=DescribeRegions&Format=XML&SignatureNonce=3ee8c1b8-83d3-44af-a94f-4e0ad82fd6cf&Version=2014-05-26&AccessKeyId=testid&Signature=CT9X0VtwR86fNWSnsc6v8YGOju****&SignatureMethod=HMAC-SHA1&TimeStamp=2016-02-23T12%3A46%3A24Z` .

2.17.1.1.5. Responses

After you make an API request, the system will return an HTTP status code. If the request is successful, the system returns a 2xx error code. If the request has failed, the system returns a 4xx or 5xx error code. For a successful request, the response is in JSON format. If you make an API request by using third-party tools, you can customize the response format in the request parameters. In this reference, line breaks are used in the response examples for readability.

Sample success responses

XML format

```
<? xml version="1.0" encoding="UTF-8"? >
<! --The root node of the response -->
<Operation name+Response>
   <! --Returned request ID-->
   <RequestId>4C467B38-3910-447D-87BC-AC049166F216</RequestId>
   <! --Returned results-->
</Operation name+response>
```

JSON format

```
{
   "RequestId": "4C467B38-3910-447D-87BC-AC049166F216",
   /*Returned results*/
}
```

Sample error responses

If an error occurs during an API call, the system will not return any results. You can troubleshoot the error based on the error code returned. Error codes can be divided into API-specific and common error codes.

When an error occurs on an HTTP request, the system returns HTTP status code 4xx or 5xx. The response body includes the error code and error message. It also includes a globally unique request ID (RequestId), and the ID of the site accessed by the request (HostId). If the cause of the error cannot be identified, you can contact Alibaba Cloud technical support personnel and provide the HostId and RequestId returned in the error.

XML format

```
<KMS>
<HttpStatus>400</HttpStatus>
<Code>IllegalTimestamp</Code>
<Message>The input parameter "Timestamp" that is mandatory for processing this request is not suppli
ed. </Message>
<RequestId>3b237773-bc2c-4bea-95fc-319a1a5baa68</RequestId>
 </KMS>
```

JSON format

```
{
"HttpStatus": 400
"Code": "IllegalTimestamp"
"Message": "The input parameter "Timestamp" that is mandatory for processing this request is not supp
lied."
"RequestId": "e85db688-a2d3-44ca-9790-4259f59e90d8"
}
```

Common error codes

Error code	Error message	HTTP status code
InternalFailure	Internal Failure	500
SerivceUnavailableTemporary	Service Unavailable Temporary	503
InvalidAccessKeyId.NotFound	The AccessKey ID provided does not exist in our records.	404
Forbidden.KeyNotFound	The specified Key is not found.	404
Forbidden.AliasNotFound	The specified Alias is not found.	404
Forbidden.NoPermission	This operation is forbidden by permission system.	403
Forbidden.AccessKey	This AccessKey is not enabled.	403
UnsupportedHTTPMethod	This http method is not supported.	403
Forbidden.UbsmsInvalidUserid	Userid Invalid For Ubsms	403
Forbidden.UbsmsInvalidBid	Your account partner does not have KMS Service	403
Forbidden.KmsServiceNotEnabled	Kms service is not Enabled for current user. Please get access permission first	403
Forbidden.ProhibitedByRiskControl	Current user is Prohibited By Risk Control	403
Forbidden.InDebtOverdue	Current user is indebted Overdue	403
Forbidden.InDebt	Current user is indebted	403
ParseRequestParameterException	Server parse parameters exception. Please check your input params.	400

Error code	Error message	HTTP status code
MissingParameter	The parameter "< parameter name >" is needed but not provided.	400
InvalidParameter	The specified parameter "< parameter name >" is not valid.	400
IncompleteSignature	The request signature does not conform to Alibaba Cloud standards.	400
IllegalTimestamp	The input parameter "Timestamp" that is required for processing this request is not supplied.	400
Rejected.LimitExceeded	The request was rejected because user create resource limit was exceeded.	400
AliasAlreadyExists	AliasName Already Exists	400
InvalidKeyMaterial	key material is invalid	400
InvalidImportToken	import token is invalid	400
ExpiredImportToken	import token is expired	400
Unsupported.Origin	This key origin is not valid for this api	400
Unsupported.Alias	Alias is not valid for this api	400
Rejected.StateModifiedFailed	Keystate modified failed	409
Rejected.Disabled	The request was rejected because the key state is Disabled	409
Rejetced.PendingDeletion	The request was rejected because the key state is PendingDeletion	409
Rejected.PendingImport	The request was rejected because the key state is PendingImport	409

2.17.1.2. Use RAM to authorize KMS resources

A Customer Master Key (CMK) that you create is your own resource.

You have full operation permissions on resources that you own, and can use APIs to perform operations on them by default.

You can use an Apsara Stack tenant account to create RAM users. Unauthorized RAM users cannot operate on resources owned by an Apsara Stack tenant account. RAM users must be granted permission to access resources owned by an Apsara Stack tenant account through RAM authorization.

Before you authorize a RAM user to access a CMK, be sure to read and understand the RAM and API documentation.

KMS resource types that can be authorized in RAM

The ARN formats for the two types of KMS key resources are as follows:

```
acs:kms:${region-id}:${resource-owner-id}:key/${key-uuid}
acs:kms:${region-id}:${resource-owner-id}:key
```

KMS operations

Operations available in KMS are as follows:

- Create a secret

  CreateKey
- Generate a DEK

  GenerateDataKey
- Encrypt data

  Encrypt
- Decrypt data

  Decrypt
- View key details

  DescribeKey
- List keys

  ListKeys

Mapping of actions and resources in the RAM authorization

Mapping of actions and resources in RAM authorization lists the actions and resources.

Mapping of actions and resources in RAM authorization

API	Action	Resource
CreateKey	kms:CreateKey	acs:kms:$regionid:${resource-owner-id}:key
ListKeys	kms:ListKeys	acs:kms:$regionid:${resource-owner-id}:key
GenerateDataKey	kms:GenerateDataKey	acs:kms:$regionid:${resource-owner-id}:key/${keyid}

API	Action	Resource
Encrypt	kms:Encrypt	acs:kms:$regionid:${resource-owner-id}:key/${keyid}
Decrypt	kms:Decrypt	acs:kms:$regionid:${resource-owner-id}:key/${keyid}
DescribeKey	kms:DescribeKey	acs:kms:$regionid:${resource-owner-id}:key/${keyid}
EnableKey	kms:EnableKey	acs:kms:$regionid:${resource-owner-id}:key/${keyid}
DisableKey	kms:DisableKey	acs:kms:$regionid:${resource-owner-id}:key/${keyid}
ScheduleKeyDeletion	kms:ScheduleKeyDeletion	acs:kms:$regionid:${resource-owner-id}:key/${keyid}
CancelKeyDeletion	kms:CancelKeyDeletion	acs:kms:$regionid:${resource-owner-id}:key/${keyid}

2.17.1.3. Encryption Context

Functions of Encryption Context

Encryption Context is a JSON string in the `string-string` format that may be used to protect data integrity in KMS APIs, such as Encrypt, GenerateDataKey, and Decrypt).

If this parameter is specified during encryption operations (Encrypt and GenerateDataKey), an equivalent parameter is also required to decrypt the ciphertext.

Encryption Context is related to decryption but it is not included in the encrypted CipherBlob.

Valid value of Encryption Context

The Encryption Context can be a JSON string up to 8,192 characters in the `string-string` format.

> **Note** When you call the preceding APIs to fill in Encryption Context, notice the escape character.

Examples:

- Valid Encryption Context

```
1. {"ValidKey":"ValidValue"}
2. {"Key1":"Value1","Key2":"Value2"}
```

- Invalid Encryption Context

```
1. [{"Key": "Value"}] // json array
2. {"Key":12345} //String-int
3. {"Key": ["value1", "value2"]} // String-array
```

Equivalent Encryption Context

In essence, Encryption Context is a hashtable map in the string-string format. Therefore, you only need to ensure that the `key-value` pairs indicated by the JSON string has the same meaning when Encryption Context is used as a parameter. In these cases, the Encryption Context is considered equivalent. You can use an equivalent Encryption Context to decrypt a ciphertext instead of the original string used for encryption.

Equivalent Encryption Context example:

```
{"Key1":"Value1","Key2":"Value2"} is equivalent to {"Key2":"Value2","Key1":"Value1"}
```

2.17.1.4. Impact of CMK states on API calls

In Key Management Service (KMS), each Customer Master Key (CMK) has three states: Enabled, Disabled, and PendingDeletion.

A new CMK is in the Enabled state by default. Only CMKs in the Enabled state can be used to encrypt and decrypt data. The expected responses of API calls vary depending on different key states.

Key status codes and the expected responses of API calls lists the status codes and expected responses.

Key status codes and the expected responses of API calls

Expected response	HTTP status code
Success	200
Rejected.Enabled	409
Rejected.Disabled	409
Rejected.PendingDeletion	409
Rejected.StateModifiedFailed	409

CMKs in the PendingDeletion state are permanently deleted after the scheduled period expires.

Key states and the expected responses of API calls lists the states and expected responses.

Key states and the expected responses of API calls

API	Enabled	Disabled	PendingDeletion
CreateKey	Success	Success	Success

API	Enabled	Disabled	PendingDeletion
GenerateDataKey	Success	Rejected.Disabled	Rejected.PendingDeletion
Encrypt	Success	Rejected.Disabled	Rejected.PendingDeletion
Decrypt	Success	Rejected.Disabled	Rejected.PendingDeletion
ListKeys	Success	Success	Success
DescribeKey	Success	Success	Success
EnableKey	Success	Success	Rejected.StateModifiedFailed
DisableKey	Success	Success	Rejected.StateModifiedFailed
ScheduleKeyDeletion	Success	Success	Rejected.StateModifiedFailed
CancelKeyDeletion	Rejected.StateModifiedFailed	Rejected.StateModifiedFailed	Success

2.17.1.5. API list

2.17.1.5.1. CancelKeyDeletion

You can call this operation to cancel the scheduled deletion of a CMK.

When the scheduled deletion of a CMK is canceled, the key returns to the Enabled state.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK.

Response parameters

Name	Type	Description
RequestId	String	The ID of the request.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=CancelKeyDeletion
&KeyId=<cmkid>
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
"RequestId": "3da5b8cc-8107-40ac-a170-793cd181d7b7"
}
```

XML format

```
//xml response
<KMS>
  <RequestId>3da5b8cc-8107-40ac-a170-793cd181d7b7</RequestId>
</KMS>
```

2.17.1.5.2. CreateKey

You can call this operation to create a CMK.

CMKs can be used to encrypt small strings of data, under 4 KB. Though these CMKs can be used to manually encrypt a DEK, in most cases you can call the GenerateDataKey API to generate DEKs. For more information about how to generate a DEK, see GenerateDataKey.

Request parameters

Name	Type	Required	Description
Origin	String	Yes	The source of the CMK material. If it is set to `External`, you must import the CMK material.
Description	String	No	The description of the CMK. It must be 0 to 8,192 characters in length.
KeyUsage	String	No	The intended use of the CMK. Default value: ENCRYPT/DECRYPT.

Response parameters

Name	Type	Description
KeyMetadata	KeyMetadata	The metadata associated with the CMK.

KeyMetadata

Name	Type	Description
CreationDate	Timestamp	The date and time when the CMK is created, in the UTC format.
Description	String	The description of the CMK.
KeyId	String	The globally unique ID of the CMK.
KeyState	String	The state of the CMK.
KeyUsage	String	The intended use of the CMK. Default value: ENCRYPT/DECRYPT.
DeleteDate	Timestamp	The scheduled period before the CMK is deleted. • If this value is null, there is no deletion scheduled for the CMK. • This parameter is present only when `KeyState` is **PendingDeletion**.
Creator	String	The creator of the CMK.
Arn	String	The Alibaba Cloud resource name of the CMK.
Origin	String	The source of the CMK material.
MaterialExpireTime	String	The date and time when the key expires, in the UTC format. If this value is null, there is no expiration time for the CMK material.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=CreateKey
&Description=test
&KeyUsage=ENCRYPT/DECRYPT
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
  "KeyMetadata": {
    "CreationDate": "2016-03-25T10:42:40Z",
    "Description": "test",
    "KeyId": "******************",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT/DECRYPT",
    "DeleteDate": ""
  },
  "RequestId": "3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

XML format

```
//xml response
<KMS>
 <KeyMetadata>
   <CreationDate>2016-03-25T10:40:47Z</CreationDate>
   <Description>test</Description>
   <KeyId>******************</KeyId>
   <KeyState>Enabled</KeyState>
   <KeyUsage>ENCRYPT/DECRYPT</KeyUsage>
 </KeyMetadata>
 <RequestId>6cb4bf6b-d9c9-4660-af5f-2328378e7257</RequestId>
</KMS>
```

2.17.1.5.3. Decrypt

You can call this operation to decrypt the encrypted `CiphertextBlob` that is generated by the following APIs:

- GenerateDataKey

- Encrypt

Request parameters

Name	Type	Required	Description
CiphertextBlob	String	Yes	The ciphertext to be decrypted.
EncryptionContext	String	No	The JSON string of the key-value pair. If you specify this parameter in the `Encrypt` or `GenerateDataKey` API, you need to provide the same parameter before you can decrypt the ciphertext. For more information, see Encryption Context.

Response parameters

Name	Type	Description
KeyId	String	The globally unique ID of the CMK. It is the CMK ID used by the encrypted ciphertext.
Plaintext	String	The decrypted plaintext.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=Decrypt
&CiphertextBlob=<your ciphertextblob>
&EncryptionContext = <json string>
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
"KeyId": "KeyId"
"Plaintext": "Plaintext"
"RequestId": "207596a2-36d3-4840-b1bd-f87044699bd7"
}
```

XML format

```
//xml response
<KMS>
   <KeyId>KeyId</KeyId>
   <Plaintext>Plaintext</Plaintext>
   <RequestId>4bd560a1-729e-45f1-a3d9-b2a33d61046b</RequestId>
</KMS>
```

2.17.1.5.4. DescribeKey

You can call this operation to return and view detailed information about a specified CMK.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK. The API supports aliases.

Response parameters

Name	Type	Description
KeyMetadata	KeyMetadata	The metadata of the CMK.

KeyMetadata

Name	Type	Description
CreationDate	Timestamp	The date and time when the CMK is created, in the UTC format.
Description	String	The description of the CMK.
KeyId	String	The globally unique ID of the CMK.

Name	Type	Description
KeyState	String	The state of the CMK.
KeyUsage	String	The intended use of the CMK.
DeleteDate	Timestamp	The scheduled period before the CMK is deleted. For more information, see ScheduleKeyDeletion. This parameter is present only when `KeyState` is *PendingDeletion*.
Creator	String	The creator of the CMK.
Arn	String	The Alibaba Cloud resource name of the CMK.
Origin	String	The source of the CMK material.
MaterialExpireTime	String	The date and time when the key expires, in the UTC format. If this value is null, there is no expiration time for the CMK material.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=DescribeKey
&KeyId=<your-key-id>
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
  "KeyMetadata": {
    "CreationDate": "2016-03-25T10:42:40Z",
    "Description": "test",
    "KeyId": "********************",
    "KeyState": "Enabled",
    "KeyUsage": "ENCRYPT/DECRYPT",
    "DeleteDate": "",
    "Creator": "********************"
  },
  "RequestId": "3455b9b4-95c1-419d-b310-db6a53b09a39"
}
```

XML format

```
//xml response
<KMS>
 <KeyMetadata>
   <CreationDate>2016-03-25T10:40:47Z</CreationDate>
   <Description>test</Description>
   <KeyId>********************</KeyId>
   <KeyState>Enabled</KeyState>
   <KeyUsage>ENCRYPT/DECRYPT</KeyUsage>
   <DeleteDate></DeleteDate>
   <Creator>********************</Creator>
 </KeyMetadata>
<RequestId>6cb4bf6b-d9c9-4660-af5f-2328378e7257</RequestId>
</KMS>
```

2.17.1.5.5. DescribeRegions

You can call this operation to view the list of regions.

Response parameters

Name	Type	Description
RegionId	String	The ID of the region.

Examples

Sample responses

JSON format

```
//json response
{
  "Regions": {
    "Region": [
      {
        "RegionId": "cn-beijing"
      },
      {
        "RegionId": "cn-zhangjiakou"
      },
      {
        "RegionId": "cn-hangzhou"
      }
    ]
  },
  "RequestId": "815240e2-aa37-4c26-9cca-05d4df3e8fe6"
}
```

XML format

```
//xml response
<KMS>
  <Regions>
    <Region>
      <RegionId>cn-beijing</RegionId>
    </Region>
    <Region>
      <RegionId>cn-zhangjiakou</RegionId>
    </Region>
    <Region>
      <RegionId>cn-hangzhou</RegionId>
    </Region>
  </Regions>
  <RequestId>f7f4f9d2-11f5-4710-bbdb-08ba27deb4b8</RequestId>
</KMS>
```

2.17.1.5.6. DisableKey

You can all this operation to disable a specified CMK. A disabled CMK cannot be used for encryption or decryption. A ciphertext key that was encrypted by a disabled CMK cannot be decrypted until the CMK is enabled again.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK.

Response parameters

Name	Type	Description
RequestId	String	The ID of the request.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=DisableKey
&KeyId=<cmkid>
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
"RequestId": "2fe70ce2-3303-4fd6-b3ac-472fb2705c62"
}
```

XML format

```
//xml response
<KMS>
  <RequestId>2fe70ce2-3303-4fd6-b3ac-472fb2705c62</RequestId>
</KMS>
```

2.17.1.5.7. EnableKey

You can call this operation to enable a specified CMK.

Request format

```
KeyId="string"
```

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK.

Response parameters

Name	Type	Description
RequestId	String	The ID of the request.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=EnableKey
&KeyId=<cmkid>
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
"RequestId": "efb1cbbd-a093-4278-bc03-639dd4fcc207"
}
```

XML format

```
//xml response
<KMS>
  <RequestId>efb1cbbd-a093-4278-bc03-639dd4fcc207</RequestId>
</KMS>
```

2.17.1.5.8. Encrypt

You can call this operation to create a ciphertext DEK by encrypting a plaintext DEK using your CMK.

- Only data keys which do not exceed 4 KB in size can be encrypted, such as RSA keys, database keys, or other sensitive customer data.

- If you migrate encrypted data from one region to another, you can use this API to encrypt the DataKey plaintext to be used for encrypting data in the previous region. By doing this, you can provide an encrypted `CiphertextBlob` that is recognized by the new region and can be decrypted by calling the Decrypt API in the new region.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK. The API supports aliases.
Plaintext	String	Yes	The plaintext key to be encrypted.
EncryptionContext	String to string map	No	The JSON string of the key-value pair. If you specify this parameter, you need to provide the same parameter when you call the `Decrypt` API. For more information, see Encryption Context.

Response parameters

Name	Type	Description
KeyId	String	The globally unique ID of the CMK. If you use an alias in the request, the CMK ID of the alias is returned.
CiphertextBlob	String	The encrypted ciphertext.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=Encrypt
&KeyId=<your-key-id>
&Plaintext=<data need encrypt>
&EncryptionContext=<json string>
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
  "KeyId": "your-key-id",
  "CiphertextBlob": "CiphertextBlob",
  "RequestId": "475f1620-b9d3-4d35-b5c6-3fbdd941423d"
}
```

XML format

```
//xml response
<KMS>
  <KeyId>your-key-id</KeyId>
  <CiphertextBlob>CiphertextBlob</CiphertextBlob>
  <RequestId>475f1620-b9d3-4d35-b5c6-3fbdd941423d</RequestId>
</KMS>
```

2.17.1.5.9. GenerateDataKey

You can call this operation to create a DEK. You can then use this DEK to encrypt data locally.

A `Plaintext` (the plaintext DEK) and a `CiphertextBlob` (the ciphertext DEK) are returned.

The DEK is encrypted by using the CMK that corresponds to the ID specified in the request. You can call the `Decrypt` API to decrypt the DEK.

> **Notice**
>
> We recommend that you encrypt data locally by using the following method:
>
> - Call the `GenerateDataKey` API. Use the Plaintext to encrypt data locally and then delete the Plaintext from memory. Store the `CiphertextBlob` and the encrypted data.
> - To decrypt data, call the `Decrypt` API and use the `CiphertextBlob` as a parameter. If the call is successful, the `Plaintext` is returned. Use the Plaintext to decrypt data locally.

Request parameters

Name	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK. The API supports aliases. For more information, see Alias instructions.

Name	Type	Required	Description
KeySpec	String	No	The length and type of the DEK: AES_256 refers to a 256-bit symmetric key. AES_128 refers to a 128-bit symmetric key.
NumberOfBytes	Integer	No	The length of the data key in bytes. Valid values: 1 to 1,024.
EncryptionContext	String to string map	No	The JSON string of the key-value pair. If you specify this parameter, you need to provide the same parameter when you call the Decrypt API. For more information, see EncryptionContext.

Response parameters

Name	Type	Description
KeyId	String	The globally unique ID of the CMK. If you use an alias in the request, the CMK ID of the alias is returned.
Plaintext	String	The plaintext DEK.
CiphertextBlob	String	The encrypted DEK.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=GenerateDataKey
&KeyId=<your-key-id>
&KeySpec=AES_256
&EncryptionContext={"Example":"Example"}
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
  "CiphertextBlob": "CiphertextBlob",
  "KeyId": "KeyId",
  "Plaintext": "Plaintext",
  "RequestId": "7021b6ec-4be7-4d3c-8a68-1e85d4d515a0"
}
```

XML format

```
//xml response
<KMS>
  <CiphertextBlob>CiphertextBlob</CiphertextBlob>
  <KeyId>KeyId</KeyId>
  <Plaintext>Plaintext</Plaintext>
  <RequestId>7021b6ec-4be7-4d3c-8a68-1e85d4d515a0</RequestId>
</KMS>
```

2.17.1.5.10. ListKeys

You can call this operation to list the IDs of all CMKs in your region.

Request parameters

Name	Type	Required	Description
PageNumber	Integer	No	The current page number. It must be an integer greater than 0. Default value: 1.
PageSize	Integer	No	The number of items on each page. It must be an integer greater than 0 but less than 101. Default value: 10.

Response parameters

Name	Type	Description
KeyId	String	The globally unique ID of the CMK.
TotalCount	Integer	The total number of CMKs.
PageNumber	Integer	The current page number.

Name	Type	Description
PageSize	Integer	The number of items on each page.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=ListKeys
&PageNumber=1
&PageSize=10
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
  "Keys": {
    "Key": [
      {
        "KeyId": "key1"
      },
      {
        "KeyId": "key2"
      },
      {
        "KeyId": "key3"
      }
    ]
  },
  "TotalCount": 3,
  "PageNumber": 1,
  "PageSize": 10,
  "RequestId": "1fbcd12a-1b7f-468f-84a3-1ff3444dfd8b"
}
```

XML format

```
//xml response
<KMS>
  <Keys>
    <Key>
      <KeyId>key1</KeyId>
    </Key>
    <Key>
      <KeyId>key2</KeyId>
    </Key>
    <Key>
      <KeyId>key3</KeyId>
    </Key>
  </Keys>
  <TotalCount>3</TotalCount>
  <PageNumber>1</PageNumber>
  <PageSize>10</PageSize>
  <RequestId>1050b8f1-b264-496d-a782-6299cbaf15f8</RequestId>
</KMS>
```

2.17.1.5.11. ScheduleKeyDeletion

You can call this operation to schedule CMK deletion.

- Before the scheduled period has expired,
  - the CMK is in the PendingDeletion state and cannot be used for encryption, decryption, or DEK generation.
  - We recommend that you use DisableKey.
  - A deleted CMK cannot be restored, and the content encrypted and the DEK generated by using the CMK cannot be decrypted. Because of these risks, CMKs cannot be deleted directly and their deletion must be scheduled in advance.
- You must specify a scheduled period for CMK deletion. The period can range from 7 to 30 days, and the CMK will be deleted when the scheduled period expires. You can call the CancelKeyDeletion API to cancel the request after submission but before the end of the scheduled period.
- The key is guaranteed to be deleted within 24 hours after the scheduled period.

  For example, suppose User A sends a request to delete a CMK at 14:00, September 10, 2016 with a scheduled period of seven days. KMS will delete the CMK within 24 hours after 14:00, September 17.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
KeyId	String	Yes	The globally unique ID of the CMK.
PendingWindowInDays	Integer	Yes	The scheduled period, specified in number of days. During this period, the CMK is in the **PendingDeletion** state and the scheduled deletion can be canceled. After the period expires, the deletion cannot be canceled. Valid values: 7 to 30.

Response parameters

Name	Type	Description
RequestId	String	The ID of the request.

Examples

Sample request

```
https://kms.cn-hangzhou.example.com/?Action=ScheduleKeyDeletion
&KeyId=<your-key-id>
&PendingWindowInDays=[7~30]
&<Common request parameters>
```

Sample responses

JSON format

```
//json response
{
"RequestId": "52ac67cb-3d3d-4ada-b4e2-7047660d3ce9"
}
```

XML format

```
//xml response
<KMS>
  <RequestId>52ac67cb-3d3d-4ada-b4e2-7047660d3ce9</RequestId>
</KMS>
```

2.17.2. SDK reference

2.17.2.1. Create an AccessKey pair

You can create an AccessKey pair in the Apsara Stack console.

2.17.2.2. SDK

Alibaba Cloud provides SDKs in the following four languages:

- Java
- Python
- PHP
- C#

For SDKs in other languages, go to Third-party SDK services.

2.17.2.3. JAVA SDK sample code

Sample code

```
package com.alibaba.samples;
import java.util.*;
import java.util.List;
import com.aliyuncs.DefaultAcsClient;
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.http.FormatType;
import com.aliyuncs.http.MethodType;
import com.aliyuncs.http.ProtocolType;
//Current KMS SDK version:2016-01-20
import com.aliyuncs.kms.model.v20160120. CreateKeyRequest;
import com.aliyuncs.kms.model.v20160120. CreateKeyResponse;
import com.aliyuncs.kms.model.v20160120. DecryptRequest;
import com.aliyuncs.kms.model.v20160120. DecryptResponse;
import com.aliyuncs.kms.model.v20160120. DescribeKeyRequest;
import com.aliyuncs.kms.model.v20160120. DescribeKeyResponse;
import com.aliyuncs.kms.model.v20160120. EncryptRequest;
import com.aliyuncs.kms.model.v20160120. EncryptResponse;
import com.aliyuncs.kms.model.v20160120. GenerateDataKeyRequest;
import com.aliyuncs.kms.model.v20160120. GenerateDataKeyResponse;
import com.aliyuncs.kms.model.v20160120. ListKeysRequest;
import com.aliyuncs.kms.model.v20160120. ListKeysResponse;
import com.aliyuncs.kms.model.v20160120. ListKeysResponse.Key;
import com.aliyuncs.profile.DefaultProfile;
```

```
import com.aliyuncs.profile.IClientProfile;
public class kmsSample
{
    static DefaultAcsClient kmsClient;
    private static DefaultAcsClient kmsClient(String regionId, String accessKeyId, String accessKeySecret)
{
        /**
         * Construct an Aliyun Client:
         * Set RegionId, AccessKeyId and AccessKeySecret
         */
        IClientProfile profile = DefaultProfile.getProfile(regionId, accessKeyId, accessKeySecret);
        DefaultAcsClient client = new DefaultAcsClient(profile);
        return client;
    }
    private static CreateKeyResponse CreateKey(String keyDesc, String keyUsage) throws ClientExceptio
n {
        final CreateKeyRequest ckReq = new CreateKeyRequest();
        ckReq.setProtocol(ProtocolType.HTTPS);
        ckReq.setAcceptFormat(FormatType.JSON);
        ckReq.setMethod(MethodType.POST);
        ckReq.setDescription(keyDesc);
        ckReq.setKeyUsage(keyUsage);
        final CreateKeyResponse response = kmsClient.getAcsResponse(ckReq);
        return response;
    }
    private static DescribeKeyResponse DescribeKey(String keyId) throws ClientException {
        final DescribeKeyRequest decKeyReq = new DescribeKeyRequest();
        decKeyReq.setProtocol(ProtocolType.HTTPS);
        decKeyReq.setAcceptFormat(FormatType.JSON);
        decKeyReq.setMethod(MethodType.POST);
        decKeyReq.setKeyId(keyId);
        final DescribeKeyResponse decKeyRes = kmsClient.getAcsResponse(decKeyReq);
        return decKeyRes;
    }
    private static ListKeysResponse ListKey(int pageNumber, int pageSize) throws ClientException {
        final ListKeysRequest listKeysReq = new ListKeysRequest();
        listKeysReq.setProtocol(ProtocolType.HTTPS);
        listKeysReq.setAcceptFormat(FormatType.JSON);
        listKeysReq.setMethod(MethodType.POST);
        listKeysReq.setPageNumber(pageNumber);
        listKeysReq.setPageSize(pageSize);
        final ListKeysResponse listKeysRes = kmsClient.getAcsResponse(listKeysReq);
```

```
        return listKeysRes;
    }
    private static GenerateDataKeyResponse GenerateDataKey(String keyId, String keyDesc, int numOfBy
tes) throws ClientException {
        final  GenerateDataKeyRequest genDKReq = new GenerateDataKeyRequest();
        genDKReq.setProtocol(ProtocolType.HTTPS);
        genDKReq.setAcceptFormat(FormatType.JSON);
        genDKReq.setMethod(MethodType.POST);
        /**
         * Set parameter according to KMS openAPI document:
         * 1. KeyId
         * 2. KeyDescription
         * 3. NumberOfBytes
         */
        genDKReq.setKeySpec(keyDesc);
        genDKReq.setKeyId(keyId);
        genDKReq.setNumberOfBytes(numOfBytes);
        final GenerateDataKeyResponse genDKRes = kmsClient.getAcsResponse(genDKReq);
        return genDKRes;
    }
    private static  EncryptResponse Encrypt(String keyId, String plainText) throws ClientException {
        final EncryptRequest encReq = new EncryptRequest();
        encReq.setProtocol(ProtocolType.HTTPS);
        encReq.setAcceptFormat(FormatType.JSON);
        encReq.setMethod(MethodType.POST);
        encReq.setKeyId(keyId);
        encReq.setPlaintext(plainText);
        final EncryptResponse encResponse = kmsClient.getAcsResponse(encReq);
        return encResponse;
    }
    private static DecryptResponse Decrypt(String cipherBlob) throws ClientException {
        final DecryptRequest decReq = new DecryptRequest();
        decReq.setProtocol(ProtocolType.HTTPS);
        decReq.setAcceptFormat(FormatType.JSON);
        decReq.setMethod(MethodType.POST);
        decReq.setCiphertextBlob(cipherBlob);
        final DecryptResponse decResponse = kmsClient.getAcsResponse(decReq);
        return decResponse;
    }
    public static void main(String[] args) {
        System.out.println("============================================");
```

```
        System.out.println("Getting Started with KMS Service");
        System.out.println("=========================================\n");
        /**
         * RegionId: "cn-hangzhou" and "ap-southeast-1", eg. "cn-hangzhou"
         */
        String regionId = "cn-hangzhou";
        String accessKeyId = "*** Provide your AccessKeyId ***";
        String accessKeySecret = "*** Provide your AccessKeySecret ***";
        kmsClient = kmsClient(regionId, accessKeyId, accessKeySecret);
        String keyId = null;
        String plainText = "hello world";
        String cipherBlob = null;
//      /*Create a Key*/
//      try {
//          final CreateKeyResponse response = CreateKey("testkey", "ENCRYPT/DECRYPT");
//
//          /**
//           * Parse response and do more further
//           */
//          System.out.println(response.getKeyMetadata());
//          CreateKeyResponse.KeyMetadata meta = response.getKeyMetadata();
//
//          System.out.println("CreateTime: " + meta.getCreationDate());
//          System.out.println("Description: " + meta.getDescription());
//          System.out.println("KeyId: " + meta.getKeyId());
//          keyId = meta.getKeyId();
//          System.out.println("KeyState: " + meta.getKeyState());
//          System.out.println("KeyUsage: " + meta.getKeyUsage());
//
//          System.out.println("=========================================");
//          System.out.println("Create MasterKey Success!") ;
//          System.out.println("=========================================\n");
//      } catch (ClientException eResponse) {
//          System.out.println("Failed.") ;
//          System.out.println("Error code: " + eResponse.getErrCode());
//          System.out.println("Error message: " + eResponse.getErrMsg());
//      }
//
        /*List all MasterKeys in your account*/
        try {
            final ListKeysResponse listKeysRes = ListKey(1, 100);
            /**
```

```
        /**
         * Parse response and do more further
         */
        System.out.println("TotalCount: " + listKeysRes.getTotalCount());
        System.out.println("PageNumber: " + listKeysRes.getPageNumber());
        System.out.println("PageSize: " + listKeysRes.getPageSize());
        List<Key> keys = listKeysRes.getKeys();
        Iterator<Key> iterator = keys.iterator();
        while (iterator.hasNext()) {
            keyId = iterator.next().getKeyId();
            System.out.println("KeyId: " + keyId);
        }
        System.out.println("==========================================");
        System.out.println("List All MasterKeys success! \n");
        System.out.println("==========================================\n");
    } catch (ClientException eResponse) {
        System.out.println("Failed.") ;
        System.out.println("Error code: " + eResponse.getErrCode());
        System.out.println("Error message: " + eResponse.getErrMsg());
    }
    /*Describe the Key */
    try {
        final DescribeKeyResponse decKeyRes = DescribeKey(keyId);
        /**
         * Parse response and do more further
         */
        System.out.println("DescribeKey Response: ");
        DescribeKeyResponse.KeyMetadata meta = decKeyRes.getKeyMetadata();
        System.out.println("KeyId: " + meta.getKeyId());
        System.out.println("Description: " + meta.getDescription());
        System.out.println("KeyState: " + meta.getKeyState());
        System.out.println("KeyUsage: " + meta.getKeyUsage());
        System.out.println("==========================================");
        System.out.println("Describe the MasterKey success!") ;
        System.out.println("==========================================\n");
    } catch (ClientException eResponse) {
        System.out.println("Failed.") ;
        System.out.println("Error code: " + eResponse.getErrCode());
        System.out.println("Error message: " + eResponse.getErrMsg());
    }
    /*Generate DataKey*/
    /**
```

```
 * Request and got response
 */
try {
    final GenerateDataKeyResponse genDKResponse = GenerateDataKey(keyId, "AES_256", 64);
    /**
     * Parse response and do more further
     */
    System.out.println("CiphertextBlob: " + genDKResponse.getCiphertextBlob());
    System.out.println("KeyId: " + genDKResponse.getKeyId());
    System.out.println("Plaintext: " + genDKResponse.getPlaintext());
    System.out.println("==========================================");
    System.out.println("Generate DataKey success!") ;
    System.out.println("==========================================\n");
} catch (ClientException eResponse) {
    System.out.println("Failed.") ;
    System.out.println("Error code: " + eResponse.getErrCode());
    System.out.println("Error message: " + eResponse.getErrMsg());
}
/**
 * Encrypt the plain text and got a cipher one
 */
try {
    EncryptResponse encResponse = Encrypt(keyId, plainText);
    cipherBlob = encResponse.getCiphertextBlob();
    System.out.println("CiphertextBlob: " + cipherBlob);
    System.out.println("KeyId: " + encResponse.getKeyId());
    System.out.println("==========================================");
    System.out.println("Encrypt the plain text success!") ;
    System.out.println("==========================================\n");
} catch (ClientException eResponse) {
    System.out.println("Failed.") ;
    System.out.println("Error code: " + eResponse.getErrCode());
    System.out.println("Error message: " + eResponse.getErrMsg());
}
/**
 * Decrypt the cipher text and verify result with original plain text.
 */
try {
    DecryptResponse decResponse = Decrypt(cipherBlob);
    System.out.println("Plaintext: " + decResponse.getPlaintext());
    String verifyPlainText = decResponse.getPlaintext();
```

```
            int isMatch = verifyPlainText.compareTo(plainText);
            System.out.println("KeyId: " + decResponse.getKeyId());
            System.out.println("=========================================");
            System.out.printf("Decrypt the cipher text success, result " + (isMatch == 0 ? "match" : "mismatch"
+ "\n"));
            System.out.println("=========================================\n");
        } catch (ClientException eResponse) {
            System.out.println("Failed.") ;
            System.out.println("Error code: " + eResponse.getErrCode());
            System.out.println("Error message: " + eResponse.getErrMsg());
        }
    }
}
```

Access KMS in a VPC environment

You must add a custom endpoint directing to a domain name in the VPC. You must also specify to use this endpoint when accessing KMS later.

```
DefaultProfile.addEndpoint("cn-hangzhou-vpc", "cn-hangzhou-vpc", "Kms", "kms-vpc.cn-hangzhou.aliyun
cs.com"); //Add a custom endpoint.
```

2.17.2.4. Create an AccessKey pair

You can create an AccessKey pair in the Apsara Stack console.

2.17.2.5. SDK

Alibaba Cloud provides SDKs in the following four languages:

- Java
- Python
- PHP
- C#

For SDKs in other languages, go to Third-party SDK services.

2.17.2.6. JAVA SDK sample code

Sample code

```
package com.alibaba.samples;
import java.util.*;
import java.util.List;
import com.aliyuncs.DefaultAcsClient;
```

```
import com.aliyuncs.exceptions.ClientException;
import com.aliyuncs.http.FormatType;
import com.aliyuncs.http.MethodType;
import com.aliyuncs.http.ProtocolType;
//Current KMS SDK version:2016-01-20
import com.aliyuncs.kms.model.v20160120. CreateKeyRequest;
import com.aliyuncs.kms.model.v20160120. CreateKeyResponse;
import com.aliyuncs.kms.model.v20160120. DecryptRequest;
import com.aliyuncs.kms.model.v20160120. DecryptResponse;
import com.aliyuncs.kms.model.v20160120. DescribeKeyRequest;
import com.aliyuncs.kms.model.v20160120. DescribeKeyResponse;
import com.aliyuncs.kms.model.v20160120. EncryptRequest;
import com.aliyuncs.kms.model.v20160120. EncryptResponse;
import com.aliyuncs.kms.model.v20160120. GenerateDataKeyRequest;
import com.aliyuncs.kms.model.v20160120. GenerateDataKeyResponse;
import com.aliyuncs.kms.model.v20160120. ListKeysRequest;
import com.aliyuncs.kms.model.v20160120. ListKeysResponse;
import com.aliyuncs.kms.model.v20160120. ListKeysResponse.Key;
import com.aliyuncs.profile.DefaultProfile;
import com.aliyuncs.profile.IClientProfile;
public class kmsSample
{
   static DefaultAcsClient kmsClient;
   private static DefaultAcsClient kmsClient(String regionId, String accessKeyId, String accessKeySecret)
{
      /**
       * Construct an Aliyun Client:
       * Set RegionId, AccessKeyId and AccessKeySecret
       */
      IClientProfile profile = DefaultProfile.getProfile(regionId, accessKeyId, accessKeySecret);
      DefaultAcsClient client = new DefaultAcsClient(profile);
      return client;
   }
   private static CreateKeyResponse CreateKey(String keyDesc, String keyUsage) throws ClientExceptio
n {
      final CreateKeyRequest ckReq = new CreateKeyRequest();
      ckReq.setProtocol(ProtocolType.HTTPS);
      ckReq.setAcceptFormat(FormatType.JSON);
      ckReq.setMethod(MethodType.POST);
      ckReq.setDescription(keyDesc);
      ckReq.setKeyUsage(keyUsage);
      final CreateKeyResponse response = kmsClient.getAcsResponse(ckReq);
```

```
        return response;
    }
    private static DescribeKeyResponse DescribeKey(String keyId) throws ClientException {
        final DescribeKeyRequest decKeyReq = new DescribeKeyRequest();
        decKeyReq.setProtocol(ProtocolType.HTTPS);
        decKeyReq.setAcceptFormat(FormatType.JSON);
        decKeyReq.setMethod(MethodType.POST);
        decKeyReq.setKeyId(keyId);
        final DescribeKeyResponse decKeyRes = kmsClient.getAcsResponse(decKeyReq);
        return decKeyRes;
    }
    private static ListKeysResponse ListKey(int pageNumber, int pageSize) throws ClientException {
        final ListKeysRequest listKeysReq = new ListKeysRequest();
        listKeysReq.setProtocol(ProtocolType.HTTPS);
        listKeysReq.setAcceptFormat(FormatType.JSON);
        listKeysReq.setMethod(MethodType.POST);
        listKeysReq.setPageNumber(pageNumber);
        listKeysReq.setPageSize(pageSize);
        final ListKeysResponse listKeysRes = kmsClient.getAcsResponse(listKeysReq);
        return listKeysRes;
    }
    private static GenerateDataKeyResponse GenerateDataKey(String keyId, String keyDesc, int numOfBy
tes) throws ClientException {
        final  GenerateDataKeyRequest genDKReq = new GenerateDataKeyRequest();
        genDKReq.setProtocol(ProtocolType.HTTPS);
        genDKReq.setAcceptFormat(FormatType.JSON);
        genDKReq.setMethod(MethodType.POST);
        /**
         * Set parameter according to KMS openAPI document:
         * 1. KeyId
         * 2. KeyDescription
         * 3. NumberOfBytes
         */
        genDKReq.setKeySpec(keyDesc);
        genDKReq.setKeyId(keyId);
        genDKReq.setNumberOfBytes(numOfBytes);
        final GenerateDataKeyResponse genDKRes = kmsClient.getAcsResponse(genDKReq);
        return genDKRes;
    }
    private static  EncryptResponse Encrypt(String keyId, String plainText) throws ClientException {
        final EncryptRequest encReq = new EncryptRequest();
```

```
        encReq.setProtocol(ProtocolType.HTTPS);
        encReq.setAcceptFormat(FormatType.JSON);
        encReq.setMethod(MethodType.POST);
        encReq.setKeyId(keyId);
        encReq.setPlaintext(plainText);
        final EncryptResponse encResponse = kmsClient.getAcsResponse(encReq);
        return encResponse;
    }
    private static DecryptResponse Decrypt(String cipherBlob) throws ClientException {
        final DecryptRequest decReq = new DecryptRequest();
        decReq.setProtocol(ProtocolType.HTTPS);
        decReq.setAcceptFormat(FormatType.JSON);
        decReq.setMethod(MethodType.POST);
        decReq.setCiphertextBlob(cipherBlob);
        final DecryptResponse decResponse = kmsClient.getAcsResponse(decReq);
        return decResponse;
    }
    public static void main(String[] args) {
        System.out.println("============================================");
        System.out.println("Getting Started with KMS Service");
        System.out.println("============================================\n");
        /**
         * RegionId: "cn-hangzhou" and "ap-southeast-1", eg. "cn-hangzhou"
         */
        String regionId = "cn-hangzhou";
        String accessKeyId = "*** Provide your AccessKeyId ***";
        String accessKeySecret = "*** Provide your AccessKeySecret ***";
        kmsClient = kmsClient(regionId, accessKeyId, accessKeySecret);
        String keyId = null;
        String plainText = "hello world";
        String cipherBlob = null;
//        /*Create a Key*/
//        try {
//            final CreateKeyResponse response = CreateKey("testkey", "ENCRYPT/DECRYPT");
//
//            /**
//             * Parse response and do more further
//             */
//            System.out.println(response.getKeyMetadata());
//            CreateKeyResponse.KeyMetadata meta = response.getKeyMetadata();
//
```

```
//          System.out.println("CreateTime: " + meta.getCreationDate());
//          System.out.println("Description: " + meta.getDescription());
//          System.out.println("KeyId: " + meta.getKeyId());
//          keyId = meta.getKeyId();
//          System.out.println("KeyState: " + meta.getKeyState());
//          System.out.println("KeyUsage: " + meta.getKeyUsage());
//
//          System.out.println("==========================================");
//          System.out.println("Create MasterKey Success!") ;
//          System.out.println("==========================================\n");
//      } catch (ClientException eResponse) {
//          System.out.println("Failed.") ;
//          System.out.println("Error code: " + eResponse.getErrCode());
//          System.out.println("Error message: " + eResponse.getErrMsg());
//      }
//
        /*List all MasterKeys in your account*/
        try {
            final ListKeysResponse listKeysRes = ListKey(1, 100);
            /**
             * Parse response and do more further
             */
            System.out.println("TotalCount: " + listKeysRes.getTotalCount());
            System.out.println("PageNumber: " + listKeysRes.getPageNumber());
            System.out.println("PageSize: " + listKeysRes.getPageSize());
            List<Key> keys = listKeysRes.getKeys();
            Iterator<Key> iterator = keys.iterator();
            while (iterator.hasNext()) {
                keyId = iterator.next().getKeyId();
                System.out.println("KeyId: " + keyId);
            }
            System.out.println("==========================================");
            System.out.println("List All MasterKeys success! \n");
            System.out.println("==========================================\n");
        } catch (ClientException eResponse) {
            System.out.println("Failed.") ;
            System.out.println("Error code: " + eResponse.getErrCode());
            System.out.println("Error message: " + eResponse.getErrMsg());
        }
        /*Describe the Key */
        try {
            final DescribeKeyResponse decKeyRes = DescribeKey(keyId);
```

```
        /**
         * Parse response and do more further
         */
        System.out.println("DescribeKey Response: ");
        DescribeKeyResponse.KeyMetadata meta = decKeyRes.getKeyMetadata();
        System.out.println("KeyId: " + meta.getKeyId());
        System.out.println("Description: " + meta.getDescription());
        System.out.println("KeyState: " + meta.getKeyState());
        System.out.println("KeyUsage: " + meta.getKeyUsage());
        System.out.println("==========================================");
        System.out.println("Describe the MasterKey success!") ;
        System.out.println("==========================================\n");
    } catch (ClientException eResponse) {
        System.out.println("Failed.") ;
        System.out.println("Error code: " + eResponse.getErrCode());
        System.out.println("Error message: " + eResponse.getErrMsg());
    }
    /*Generate DataKey*/
    /**
     * Request and got response
     */
    try {
        final GenerateDataKeyResponse genDKResponse = GenerateDataKey(keyId, "AES_256", 64);
        /**
         * Parse response and do more further
         */
        System.out.println("CiphertextBlob: " + genDKResponse.getCiphertextBlob());
        System.out.println("KeyId: " + genDKResponse.getKeyId());
        System.out.println("Plaintext: " + genDKResponse.getPlaintext());
        System.out.println("==========================================");
        System.out.println("Generate DataKey success!") ;
        System.out.println("==========================================\n");
    } catch (ClientException eResponse) {
        System.out.println("Failed.") ;
        System.out.println("Error code: " + eResponse.getErrCode());
        System.out.println("Error message: " + eResponse.getErrMsg());
    }
    /**
     * Encrypt the plain text and got a cipher one
     */
    try {
```

```
            EncryptResponse encResponse = Encrypt(keyId, plainText);
            cipherBlob = encResponse.getCiphertextBlob();
            System.out.println("CiphertextBlob: " + cipherBlob);
            System.out.println("KeyId: " + encResponse.getKeyId());
            System.out.println("==========================================");
            System.out.println("Encrypt the plain text success!") ;
            System.out.println("==========================================\n");
        } catch (ClientException eResponse) {
            System.out.println("Failed.") ;
            System.out.println("Error code: " + eResponse.getErrCode());
            System.out.println("Error message: " + eResponse.getErrMsg());
        }
        /**
         * Decrypt the cipher text and verify result with original plain text.
         */
        try {
            DecryptResponse decResponse = Decrypt(cipherBlob);
            System.out.println("Plaintext: " + decResponse.getPlaintext());
            String verifyPlainText = decResponse.getPlaintext();
            int isMatch = verifyPlainText.compareTo(plainText);
            System.out.println("KeyId: " + decResponse.getKeyId());
            System.out.println("==========================================");
            System.out.printf("Decrypt the cipher text success, result " + (isMatch == 0 ? "match" : "mismatch"
+ "\n"));
            System.out.println("==========================================\n");
        } catch (ClientException eResponse) {
            System.out.println("Failed.") ;
            System.out.println("Error code: " + eResponse.getErrCode());
            System.out.println("Error message: " + eResponse.getErrMsg());
        }
    }
}
```

Access KMS in a VPC environment

You must add a custom endpoint directing to a domain name in the VPC. You must also specify to use this endpoint when accessing KMS later.

```
DefaultProfile.addEndpoint("cn-hangzhou-vpc", "cn-hangzhou-vpc", "Kms", "kms-vpc.cn-hangzhou.aliyun
cs.com"); //Add a custom endpoint.
```

2.18. Apsara Stack DNS

2.18.1. Overview

2.18.1.1. Calling methods

You can use a pair of AccessKey ID and AccessKey Secret to call API operations. You can use SDKs of different languages, or create a client based on the signature description provided by the POP gateway.

2.18.1.2. Supported formats

- AccessKey ID and AccessKey Secret of an Apsara Stack tenant account
- Temporary AccessKey ID and AccessKey Secret of an Apsara Stack tenant account
- AccessKey ID and AccessKey Secret of a RAM user account
- Temporary AccessKey ID and AccessKey Secret of a RAM user account

2.18.1.3. Instructions

- The AccessKey ID is used to identify users.
- The AccessKey Secret is used to compute the request signature.

2.18.1.4. Time format

Unless otherwise specified, the time string is a UTC+0 time in the format of YYYY-MM-DDTHH:mm:ssZ. For example, 2018-01-16T09:00:01Z indicates 17:00:01 on January 16, 2018, in China Standard Time (UTC+8).

2.18.2. List of operations by function

DNS V2.0 provides the following API operations.

API	Description
ObtainGlobalAuthZoneList	Obtains global authoritative zones
ObtainGlobalAuthRecordList	Obtains global authoritative RRSets
AddGlobalRrSet	Adds global RRSets
DeleteGlobalRrSet	Deletes global RRSets
UpdateGlobalRrSet	Updates global RRSets
RemarkGlobalRrSet	Configures descriptions for global RRSets

2.18.3. Prerequisites

2.18.3.1. Obtain an AccessKey pair

You can obtain an AccessKey pair in the Apsara Stack console.

Obtain an AccessKey pair of a department

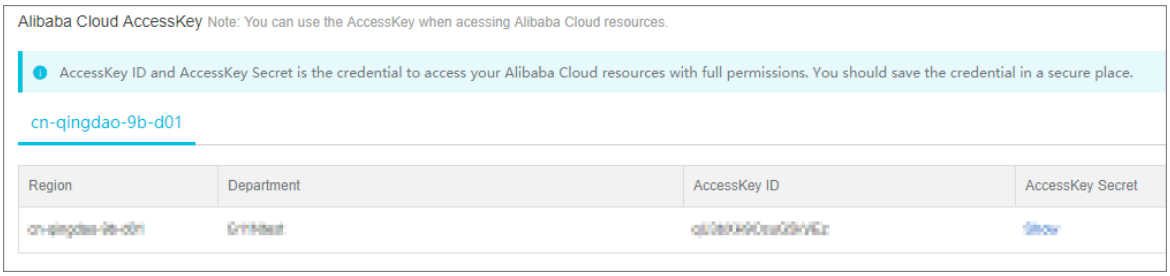
To obtain an AccessKey pair of a department, follow these steps:

1. Log on to the Apsara Stack console as an administrator.
2. In the top navigation bar, click and choose **User Center > Department Management**.
3. On the Department Management page that appears, select a department for which you want to obtain an AccessKey pair, and click **Get AccessKey**.

Obtain an AccessKey pair of a personal account

To obtain an AccessKey pair of a personal account, follow these steps:

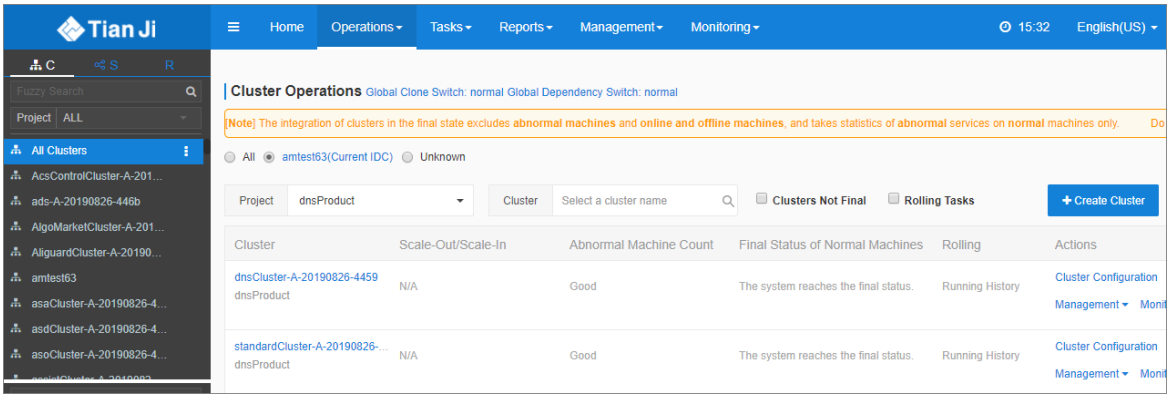
1. Log on to the Apsara Stack console as an administrator.
2. In the upper-right corner of the home page, move the pointer over the profile image and click **Personal Information**.
3. On the Personal Information page, locate the AccessKey ID in the **Alibaba Cloud AccessKey** section.



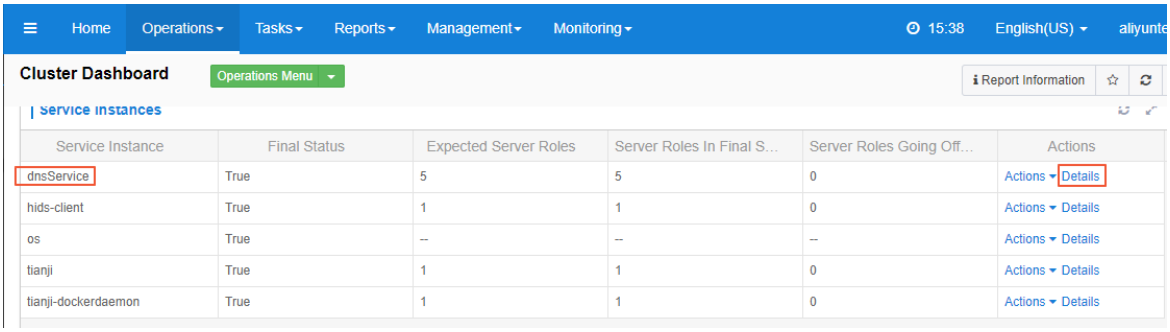
2.18.3.2. Obtain an endpoint

Procedure

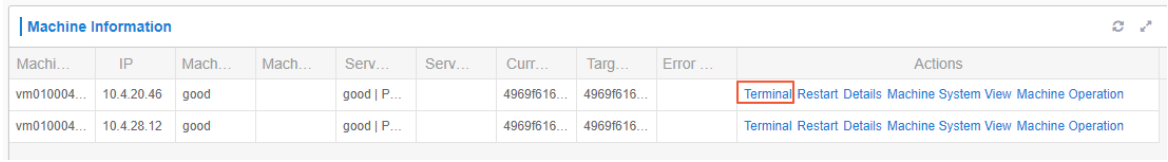
1. Log on to the Apsara Infrastructure Management Framework console as an administrator.
2. In the top navigation bar, choose Operations > Cluster Operations. On the Cluster Operations page, select **dnsProduct** from the Project drop-down list. Click a cluster name in the Cluster column to go to the Cluster Dashboard page.



3. In the Service Instances section, click **Details** in the Actions column of dnsService. The Service Instance Information Dashboard page opens. In the Server Role List section, click Details in the Actions column of dnsServerRole#.



4. On the Server Role Dashboard page, click **Terminal** in the Actions column of a machine to go to the console.



5. Run the `sudo docker ps -l` command to obtain the ID of the current container.
6. Run the `sudo docker inspect ${container id}|grep env` command to obtain the endpoint of the current environment. The endpoint is the value corresponding to pop_out_endpoint (the character string starting with "api.").

2.18.4. SDK example

2.18.4.1. Create a client

You need to specify a region ID, AccessKey ID, and AccessKey Secret to create a client.

Go SDK

```
1. if client, err := genesisdns.NewClientWithAccessKey(RegionId, AccessKey, AccessSecret); err == nil {
2.   //Write your code for processing normal requests.
3. } else {
4.   //Write your code for processing creation failures.
5. }
```

Python SDK

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException


client = AcsClient("<access-key-id>",
   "<access-key-secret>",
   "<region-id>");
```

Java SDK

```
public static void main(String[] args) {
    DefaultProfile profile = DefaultProfile.getProfile("{regionid}","{ak}", "{secret}");
    IAcsClient client = new DefaultAcsClient(profile);
}
```

2.18.4.2. Obtain global authoritative zones

Go SDK

```
if client, err := genesisdns.NewClientWithAccessKey("{regionid}","{ak}", "{secret}"); err == nil {
   request := genesisdns.CreateObtainGlobalAuthZoneListRequest()
   request.SetDomain("{endpoint}")
   if response, err := client.ObtainGlobalAuthZoneList(request); err == nil {
      fmt.Println(response.ZoneList)
   }
}
```

Python SDK

```
client = AcsClient("{ak}", "{secret}", "{regionid}");

request = ObtainGlobalAuthZoneListRequest.ObtainGlobalAuthZoneListRequest()
request.set_PageSize(10)
region_provider.modify_point("GenesisDns", "{regionid}","{endpoint}")
try:
    response = client.do_action_with_exception(request)
    print(response)
except ServerException as e:
    print(e)
except ClientException as e:
    print(e)
```

Java SDK

```
public static void main(String[] args) {
    DefaultProfile profile = DefaultProfile.getProfile("{regionid}","{ak}", "{secret}");
    IAcsClient client = new DefaultAcsClient(profile);
    ObtainGlobalAuthZoneListRequest request = new ObtainGlobalAuthZoneListRequest();
    try {
        request.setEndpoint("{endpoint}");
        request.setConnectTimeout(1000);
        request.setReadTimeout(1000);
        request.setPageSize(10);
        ObtainGlobalAuthZoneListResponse response = client.getAcsResponse(request);
        System.out.println(JSON.toJSONString(response.getZoneList()));
    } catch (Exception ex) {
        System.out.println(ex.getMessage());
    }
}
```

2.18.4.3. Obtain global authoritative RRSets

Go SDK

```
if client, err := genesisdns.NewClientWithAccessKey("{regionid}","{ak}", "{secret}")); err == nil {
    request := genesisdns.CreateObtainGlobalAuthRecordListRequest()
    request.SetDomain("{endpoint}")
    request.Id = requests.Integer("{zone id}")
    if response, err := client.ObtainGlobalAuthRecordList(request); err == nil {
        fmt.Println(response.Records)
    }
}
```

Python SDK

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.profile import region_provider
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkgenesisdns.request.v20180925 import ObtainGlobalAuthRecordListRequest

client = AcsClient("{ak}", "{secret}", "{regionid}")

request = ObtainGlobalAuthRecordListRequest.ObtainGlobalAuthRecordListRequest()
request.set_PageSize(10)
request.set_Id({zone id})
region_provider.modify_point("GenesisDns", "{regionid}", "{endpoint}")
try:
    response = client.do_action_with_exception(request)
    print(response)
except ServerException as e:
    print(e)
except ClientException as e:
    print(e)
```

Java SDK

```
1. public static void main(String[] args) {
2.     DefaultProfile profile = DefaultProfile.getProfile("{regionid}","{ak}", "{secret}");
3.     IAcsClient client = new DefaultAcsClient(profile);
4.     ObtainGlobalAuthRecordListRequest request = new ObtainGlobalAuthRecordListRequest();
5.     try {
6.         request.setEndpoint("{endpoint}");
7.         request.setConnectTimeout(1000);
8.         request.setReadTimeout(1000);
9.         request.setPageSize(10);
10.         request.setId(Long.parseLong("{zone id}"));
11.         ObtainGlobalAuthRecordListResponse response = client.getAcsResponse(request);
12.         System.out.println(JSON.toJSONString(response.getRecords()));
13.     } catch (Exception ex) {
14.         System.out.println(ex.getMessage());
15.     }
16. }
```

2.18.4.4. Add global RRSets

The following examples describe how a Resource Record Set (RRSet) is defined.

```
request.RrSet = "[\"2001:0:0:0:0:0:0:1\"]" //A RRSet with an AAAA record
request.RrSet = "[\"2001:0:0:0:0:0:0:1\", \"2001::2\"]" //A RRSet with two AAAA records
request.RrSet = "[\"2001:0:0:0:0:0:0:1 10\", \"2001::2 10\"]" //A RRSet with two weighted AAAA records
request.Type = "AAAA"

request.RrSet = "[\"www.aliyun.com. \"]" //A RRSet with a CNAME record
request.RrSet = "[\"www.aliyun.com. 10\",\"www.taobao.com 30\"]" //A RRSet with two weighted CNAME records
request.Type = "CNAME"

request.RrSet = "[\"10 mailserver1.example.com. \"]" //A RRSet with an MX record
request.Type = "MX"

request.RrSet = "[\"10 mailserver1.example.com.\",\"20 mailserver2.example.com. \"]" //A RRSet with two MX records
request.RrSet = "[\"v=spf1 ip4:192.168.0.1/16 ip6:2001::1/96 ~all\"]" //A RRSet with a TXT record
request.Type = "TXT"

request.RrSet = "[\"1 10 8080 www1.example.com.\", \"2 20 8081 www2.example.com. \"]" //A RRSet with two SRV records
request.Type = "SRV"

request.RrSet = "[\"100 50 \\\"S\\\" \\\"Z3950+I2L+I2C\\\" \\\"\\\" _z3950._tcp.example.com. \"]" //A RRSet with a NAPTR record
request.Type = "NAPTR"

request.RrSet = "[\"0 issue \\\"caa.example.com\\\"\",\"0 issuewild \\\";\\\"\"]" //A RRSet with a CAA record
request.Type = "CAA"

request.RrSet = "[\"inner-ns1.example01.com. hostmaster.example01.com. 1 7200 900 1209600 86400\"]" //A RRSet with an SOA record
request.Type = "SOA"

request.RrSet = "[\"ns1.example.com.\",\"ns2.example.com. \"]" //A RRSet with two NS records
request.Type = "NS"
```

Go SDK

```
1. func main()  {
2.    if client, err := genesisdns.NewClientWithAccessKey("{regionid}","{ak}", "{secret}"); err == nil {
3.       request := genesisdns.CreateAddGlobalRrSetRequest()
4.       request.SetDomain("{endpoint}")
5.       request.ZoneId = requests.Integer("{zone id}")
6.       request.Ttl = requests.Integer("300")
7.       request.Type = "A"
8.       request.RrSet = "[\"1.1.1.1\"]"
9.       request.Rr = "sdka"
10.
11.       if response, err := client.AddGlobalRrSet(request); err == nil {
12.          fmt.Println(response.RequestId, response.Id)
13.       }
14.    }
15. }
```

Python SDK

```
1. from aliyunsdkcore.client import AcsClient
2. from aliyunsdkcore.profile import region_provider
3. from aliyunsdkcore.acs_exception.exceptions import ClientException
4. from aliyunsdkcore.acs_exception.exceptions import ServerException
5. from aliyunsdkgenesisdns.request.v20180925 import AddGlobalRrSetRequest
6.
7. client = AcsClient("{ak}", "{secret}", "{regionid}")
8.
9. request = AddGlobalRrSetRequest.AddGlobalRrSetRequest()
10. request.set_ZoneId(93)
11. request.set_Rr("sdk_python_a")
12. request.set_RrSet("[\"3.3.3.3\"]")
13. request.set_Ttl(300)
14. request.set_Type("A")
15.
16. region_provider.modify_point("GenesisDns", "{regionid}", "{endpoint}")
17. try:
18.     response = client.do_action_with_exception(request)
19.     print(response)
20. except ServerException as e:
21.     print(e)
22. except ClientException as e:
23.     print(e)
```

Java SDK

```
1. public static void main(String[] args) {
2.     DefaultProfile profile = DefaultProfile.getProfile("{regionid}","{ak}", "{secret}");
3.     IAcsClient client = new DefaultAcsClient(profile);
4.     AddGlobalRrSetRequest request = new AddGlobalRrSetRequest();
5.     try {
6.         request.setEndpoint("{endpoint}");
7.         request.setConnectTimeout(1000);
8.         request.setReadTimeout(1000);
9.         request.setZoneId(Long.parseLong("93"));
10.         request.setRr("sdk_java_a");
11.         request.setTtl(300);
12.         request.setType("A");
13.         request.setRrSet("[\"1.1.1.1\", \"2.2.2.2\"]");
14.         AddGlobalRrSetResponse response = client.getAcsResponse(request);
15.         System.out.println(JSON.toJSONString(response));
16.     } catch (Exception ex) {
17.         System.out.println(ex.getMessage());
18.     }
19. }
```

2.18.4.5. Delete global RRSets

Go SDK

```
package main

import (
    "fmt"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "github.com/aliyun/alibaba-cloud-sdk-go/services/genesisdns"
)

func main()  {
    if client, err := genesisdns.NewClientWithAccessKey("{regionid}","{ak}", "{secret}"); err == nil {
        request := genesisdns.CreateDeleteGlobalRrSetRequest()
        request.SetDomain("{endpoint}")
        request.Id = requests.Integer("{rrSet id")

        if response, err := client.DeleteGlobalRrSet(request); err == nil {
            fmt.Println(response.RequestId)
        }
    }
}
```

Python SDK

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.profile import region_provider
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkgenesisdns.request.v20180925 import DeleteGlobalRrSetRequest

client = AcsClient("{ak}", "{secret}", "{regionid}")

request = DeleteGlobalRrSetRequest.DeleteGlobalRrSetRequest()
 request.set_Id(170)

 region_provider.modify_point("GenesisDns", "{regionid}", "{endpoint}")
 try:
     response = client.do_action_with_exception(request)
     print(response)
 except ServerException as e:
     print(e)
 except ClientException as e:
     print(e)
```

Java SDK

```
public static void main(String[] args) {
    DefaultProfile profile = DefaultProfile.getProfile("{regionid}","{ak}", "{secret}");
    IAcsClient client = new DefaultAcsClient(profile);
    DeleteGlobalRrSetRequest request = new DeleteGlobalRrSetRequest();
    try {
        request.setEndpoint("{endpoint}");
        request.setConnectTimeout(1000);
        request.setReadTimeout(1000);
        request.setId(Long.parseLong("{RrSet id}"));
         DeleteGlobalRrSetResponse response = client.getAcsResponse(request);
         System.out.println(JSON.toJSONString(response));
    } catch (Exception ex) {
         System.out.println(ex.getMessage());
    }
```

2.18.4.6. Update global RRSets

Go SDK

```
package main

import (
    "fmt"
    "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
    "github.com/aliyun/alibaba-cloud-sdk-go/services/genesisdns"
)

func main()  {
    if client, err := genesisdns.NewClientWithAccessKey("{regionid}","{ak}", "{secret}"); err == nil {
        request := genesisdns.CreateUpdateGlobalRrSetRequest()
        request.SetDomain("{endpoint}")
        request.RrsetId = requests.Integer("{RrSet id}")
        request.Rr = "go_sdk_a"
        request.RrSet = "[\"8.8.8.8\"]"
        request.Ttl = requests.Integer("300")
        request.Type = "A"


        if response, err := client.UpdateGlobalRrSet(request); err == nil {
            fmt.Println(response.RequestId)
        }
    }
}
```

Python SDK

```
from aliyunsdkcore.client import AcsClient
from aliyunsdkcore.profile import region_provider
from aliyunsdkcore.acs_exception.exceptions import ClientException
from aliyunsdkcore.acs_exception.exceptions import ServerException
from aliyunsdkgenesisdns.request.v20180925 import UpdateGlobalRrSetRequest

client = AcsClient("{ak}", "{secret}", "{regionid}")

request = UpdateGlobalRrSetRequest.UpdateGlobalRrSetRequest()
 request.set_RrsetId(165)
 request.set_Type("A")
 request.set_Rr("sdk_python_a")
 request.set_RrSet("[\"3.3.3.3\"]")
 request.set_Ttl(300)

 region_provider.modify_point("GenesisDns", "{regionid}", "{endpoint}")
 try:
     response = client.do_action_with_exception(request)
     print(response)
 except ServerException as e:
     print(e)
 except ClientException as e:
     print(e)
```

Java SDK

```
public static void main(String[] args) {
    DefaultProfile profile = DefaultProfile.getProfile("{regionid}","{ak}", "{secret}");
    IAcsClient client = new DefaultAcsClient(profile);
    UpdateGlobalRrSetRequest request = new UpdateGlobalRrSetRequest();
    try {
        request.setEndpoint("{endpoint}");
        request.setConnectTimeout(1000);
        request.setReadTimeout(1000);
        request.setRrsetId(Long.parseLong("165"));
        request.setRr("sdk_java_a");
        request.setRrSet("[\"4.4.4.4\"]");
        request.setTtl(300);
        request.setType("A");

        UpdateGlobalRrSetResponse response = client.getAcsResponse(request);
        System.out.println(JSON.toJSONString(response));
    } catch (Exception ex) {
        System.out.println(ex.getMessage());
    }
}
```

2.18.4.7. Configure descriptions for global RRSets

Go SDK

```
1. package main
2.
3. import (
4.     "fmt"
5.     "github.com/aliyun/alibaba-cloud-sdk-go/sdk/requests"
6.     "github.com/aliyun/alibaba-cloud-sdk-go/services/genesisdns"
7. )
8.
9. func main()  {
10.     if client, err := genesisdns.NewClientWithAccessKey(""{regionid}","{ak}", "{secret}"); err == nil {
11.         request := genesisdns.CreateRemarkGlobalRrSetRequest()
12.         request.SetDomain("{endpoint}")
13.         request.Id = requests.Integer("165")
14.         request.Remark = "go remark"
15.
16.
17.         if response, err := client.RemarkGlobalRrSet(request); err == nil {
18.             fmt.Println(response.RequestId)
19.         }
20.     }
21. }
```

Python SDK

```
1. from aliyunsdkcore.client import AcsClient
2. from aliyunsdkcore.profile import region_provider
3. from aliyunsdkcore.acs_exception.exceptions import ClientException
4. from aliyunsdkcore.acs_exception.exceptions import ServerException
5. from aliyunsdkgenesisdns.request.v20180925 import RemarkGlobalRrSetRequest
6.
7. client = AcsClient("{ak}", "{secret}", "{regionid}")
8.
9. request = RemarkGlobalRrSetRequest.RemarkGlobalRrSetRequest()
10. request.set_Id(165)
11. request.set_Remark("test remark python")
12. region_provider.modify_point("GenesisDns", "{regionid}", "{endpoint}")
13. try:
14.     response = client.do_action_with_exception(request)
15.     print(response)
16. except ServerException as e:
17.     print(e)
18. except ClientException as e:
19.     print(e)
```

Java SDK

```
1. public static void main(String[] args) {
2.     DefaultProfile profile = DefaultProfile.getProfile("{regionid}","{ak}", "{secret}");
3.     IAcsClient client = new DefaultAcsClient(profile);
4.     RemarkGlobalRrSetRequest request = new RemarkGlobalRrSetRequest();
5.     try {
6.         request.setEndpoint("{endpoint}");
7.         request.setConnectTimeout(1000);
8.         request.setReadTimeout(1000);
9.         request.setId(Long.parseLong("165"));
10.         request.setRemark("test java remark");
11.
12.         RemarkGlobalRrSetResponse response = client.getAcsResponse(request);
13.         System.out.println(JSON.toJSONString(response));
14.     } catch (Exception ex) {
15.         System.out.println(ex.getMessage());
16.     }
17. }
```