

Alibaba Cloud

Apsara Stack Enterprise

Apsara Stack Security Developer Guide

Product Version: v3.16.2

Document Version: 20220913

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 .
<code>Courier font</code>	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Preparations	16
1.1. Log on to the API Tool console	16
1.2. View the information about an operation	17
1.3. Obtain an AccessKey pair	17
1.4. Obtain an AccessKey pair assigned by STS	19
1.5. Obtain an endpoint	23
2.Call examples	25
2.1. Call examples for SDK for Java	25
2.1.1. Quick start	25
2.1.2. Use SDK	26
2.1.2.1. Install SDK for Java	26
2.1.2.2. Use CommonRequest to call API operations	27
2.2. Call examples for SDK for Python	28
2.2.1. Quick start	28
2.2.2. Use SDK	30
2.2.2.1. Install SDK for Python	30
2.2.2.2. Use CommonRequest to call API operations	30
2.3. Call examples for SDK for Go	32
2.3.1. Quick start	32
2.3.2. Use SDK	33
2.3.2.1. Install Go SDK	33
2.3.2.2. Use CommonRequest to call API operations	33
3.Common parameters	36
4.Server Guard	38
4.1. Asset management	38
4.1.1. DescribeGroupSummary	38

4.1.2. DescribeGroupStruct	39
4.1.3. DescribeAllEntity	41
4.1.4. DescribeEntityList	43
4.1.5. DescribeMachines	46
4.1.6. DescribeMachineDetail	48
4.1.7. DescribePropertyStatistic	50
4.1.8. DescribePropertyPortItem	51
4.1.9. DescribePropertyPortDetail	53
4.1.10. DescribePropertyProcItem	55
4.1.11. DescribePropertyProcDetail	57
4.1.12. DescribePropertySoftwareItem	60
4.1.13. DescribePropertySoftwareDetail	62
4.1.14. DescribePropertyUserItem	64
4.1.15. DescribePropertyUserDetail	66
4.1.16. DescribeTopRiskyAssets	68
4.2. Vulnerability management	70
4.2.1. DescribeTarget	70
4.2.2. DescribeVulTargetStatistics	71
4.2.3. DescribeTargetConfig	73
4.2.4. DescribeVulConfig	74
4.2.5. DescribeAutoDelConfig	75
4.2.6. DescribeVulLevel	76
4.2.7. DescribeVulWhitelist	77
4.2.8. DescribeGroupedVul	79
4.2.9. DescribeVulList	83
4.2.10. DescribeVulDetails	88
4.2.11. DescribeVulNumStatistics	90
4.2.12. DescribeVulLevelStatistics	92

4.2.13. DescribeVulMachineList	94
4.3. Baseline check	96
4.3.1. DescribeStratetyDetail	96
4.3.2. DescribeStrategyTarget	99
4.3.3. DescribeUuidConfig	101
4.3.4. DescribeUserSetting	102
4.3.5. DescribeRiskWhiteList	103
4.3.6. DescribeStratety	104
4.3.7. DescribeStrategyExecDetail	106
4.3.8. DescribeRiskType	108
4.3.9. Describsummary	110
4.4. Unusual logon detection	113
4.4.1. DescribeBaseConfigs	113
4.4.2. DescribeSwitchConfigs	115
4.4.3. DescribeConfigTarget	117
4.5. Webshell detection	119
4.5.1. DescribeCategoryCount	119
4.5.2. DescribeWebshell	120
4.5.3. DescribeQuaraFile	122
4.6. Exception detection on hosts	124
4.6.1. DescribeSuspEventTypes	124
4.6.2. DescribeSuspTrendStatistics	125
4.6.3. DescribeSuspiciousExportInfo	126
4.7. Retrieval of host logs	128
4.7.1. DescribeFilterFields	128
4.7.2. DescribeHistogram	129
4.7.3. DescribeLogInfo	131
4.7.4. DescribeLogItems	133

5.Sensitive Data Discovery and Protection	137
5.1. APIs	137
5.1.1. DescribeDataAssets	137
5.1.2. DescribeInstances	139
5.1.3. DescribeTables	141
5.1.4. DescribePackages	143
5.1.5. DescribeColumns	145
5.1.6. DescribeOssObjects	147
5.1.7. DescribeOssObjectDetail	149
5.1.8. DescribeDeparts	150
5.1.9. DescribeAccounts	152
5.1.10. DescribeAccountDetail	154
5.1.11. DescribePrivileges	156
5.1.12. DescribeEventTypes	159
5.1.13. DescribeEvents	161
5.1.14. DescribeEventDetail	164
5.1.15. ModifyEventStatus	167
5.1.16. ModifyEventTypeStatus	168
5.1.17. ModifyDefaultLevel	169
5.1.18. DescribeRules	170
5.1.19. CreateRule	172
5.1.20. ModifyRule	173
5.1.21. ModifyRuleStatus	174
5.1.22. DeleteRule	175
5.1.23. DescribeDataLimitSet	176
5.1.24. CreateDataLimit	178
5.1.25. DeleteDataLimit	179
6.Container Protection	181

6.1. DescribeImageInfoList	181
6.2. DescribeImageBaselineCheckSummary	184
6.3. DescribeImageBaselineItemList	188
6.4. DescribeImageListWithBaselineName	191
6.5. DescribeCycleTaskList	196
6.6. DescribeContainerCriteria	199
6.7. DescribeContainerFieldStatistics	201
6.8. DescribeContainerGroupedFieldDetail	203
6.9. DescribeContainerInstances	207
6.10. DescribeGroupedContainerInstances	213
6.11. DescribeImageCriteria	219
6.12. DescribeImageInstances	220
6.13. DescribeImageSecurityScanCount	225
6.14. GetRegistryScanDayNum	227
6.15. ListPrivateRegistryList	229
6.16. ListPrivateRegistryType	231
6.17. DescribeAlarmEventDetail	232
6.18. DescribeNsasSuspEventType	238
6.19. DescribeSecurityEventOperations	240
6.20. DescribeSuspEvents	243
6.21. DescribeEventLevelCount	256
6.22. DescribeConcernNecessity	257
6.23. DescribeGroupedVul	258
6.24. DescribeImageGroupedVulList	264
6.25. DescribeImageVulList	268
6.26. DescribeVulDetails	275
6.27. DescribeAllGroups	281
6.28. DescribeAssetDetailByUuid	283

7.Threat Detection Service (TDS)	289
7.1. Asset management	289
7.1.1. DescribeFieldStatistics	289
7.1.2. DescribeGroupedTags	291
7.1.3. DescribeAllGroups	293
7.1.4. DescribeInstanceStatistics	295
7.1.5. DescribeCloudProductFieldStatistics	298
7.1.6. DescribeCloudCenterInstances	300
7.1.7. DescribeSummaryInfo	307
7.2. Secure score	309
7.2.1. DescribeSecureSuggestion	309
7.3. Security alerts	314
7.3.1. DescribeAlarmEventList	314
7.3.2. DescribeAlarmEventDetail	321
7.3.3. DescribeSuspEvents	328
7.3.4. DescribeSuspEventDetail	333
7.4. Configuration assessment	339
7.4.1. DescribeRiskItemType	339
7.4.2. StartBaselineSecurityCheck	341
7.4.3. DescribeRiskCheckSummary	343
7.4.4. DescribeRiskCheckResult	348
7.4.5. DescribeSecurityCheckScheduleConfig	366
7.5. Vulnerability management	368
7.5.1. DescribeVulList	368
7.5.2. DescribeVulWhitelist	378
7.5.3. DescribeConcernNecessity	380
7.5.4. DescribeGroupedVul	381
7.5.5. DescribeAutoDelConfig	386

7.6. Baseline check	387
7.6.1. DescribeCheckWarningSummary	387
7.6.2. DescribeStrategy	400
7.6.3. DescribeStrategyExecDetail	405
7.6.4. DescribeCheckWarnings	407
7.6.5. DescribeCheckWarningDetail	416
7.6.6. DescribeWarningMachines	418
7.7. Asset fingerprints	422
7.7.1. DescribePropertyCount	422
7.7.2. DescribePropertyPortDetail	424
7.7.3. DescribePropertyProcDetail	429
7.7.4. DescribePropertyPortItem	434
7.7.5. DescribePropertyProcItem	437
7.7.6. DescribePropertySoftwareDetail	440
7.7.7. DescribePropertySoftwareItem	443
7.7.8. DescribePropertyUserDetail	446
7.7.9. DescribePropertyUserItem	450
7.8. Asset exposure	453
7.8.1. DescribeExposedInstanceList	453
8. Network Traffic Monitoring System	458
8.1. IP address blocking	458
8.1.1. AddToBlackList	458
8.1.2. AddToWhiteList	460
8.1.3. DelFromBlackList	462
8.1.4. DelFromWhiteList	464
8.1.5. DescribeBlackList	466
8.1.6. DescribeWhiteList	469
8.2. Application-layer rules	473

8.2.1. DescribeL7Rule	473
8.2.2. SwitchL7RuleStatus	480
8.2.3. AddL7Rule	482
8.2.4. DelL7Rule	484
9.Web Application Firewall	487
9.1. Website protection	487
9.1.1. DescribeWebsite	487
9.1.2. CreateWebsite	490
9.1.3. EditWebsite	501
9.1.4. ToggleWebsite	513
9.1.5. QueryAsyncTaskStatus	515
9.1.6. UploadResponsePage	517
9.1.7. DescribeInvalidWebsite	518
9.1.8. DeleteInvalidWebsite	521
9.1.9. DescribeInternetVip	523
9.1.10. CreateInternetVip	524
9.1.11. DeleteInternetVip	525
9.1.12. DescribeVpc	526
9.1.13. DescribeVSwitch	528
9.1.14. DescribeVpcVip	529
9.1.15. CreateVpcVip	530
9.1.16. DeleteVpcVip	532
9.1.17. DescribeEcs	533
9.1.18. DescribeSlb	535
9.2. HTTP flood protection rules	536
9.2.1. DescribeCCRuleTemplate	537
9.2.2. CreateCCRuleTemplate	539
9.2.3. EditCCRuleTemplate	544

9.2.4. ToggleCCRuleTemplate	550
9.2.5. DeleteCCRuleTemplate	552
9.2.6. ClearCCRestrictionList	554
9.2.7. DescribeCCWhitelist	556
9.2.8. CreateCCWhitelist	558
9.2.9. DeleteCCWhitelist	560
9.3. Custom rules	562
9.3.1. DescribePolicyRule	562
9.3.2. CreatePolicyRule	565
9.3.3. EditPolicyRule	573
9.3.4. TogglePolicyRule	579
9.3.5. DeletePolicyRule	581
9.3.6. EditPolicyRulePriority	583
9.3.7. GenerateFalsePositiveRuleCorrection	585
9.3.8. CreateDetectionModuleRule	588
9.3.9. EditDetectionModuleRule	593
9.3.10. EditPolicyRuleWebsiteBinding	598
9.3.11. DeletePolicyRuleWebsiteBinding	601
9.4. Protection policies	603
9.4.1. DescribePolicyGroup	603
9.4.2. CreatePolicyGroup	608
9.4.3. EditPolicyGroup	613
9.4.4. DeletePolicyGroup	623
9.5. Protection logs	624
9.5.1. QueryAsyncTaskStatus	624
9.5.2. QueryAttackDetectionLog	626
9.5.3. QueryAttackDetectionDetailLog	632
9.5.4. QueryAuditLog	634

9.5.5. QueryCCRuleExecutionLog	636
9.5.6. QueryFullAccessLog	638
9.5.7. QueryFullAccessDetailLog	641
9.5.8. QueryPerformanceStatistics	643
9.6. SSL certificate management	645
9.6.1. DescribeSSLCert	645
9.6.2. UploadSSLCert	646
9.6.3. EditSSLCert	648
9.6.4. DeleteSSLCert	650
9.7. System information	651
9.7.1. DescribeMetrics	651
9.7.2. DescribeNodeStatus	653
9.7.3. DescribeRealTimeAccess	659
9.7.4. DescribeAttackDetectionAggregationConfig	661
9.7.5. ToggleAttackDetectionAggregation	662
10. Security Operations Center	664
10.1. Operations	664
10.1.1. DescribeAttacks	664
10.1.2. DescribeAlarms	666
10.1.3. DescribeVulFrangs	669
10.1.4. DescribeHcFrangs	672
10.2. SOAR	675
10.2.1. Playbooks	675
10.2.1.1. ModifyPlaybook	675
10.2.1.2. TriggerPlaybook	677
10.2.1.3. PublishPlaybook	678
10.2.1.4. StopOneAction	680
10.2.1.5. DescribePlaybook	681

10.2.1.6. DescribeSoarRecords	686
10.2.2. Intelligence	691
10.2.2.1. SyncBanRecord	691
10.2.3. Cases	693
10.2.3.1. CreateEventByAlert	693
10.2.4. Tasks	696
10.2.4.1. DescribeManualTaskInfo	696
10.3. Operations Center	700
10.3.1. QueryThreats	700
10.3.2. QueryThreatChartData	704
11.Security Audit	708
11.1. APIs	708
11.1.1. CreateEventType	708
11.1.2. DescribeEventType	709
11.1.3. DeleteEventType	711
11.1.4. CreateLogFilter	712
11.1.5. DescribeLogFilter	715
11.1.6. DeleteLogFilter	717
11.1.7. CreateReceiver	718
11.1.8. DescribeReceiver	720
11.1.9. DeleteReceiver	722
11.1.10. CreateRule	723
11.1.11. DescribeRule	725
11.1.12. EnableRule	728
11.1.13. DisableRule	729
11.1.14. DeleteRule	730
11.1.15. CreateTask	730
11.1.16. DescribeTask	732

11.1.17. DeleteTask	734
11.1.18. DescribeSetting	735
11.1.19. ModifySetting	736
11.1.20. DescribeLogType	737
11.1.21. DescribeLogSource	738
11.1.22. DescribeLogCountStat	739
11.1.23. DescribeLog	741
11.1.24. DescribeEventRisk	744
11.1.25. DescribeEventRiskStat	744
11.1.26. DescribeEventTypeStat	746
11.1.27. DescribeEventCountStat	747
11.1.28. DescribeEvent	749
11.1.29. DescribeArchiveCountStat	753
11.1.30. DescribeArchive	755
12. Error codes	758

1. Preparations

1.1. Log on to the API Tool console

You can log on to the API Tool console from the Apsara Uni-manager Management Console.

Prerequisites

- Before you log on to the Apsara Uni-manager Management Console, the endpoint of the console is obtained from the deployment personnel.
- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Enter the URL of the Apsara Uni-manager Management Console in the address bar and press Enter.
2. Enter your username and password.

Obtain the username and password that are used to log on to the Apsara Uni-manager Management Console from the operations administrator.

 **Note** When you log on to the Apsara Uni-manager Management Console for the first time, you must change the password of your account. For security purposes, your password must meet the minimum complexity requirements. The password must be 10 to 32 characters in length and must contain at least two of the following character types:

- Uppercase or lowercase letters
- Digits
- Special characters, which include ! @ # \$ %

3. Click **Log On**.
4. If your account has multi-factor authentication (MFA) enabled, perform corresponding operations in the following scenarios:
 - You log on to the Apsara Uni-manager Management Console for the first time after MFA is enabled by the administrator.
 - a. On the Bind Virtual MFA Device page, bind an MFA device.
 - b. Enter the username and password again as in Step 2 and click **Log On**.
 - c. Enter a six-digit MFA verification code and click **Authenticate**.
 - You have enabled MFA and bound an MFA device.

Enter a six-digit MFA verification code and click **Authenticate**.

 **Note** For more information, see the *Bind a virtual MFA device to enable MFA* topic in *Apsara Uni-manager Management Console User Guide*.

5. In the top navigation bar, choose **Products > Others > API Tool**.

1.2. View the information about an operation

When you use a service SDK to call an operation of the service, you must obtain the service name, operation name, and API version. This topic describes how to view the information about an operation.

Context

The operations on the API Directory page are for reference only. For information about how to call operations, see API references of the corresponding services. If the information on the API Directory page is inconsistent with that in the API reference of the corresponding service, the information in the API reference takes precedence.

Procedure

1. [Log on to the API Tool console.](#)
2. In the left-side navigation pane, click **API Directory**.
3. On the **API Directory** page, select the required service from the drop-down list, enter a keyword of an operation name in the search box, and then click Search.
4. View and record the service name, operation name, and API version.

1.3. Obtain an AccessKey pair

AccessKey pairs are classified into AccessKey pairs assigned by Resource Access Management (RAM) and AccessKey pairs assigned by Security Token Service (STS). You can use either type of AccessKey pair for authentication when you call operations. This topic describes how to obtain an AccessKey pair that is assigned by RAM.

Context

An AccessKey pair is used to verify the identity of request senders. An AccessKey pair consists of an AccessKey ID and an AccessKey secret that are used to implement symmetric encryption. The AccessKey ID is used to identify a user. The AccessKey secret is used to encrypt the signature string.

You can use RAM or STS to assign an AccessKey pair for authentication.

- Use RAM to assign an AccessKey ID and an AccessKey secret to a third party.
- Use STS to assign an AccessKey ID, an AccessKey secret, and a security token to a third party. For more information, see [Obtain an STS AccessKey pair](#).

The Apsara Uni-manager Management Console provides AccessKey pairs for personal accounts or organizations. Only the administrators of level-1 organizations and operations administrators can obtain the AccessKey pairs of organizations. We recommend that you use the AccessKey pairs of personal accounts to call the operations provided by the Apsara Uni-manager Management Console and cloud services. If you use the AccessKey pair of a personal account, you must add the following parameters in request headers for access control. If you do not add the parameters, an error may occur. The error indicates that permissions are insufficient.

 **Warning** The AccessKey pair of a personal account is managed by the permission system of the Apsara Uni-manager Management Console. The AccessKey pair of an organization has more permissions than the AccessKey pair of a personal account. If you want to obtain the AccessKey pair of an organization, make sure that you are authorized by an administrator. This helps ensure security.

Parameter	Description
x-acs-regionid	The ID of the region. Example: cn-hangzhou-*
x-acs-organizationid	The ID of the organization in the Apsara Uni-manager Management Console. For more information about how to obtain organization IDs, see the <i>GetOrganizationList</i> section in <i>Apsara Uni-manager Management Console Developer Guide</i> .
x-acs-resourcegroupid	The ID of the resource set in the Apsara Uni-manager Management Console. For more information about how to obtain resource set IDs, see the <i>ListResourceGroup</i> section in <i>Apsara Uni-manager Management Console Developer Guide</i> .
x-acs-instanceid	The ID of the instance on which you want to perform operations. For example, you can obtain the ID of an Elastic Compute Service (ECS) instance from the ECS instance list.

Obtain the AccessKey pair of a personal account

To obtain the AccessKey pair of a personal account, perform the following operations:

1. Log on to the Apsara Uni-manager Management Console.
2. In the upper-right corner of the homepage, move the pointer over the profile picture and click **User Information**.
3. In the **AccessKey Pair** section, view the AccessKey pair of your account.

AccessKey Create AccessKey Pair					
 The AccessKey ID and AccessKey Secret are the keys used to access the cloud service resources. They have full permissions on the account. Please keep them properly. ×					
AccessKey ID	AccessKey Secret	Status	Created At	Actions	
W1YRFvKH...		 Enable	Sep 18, 2021, 11:05:57	Disable	Delete
IsJsAUyX...		 Enable	Sep 10, 2021, 12:28:35	Disable	Delete

 **Note** An AccessKey pair consists of an AccessKey ID and an AccessKey secret. These credentials provide full permissions on cloud resources within your account. You must keep the AccessKey pair confidential.

Obtain the AccessKey pair of an organization

To obtain the AccessKey pair of an organization, perform the following operations:

1. Log on to the Apsara Uni-manager Management Console as an administrator.
2. In the top navigation bar, click **Enterprise**.
3. In the left-side navigation pane, choose **Resources > Organizations**.
4. In the organization list, click the name of the level-1 organization whose AccessKey pair you want to obtain.
5. Click **Management Accesskey**.
6. In the dialog box that appears, view the AccessKey pair of the organization.

1.4. Obtain an AccessKey pair assigned by STS

This topic describes how to use Security Token Service (STS) to make API calls.

Background information

Alibaba Cloud STS allows you to manage temporary credentials to your Alibaba Cloud resources. You can use STS to make API calls.

An AccessKey pair assigned by STS consists of an AccessKey ID, an AccessKey secret, and a security token. When you use STS to make API calls, you must use an AccessKey pair assigned by STS. For more information about STS, see [What is STS?](#)

Procedure

1. Obtain your `RAM role`.
 - i. Log on to the Apsara Uni-manager Management Console.
 - ii. Click the profile picture in the upper-right corner of the page and click **User Information**.
 - iii. Click **View Current Role Policy**.

In the **View Policies of Current Role** dialog box, view your `RAM role`.

2. Obtain the AccessKey pair assigned by STS.

 Note

You must use the actual values to replace the variables in the following sample code. The angle brackets <> are not retained in the final code.

The following list describes the variables:

- <yourRegionID>: Replace it with the actual region ID.
- <yourAccessKeyID>: Replace it with your AccessKey ID.
- <yourAccessKeySecret>: Replace it with your AccessKey secret.
- <yourRoleSessionName>: Replace it with your current session name.
- <yourRoleArn>: Replace it with the Alibaba Cloud Resource Name (ARN) of your RAM role.
- "sts.aliyuns.com": Replace it with the endpoint of STS.


```

public static void main(String[] args) {
    // Create a DefaultAcsClient instance and initialize it.
    Replace <yourRegionID>, <yourAccessKeyID>, and <yourAccessKeySecret> with the actual region ID, your AccessKey ID, and your AccessKey secret.
    DefaultProfile profile = DefaultProfile.getProfile("<yourRegionID>", "<yourAccessKeyID>", "<yourAccessKeySecret>");
    HttpClientConfig clientConfig = HttpClientConfig.getDefault();
    clientConfig.setIgnoreSSLCerts(true);
    clientConfig.setProtocolType(ProtocolType.HTTPS);
    profile.setHttpClientConfig(clientConfig);
    IAcsClient client = new DefaultAcsClient(profile);
    String assumeRole = callAssumeRole(client);
    if (StringUtils.isEmpty(assumeRole)) return;
    JSONObject assumeRoleJson = JSONObject.parseObject(assumeRole);
    JSONObject credentials = assumeRoleJson.getJSONObject("Credentials");
    // Obtain the AccessKey pair assigned by STS.
    String stsAK = credentials.getString("AccessKeyId");
    String stsSK = credentials.getString("AccessKeySecret");
    String stsToken = credentials.getString("SecurityToken");
}

private static String callAssumeRole(IAcsClient client) {
    CommonRequest request = new CommonRequest();
    // Replace "sts.aliyuns.com" with the endpoint of STS. The format of an STS endpoint is sts-vpc.${global:region}.${global:internet-domain}.
    request.setSysDomain("sts.aliyuns.com");
    request.setSysProduct("Sts");
    request.setSysAction("AssumeRole");
    request.setSysVersion("2015-04-01");
    request.setSysMethod(MethodType.POST);
    request.setHttpContentType(FormatType.FORM);
    // The business parameter. Specify an alias for the current session. Replace "<yourRoleSessionName>" with the actual session name.
    request.putQueryParameter("RoleSessionName", "<yourRoleSessionName>");
    // The ARN of your RAM role. Replace "<yourRoleArn>" with the ARN of your RAM role that is obtained in the previous step.
    request.putQueryParameter("RoleArn", "<yourRoleArn>");
    try {
        CommonResponse response = client.getCommonResponse(request);
        return response.getData();
    } catch (ServerException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    } catch (ClientException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    }
    return null;
}

```

3. Use the AccessKey pair assigned by STS to call an operation of a service. The following sample code provides an example on how to use the AccessKey pair assigned by STS to call the

`DescribeZones` operation of Elastic Compute Service (ECS):

 Note

You must use the actual values to replace the variables in the following sample code. The angle brackets <> are not retained in the final code.

The following list describes the variables:

- <yourRegionID>: Replace it with the actual region ID.
- <yourAccessKeyID>: Replace it with your AccessKey ID.
- <yourAccessKeySecret>: Replace it with your AccessKey secret.
- <yourStsToken>: Replace it with the security token of the AccessKey pair assigned by STS.
- <yourRegionID>: Replace it with the actual resource set ID.
- <yourRegionID>: Replace it with the actual organization ID.

```

public static void main(String[] args) {
    // Replace "<yourRegionID>" with the actual region ID.
    // Replace "<yourStsAccessKeyID>" and "<yourStsAccessKeySecret>" with the AccessKey
    ID and AccessKey secret of the AccessKey pair assigned by STS that is obtained in the p
    revious step.
    DefaultProfile profile = DefaultProfile.getProfile("<yourRegionID>", "<yourStsAcces
    skey>", "<yourStsAccessSecret>");
    HttpClientConfig clientConfig = HttpClientConfig.getDefault();
    clientConfig.setIgnoreSSLCerts(true);
    clientConfig.setProtocolType(ProtocolType.HTTPS);
    profile.setHttpClientConfig(clientConfig);
    IAcsClient client = new DefaultAcsClient(profile);
    CommonRequest request = new CommonRequest();
    request.setSysDomain("ecs.aliyuns.com");
    request.setSysProduct("Ecs");
    request.setSysAction("DescribeZones");
    request.setSysVersion("2014-05-26");
    request.setSysMethod(MethodType.POST);
    request.setHttpContentType(FormatType.FORM);
    // Replace "<yourRegionID>" with the actual region ID.
    request.putHeadParameter("x-acs-regionid", "<yourRegionID>");
    // Replace "<yourStsToken>" with the STS token of the AccessKey pair assigned by ST
    S that is obtained in the previous step.
    request.putQueryParameter("SecurityToken", "<yourStsToken>");
    // Optional. Replace "<yourResourceGroupID>" with the actual resource set ID.
    // request.putHeadParameter("x-acs-resourcegroupid", "<yourResourceGroupID>");
    // Required. Replace "<yourOrganizationID>" with the actual organization ID.
    request.putHeadParameter("x-acs-organizationid", "<yourOrganizationID>");
    try {
        CommonResponse response = client.getCommonResponse(request);
        System.out.println(response.getData());
    } catch (ServerException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    } catch (ClientException e) {
        System.out.println(e.getErrCode());
        System.out.println(e.getErrMsg());
    }
}

```

1.5. Obtain an endpoint

This topic describes how to obtain the endpoint of an Apsara Stack Security service.

Context

To use the POP gateway to call the API operations of a cloud service, you must specify the endpoint of the cloud service. You can obtain the endpoint from Apsara Stack onsite O&M engineers. You can also perform the following steps to obtain the endpoint.

Procedure

1. **Log on to the Apsara Infrastructure Management console.** In the left-side navigation pane, choose

Operations > Cluster Operations.

2. On the **Clusters** page, enter yundun-advance in the **Project** search box and enter BasicThinCluster in the **Cluster** search box. Click the name of the **BasicThinCluster** cluster or click **Operations** in the Actions column of the **BasicThinCluster** cluster.
3. On the **Cluster Details** page, click the **Cluster Configuration** tab, find and open the **kv.conf** file, and then obtain the values of the region and internet-domain parameters.
4. Obtain the value of the EndpointPre parameter. For more information, see [Common parameters](#).
5. Obtain the endpoint based on the region, internet-domain, and EndpointPre parameters.

The endpoint of a cloud service is in the following format:

```
${EndpointPre}.${global:region}.${global:internet-domain}
```

What to do next

If you want to call the API operations of Apsara Stack Security services from the service domain or O&M domain, you must configure the hosts file on your computer.

1. Obtain the virtual IP address (VIP) of the POP.
 - i. Click **Back to Old Version** to switch to Apsara Infrastructure Management of the previous version. In the top navigation bar, choose **Operations > Cluster Operations**.
 - ii. In the cluster list, enter webappAll in the **Project** search box and enter StandardCloudCluster in the **Cluster** search box. Click the name of the first **StandardCloudCluster** cluster.
 - iii. In the **Cluster Resource** section, click the  icon to the right of the Type parameter, select **Contains** from the drop-down list, and then enter `vip` as the filter condition to locate the O&M domain, management domain, and service domain.

 **Note** The following list describes the cluster resources that correspond to the three domains:

- O&M domain: The **Name** parameter of the cluster resource is **pop-vip-ops**.
- Management domain: The **Name** parameter of the cluster resource is **pop-vip-mgmt**.
- Service domain: The **Name** parameter of the cluster resource is **pop-vip-biz**.

- iv. Right-click the value in the Result volume for the O&M domain, management domain, or service domain and select **Show More**. In the Details dialog box, obtain the value of the vip_ip parameter.
2. Configure the hosts file on your local computer.

```
<vip_ip> <Endpoint of the API that you want to request>
```

2. Call examples

2.1. Call examples for SDK for Java

2.1.1. Quick start

This topic describes how to obtain and use Apsara Stack SDK for Java.

Prerequisites

- An Apsara Stack tenant account that has the required permissions and an AccessKey pair that consists of an AccessKey ID and an AccessKey secret are obtained before you can use Apsara Stack SDK for Java. You can view and obtain your AccessKey pair in the Apsara Uni-manager Management Console. For more information, see [Obtain an AccessKey pair](#).
- For more information about how to obtain the endpoint, see [Obtain an endpoint](#).
- Java Development Kit (JDK) 1.8 or later is installed before you can use Apsara Stack SDK for Java.

Installation

If you use Apache Maven to manage a Java project, you need to only import the JAR file of Apsara Stack SDK for Java to the pom.xml file of the project.

If you want to use Apsara Stack Security SDK for Java, you must install the core library of Apsara Stack SDK for Java. We recommend that you use V4.5.17 or later of the core library.

Usage

To use Apsara Stack SDK for Java, perform the following steps:

1. Create a DefaultAcsClient instance and initialize the instance.
2. Create an API request and configure the required parameters.
3. Initiate the API request and process the response or exception.

Note

In the following code, replace the variables with actual values. Delete the angle brackets <> in the final code.

The following section describes the variables:

- <your-region-id>: Replace this variable with the region ID.
- <your-access-key-id>: Replace this variable with your AccessKey ID.
- <your-access-key-secret>: Replace this variable with your AccessKey secret.
- <your-endpoint>: Replace this variable with the endpoint of the service.
- <API-version>: Replace this variable with the version of the API.
- <your-action>: Replace this variable with the name of the API operation.

```
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.
            "<your-access-key-id>", // The AccessKey ID.
            "<your-access-key-secret>"); // The AccessKey secret.
        IAcsClient client = new DefaultAcsClient(profile);
        // Create an API request and configure the required parameters.
        CommonRequest request = new CommonRequest();
        request.setDomain("<your-endpoint>");// The endpoint of the service.
        request.setVersion("<API-version>");// The version of the API.
        request.setAction("<your-action>");// The name of the API operation.
        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();
        }
    }
}
```

2.1.2. Use SDK

2.1.2.1. Install SDK for Java

This topic describes how to install and use Apsara Stack Security SDK for Java.

Apsara Stack SDK for Java supports Java Development Kit (JDK) 1.8 or later. You can install Apsara Stack SDK for Java by adding Maven dependencies or downloading the SDK. For more information, visit [Alibaba Cloud SDKs](#).

If you want to use Apsara Stack Security SDK for Java, you must install the core library of Apsara Stack SDK for Java. We recommend that you use V4.5.17 or later of the core library.

When you install the core library, you must add the following dependency to the pom.xml file. For more information about the specific SDK version, visit [Alibaba Cloud SDKs](#).

```
<!-- Alibaba Cloud SDK for Java -->
<dependency>
  <groupId>com.aliyun</groupId>
  <artifactId>aliyun-java-sdk-core</artifactId>
  <version>4.5.17</version>
</dependency>
```

2.1.2.2. Use CommonRequest to call API operations

Note

If you want to call the API operations of a service that does not provide SDKs, you can use CommonRequest. You can use CommonRequest to call API operations.

Benefits

CommonRequest provides the following benefits:

1. **Lightweight**: You need to only download the core package. You do not need to download and install SDKs of services.
2. **Easy to use**: You can call the newly released API operations of a service without the need to update the SDK for the service.
3. **Fast iteration**.

Use CommonRequest to call an API operation

Apsara Stack services provide RPC and RESTful APIs. The request method of CommonRequest varies based on the style of the API that you want to call.

In most cases, an API uses the RPC style if the API operations include the Action parameter. An API uses the RESTful style if the API operations include the PathPattern parameter. All API operations of a service use the same API style. The API of each service supports only one style. If you pass an invalid identifier, another API operation may be called, or the `ApiNotFound` error is returned.

If you want to send a CommonRequest request, you must obtain the values of the following parameters. For more information about the values of these parameters, see the API reference in [Documentation](#). You can also visit [OpenAPI Explorer](#) to obtain the parameter values of API operations for some services.

- **Endpoint**: the endpoint of a service.
- **Version**: the version of the API. The version is in the YYYY-MM-DD format.
- **Operation information**: the name of the API operation that you want to call.
 - The APIs of most Apsara Stack services, such as Threat Detection Service, are RPC APIs. If you want to call an RPC API operation, you must obtain the value of the Action parameter, and then specify the value in the `request.ApiName = "<Action>"` format.

- If you want to call a RESTful API operation of a service, such as Container Service for Kubernetes (ACK), you must obtain the value of the PathPattern parameter, and then specify the RESTful path in the `request.PathPattern = "<PathPattern>"` format.

Example: Call an RPC API operation

The following sample code shows how to use CommonRequest to call an API operation of Apsara Stack Security:

```
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.
            "<your-access-key-id>",      // The AccessKey ID.
            "<your-access-key-secret>"); // The AccessKey secret.
        IAcsClient client = new DefaultAcsClient(profile);
        // Create an API request and specify parameters.
        CommonRequest request = new CommonRequest();
        request.setDomain("<your-endpoint>");// The endpoint of the service.
        request.setVersion("<API-version>");// The version of the API.
        request.setAction("<your-action>");// The name of the API operation.
        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();
        }
    }
}
```

2.2. Call examples for SDK for Python

2.2.1. Quick start

This topic describes how to obtain and use the SDK for Python.

Prerequisites

- An authorized account and an AccessKey pair (AccessKey ID and AccessKey secret) are obtained. For more information, see [Obtain an AccessKey pair](#).
- The endpoint of a service is obtained. For more information, see .

Install the core library of the SDK for Python

- If you use Python 2.x, run the following command:

```
pip install aliyun-python-sdk-core
```

- If you use Python 3.x, run the following command:

```
pip3 install aliyun-python-sdk-core-v3
```

Use the SDK for Python

To use the SDK for Python, perform the following steps:

1. Create a client instance.

When you create a client instance, you must obtain a region ID, AccessKey ID, and AccessKey secret.

2. Create an API request and specify the required parameters.
3. Initiate the API request and process the response or exception.

 **Note** In the following code, replace the variables with actual values. Delete the angle brackets <> in the final code.

The following section describes the variables:

- <your_region_id>: Replace the value of this parameter with the region ID.
- <your_access_key_id>: Replace the value of this parameter with your AccessKey ID.
- <your_access_key_secret>: Replace the value of this parameter with your AccessKey secret.
- <your-endpoint>: Replace the value of this parameter with the endpoint of the service.
- <API-version>: Replace the value of this parameter with the version of the API.
- <your-action>: Replace the value of this parameter with the name of the API operation.

```
from aliynsdkcore.client import AcsClient
from aliynsdkcore.request import
CommonRequest
client = AcsClient('{your_access_key_id}',
'your_access_key_secret', '{your_region_id}')
request = CommonRequest()
request.set_domain('<your-endpoint>')// The endpoint of the service.
request.set_version('<API-version>')// The version of the API.
request.set_action_name('<your-action>')// The name of the API operation.
# or:
# request =
CommonRequest(domain='<your-endpoint>', version='<API-version>',
action_name='<your-action>')
request.add_query_param('PageNumber', '1')
request.add_query_param('PageSize', '30')
response =
client.do_action_with_exception(request)
```

2.2.2. Use SDK

2.2.2.1. Install SDK for Python

This topic describes how to install and use SDK for Python.

Apsara Stack SDK for Python supports Python 2.6.x, Python 2.7.x, and Python 3.x or later. You can install Apsara Stack SDK for Python by using pip.

 **Note** To use the SDK of an Apsara Stack service, you must install the core library of Apsara Stack SDK for Python.

- If you use Python 2.x, run the following command to install the core library:

```
pip install aliyun-python-sdk-core
```

- If you use Python 3.x, run the following command to install the core library:

```
pip3 install aliyun-python-sdk-core-v3
```

2.2.2.2. Use CommonRequest to call API operations

 **Note** If you want to call the API operations of an Apsara Stack service that does not provide SDKs, you can use CommonRequest. You can use CommonRequest to call API operations.

Benefits

CommonRequest provides the following benefits:

1. **Lightweight**: You need only to download the core package. You do not need to download and install SDKs of Apsara Stack services.
2. **Easy to use**: You can call the newly released API operations of an Apsara Stack service without the need to update the SDK for the service.
3. **Fast iteration**.

Use CommonRequest to call an API operation

Apsara Stack services provide RPC and RESTful APIs. The request method of CommonRequest varies based on the style of the API that you want to call.

In most cases, an API uses the RPC style if the API operations include the Action parameter. An API uses the RESTful style if the API operations include the PathPattern parameter. All API operations of a service use the same API style. The API of each service supports only one style. If you pass an invalid identifier, another API operation may be called, or the `ApiNotFound` error is returned.

If you want to send a CommonRequest request, you must obtain the values of the following parameters. For more information about the values of these parameters, see the API reference in [Documentation](#). You can also visit [OpenAPI Explorer](#) to obtain the parameter values of API operations for some services.

- **Endpoint**: the endpoint of a service.
- **Version**: the version of the API. The version is in the YYYY-MM-DD format.
- **Operation information**: the name of the API operation that you want to call.
 - The APIs of most Apsara Stack services, such as Threat Detection Service, are RPC APIs. If you want to call an RPC API operation, you must obtain the value of the Action parameter, and then specify the value in the `request.ApiName = "<Action>"` format.
 - If you want to call a RESTful API operation of a service, such as Container Service for Kubernetes (ACK), you must obtain the value of the PathPattern parameter, and then specify the RESTful path in the `request.PathPattern = "<PathPattern>"` format.

Example: Call an RPC API operation

The following sample code shows how to use the CommonRequest method to call the API operation:

```
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('<your-endpoint>') //The endpoint of the service.
request.set_version('<API-version>') //The version of the API.
request.set_action_name('<your-action>') //The name of the API operation.
# or:
# request = CommonRequest(domain='<your-endpoint>', version='<API-version>', action_name='your-action')
request.add_query_param('PageNumber', '1')
request.add_query_param('PageSize', '30')
response = client.do_action_with_exception(request)
```

2.3. Call examples for SDK for Go

2.3.1. Quick start

Apsara Stack SDK for Go allows you to access services without complex coding. This topic describes how to obtain and use the SDK for Go.

Prerequisites

- An authorized account and an AccessKey pair (AccessKey ID and AccessKey secret) are obtained. You can obtain and view your AccessKey pair in the Apsara Uni-manager Management Console. For more information, see [Obtain an AccessKey pair](#).
- The endpoint of a service is obtained. For more information, see .

Install the core package of Apsara Stack SDK for Go

Apsara Stack SDK for Go supports Go 1.10.x and later. You can run the following command to install the core package:

```
go get -u github.com/aliyun/alibaba-cloud-sdk-go/sdk
```

Use the SDK for Go

To use the SDK for Go, perform the following steps:

1. Initialize a client instance.
2. Create an API request and specify the required parameters.
3. Initiate the API request and process the response or exception.

 **Note** In the following code, replace the variables with actual values. Delete the angle brackets <> in the final code.

The following section describes the variables:

- <your_region_id>: Replace the value of this parameter with the region ID.
- <your_access_key_id>: Replace the value of this parameter with your AccessKey ID.
- <your_access_key_secret>: Replace the value of this parameter with your AccessKey secret.
- <your-endpoint>: Replace the value of this parameter with the endpoint of the service.
- <API-version>: Replace the value of this parameter with the version of the API.
- <your-action>: Replace the value of this parameter with the name of the API operation.

```
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_key_secret}")
    if err != nil {
        panic(err)
    }
    request
    := requests.NewCommonRequest()
    request.Domain = "<your-endpoint>"// The endpoint of the service.
    request.Version = "<API-version>"// The version of the API.
    request.ApiName = "<your-action>"// The name of the API operation.
    request.QueryParams["PageNumber"] = "1"
    request.QueryParams["PageSize"] = "30"
    response, err := client.ProcessCommonRequest(request)
    if err != nil {
        panic(err)
    }
    fmt.Print(response.GetHttpContentString())
}
```

2.3.2. Use SDK

2.3.2.1. Install Go SDK

This topic describes how to install the Go SDK.

The Alibaba Cloud Go SDK supports Go 1.7 or later versions. Install the Go SDK manually.

1. Download the source code of the Go SDK from the [official site of Apsara Stack](#).
2. Extract the package to the directory where the `GO_PATH` file of the current user resides.

2.3.2.2. Use CommonRequest to call API operations

Note

If you want to call the API operations of an Apsara Stack service that does not provide SDKs, you can use `CommonRequest`. You can use `CommonRequest` to call API operations.

Benefits

`CommonRequest` provides the following benefits:

1. **Lightweight**: You need only to download the core package. You do not need to download and install SDKs of Apsara Stack services.

2. Easy to use: You can call the newly released API operations of an Apsara Stack service without the need to update the SDK for the service.
3. Fast iteration.

Use CommonRequest to call an API operation

Apsara Stack services provide RPC and RESTful APIs. The request method of CommonRequest varies based on the style of the API that you want to call.

In most cases, an API uses the RPC style if the API operations include the Action parameter. An API uses the RESTful style if the API operations include the PathPattern parameter. All API operations of a service use the same API style. The API of each service supports only one style. If you pass an invalid identifier, another API operation may be called, or the `ApiNotFound` error is returned.

If you want to send a CommonRequest request, you must obtain the values of the following parameters. For more information about the values of these parameters, see the API reference in [Documentation](#). You can also visit [OpenAPI Explorer](#) to obtain the parameter values of API operations for some services.

- Endpoint: the endpoint of a service.
- Version: the version of the API. The version is in the YYYY-MM-DD format.
- Operation information: the name of the API operation that you want to call.
 - The APIs of most Apsara Stack services, such as Threat Detection Service, are RPC APIs. If you want to call an RPC API operation, you must obtain the value of the Action parameter, and then specify the value in the `request.ApiName = "<Action>"` format.
 - If you want to call a RESTful API operation of a service, such as Container Service for Kubernetes (ACK), you must obtain the value of the PathPattern parameter, and then specify the RESTful path in the `request.PathPattern = "<PathPattern>"` format.

Example: Call an RPC API operation

The following sample code shows how to use the CommonRequest method to call the API operation:


```
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("cn-hangzhou", "{your_access_key_id}", "{your_access_key_secret}")
    if err != nil {
        panic(err)
    }
    request := requests.NewCommonRequest()
    request.Domain = "<your-endpoint>" // The endpoint of the service.
    request.Version = "<API-version>" // The version of the API.
    request.ApiName = "<your-action>" // The name of the API operation.
    request.QueryParams["PageNumber"] = "1"
    request.QueryParams["PageSize"] = "30"
    response, err := client.ProcessCommonRequest(request)
    if err != nil {
        panic(err)
    }
    fmt.Print(response.GetHttpContentString())
}
```

3.Common parameters

Common request parameters

Common request parameters must be included in all Apsara Stack Security API requests.

Table of common request parameters

Parameter	Type	Required	Description
Format	String	No	The format in which to return the response. Set the value to JSON.
Version	String	Yes	The version number of the API. Specify the version number in the YYYY-MM-DD format. Valid values: - If you call the API operations of the cloud service whose service code is Auditprivate, set the value to 2018-01-16. - If you call the API operations of the cloud service whose service code is yundunnextsoc, set the value to 2019-07-23. - If you call the API operations of the cloud service whose service code is Sas, set the value to 2018-12-03. - If you call the API operations of the cloud service whose service code is aegis, set the value to 2016-11-11. - If you call the API operations of the cloud service whose service code is yundun-css, set the value to 2021-10-11. - If you call the API operations of the cloud service whose service code is secspy, set the value to 2019-08-05. - If you call the API operations of the cloud service whose service code is Ddosprivate, set the value to 2018-01-16. - If you call the API operations of the cloud service whose service code is hsm-private, set the value to 2018-06-30. - If you call the API operations of the cloud service whose service code is Cloudfw, set the value to 2017-12-07. - If you call the API operations of the cloud service whose service code is Sddp, set the value to 2019-01-03. - If you call the API operations of the cloud service whose service code is semawaf, set the value to 2020-07-01. - If you call the API operations of the cloud service whose service code is soar, set the value to 2018-12-03.
AccessKeyId	String	Yes	The AccessKey ID provided to you by Apsara Stack.
AccessKeySecret	String	Yes	The AccessKey secret provided to you by Apsara Stack.
RegionId	String	Yes	The region ID of the service.

Parameter	Type	Required	Description
Product	String	Yes	The name of the service to which the API operation belongs. Valid values: • Auditprivate: basic components of Apsara Stack Security • yundunnextsoc: Security Operations Center (SOC) • Sas: Threat Detection Service • aegis: Server Guard • yundun-css: Container Production • secspy: Network Detection and Response • Ddosprivate: Anti-DDoS Service • hsm-private: Data Encryption Service • Cloudfw: Cloud Firewall • Sddp: Sensitive Data Discovery and Protection (SDDP) • semawaf: Web Application Firewall (WAF) • soar: Security Orchestration and Automation Response (SOAR)
EndpointPre	String	Yes	The prefix in the endpoint of the service to which the API operation belongs. Valid values: • auditprivate: the prefix in the endpoint of basic components of Apsara Stack Security • yundunnextsoc-pop: the prefix in the endpoint of SOC • tds: the prefix in the endpoint of Threat Detection Service • aegis: the prefix in the endpoint of Server Guard • yundun-css: the prefix in the endpoint of Container Protection • secspy-share: the prefix in the endpoint of Network Detection and Response • ddosprivate: the prefix in the endpoint of Anti-DDoS Service • hsmprivate: the prefix in the endpoint of Data Encryption Service • cloudfw: the prefix in the endpoint of Cloud Firewall • sddp-api: the prefix in the endpoint of SDDP • semawaf: the prefix in the endpoint of WAF • soar: the prefix in the endpoint of SOAR

Common response parameters

API responses use the HTTP response format:

- A 2xx status code indicates a successful call.
- A 4xx or 5xx status code indicates a failed call.

Responses are returned in the JSON format. Every response returns a unique RequestID regardless of whether the call is successful.

4. Server Guard

4.1. Asset management

4.1.1. 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 <i>DescribeGroupSummary</i> .

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"
}
```

4.1.2. 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 <i>DescribeGroupStruct</i> .
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: 7: 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
}
```

4.1.3. 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 <i>DescribeAllEntity</i> .
GroupId	Long	No	The ID of the asset group.
Os	String	No	The operating system of the server. Valid values: • <i>win</i>: indicates the Windows operating system. • <i>linux</i>: 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":"*****"
    },
    .....
  ]
}
```

4.1.4. 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 <i>DescribeEntityList</i> .
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: <i>wir</i>: indicates the Windows operating system. <i>linux</i>: indicates the Linux operating system.
Account	String	No	Queries servers with unusual logons detected. Set this parameter to <i>remoteLogin</i> .
Health	String	No	Queries servers with baseline check issues detected. Set this parameter to <i>exception</i> .
Patch	String	No	Queries servers with vulnerabilities detected. Set this parameter to <i>vul</i> .
Suspicious	String	No	Queries servers with unusual events detected. Set this parameter to <i>exception</i> .
Trojan	String	No	Queries servers with webshells detected. Valid values: <i>webshell</i>: indicates trojan files. <i>process</i>: indicates trojan processes.
Status	String	No	The status of the Server Guard Agent. Valid values: <i>offline</i>: indicates that the Server Guard Agent is offline. <i>pause</i>: 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.

Parameter	Type	Description
CurrentPage	Integer	The number of the current page returned.
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":"****"
    }
  ]
}
```

4.1.5. 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

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set this parameter to <i>DescribeMachines</i> .
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"
}
```

4.1.6. 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 <i>DescribeMachineDetail</i> .
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.
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.

Parameter	Type	Description
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": "****"
  }
}
```

4.1.7. 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 <i>DescribePropertyStatistic</i> .
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.

Name	Type	Description
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"
}
```

4.1.8. DescribePropertyPortItem

Description

You can call this operation to obtain a list of listener ports on hosts.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribePropertyPortItem</i> .
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: <i>20</i> .
CurrentPage	Integer	No	The current page number. Default value: <i>1</i> .
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
}
```

4.1.9. 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 <i>DescribePropertyPortDetail</i> .
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.
Port	String	No	The port number.

Parameter	Type	Required	Description
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.
Port	String	The port number.

Parameter	Type	Description
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
}
```

4.1.10. 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 <i>DescribePropertyProcltem</i> .
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: <i>20</i> .
CurrentPage	Integer	No	The current page number. Default value: <i>1</i> .
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.
PropertyProcltems	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
}
```

4.1.11. 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 <i>DescribePropertyProcDetail</i> .
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
}
```

4.1.12. 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 <i>DescribePropertySoftwareItem</i> .
PageSize	Integer	No	The maximum number of records displayed on a page. Default value: 20.
CurrentPage	Integer	No	The current page number. Default value: 7.
Name	String	No	The name of the application.
Path	String	No	The application installation path.

Name	Type	Required	Description
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,
}
```

4.1.13. 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 <i>DescribePropertySoftwareDetail</i> .
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.
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.

Parameter	Type	Required	Description
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.
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
}
```

4.1.14. 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 <i>DescribePropertyUserItem</i> .
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
}
```

4.1.15. 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 <i>DescribePropertyUserDetail</i> .
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.
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.

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.
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.
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"
    }
  ]
}
```

4.1.16. 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 <i>DescribeTopRiskyAssets</i> .

Parameter	Type	Required	Description
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
    }
  ]
}
```

4.2. Vulnerability management

4.2.1. 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 <i>DescribeTarget</i> .
Type	String	No	The type of the risks. For example, <i>vul</i> 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: <i>groupId</i>: indicates the ID of an asset group. <i>uuid</i>: 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"
    }
  ]
}
```

4.2.2. 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

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeVulTargetStatistics</i> .
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: <i>groupId</i>: indicates an asset group ID. <i>uuid</i>: 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
}
```

4.2.3. 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 <i>DescribeTargetConfig</i> .
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.
Type	String	The type of the vulnerability.
Config	String	Whether vulnerability scanning is enabled. Valid values: on and off.

Name	Type	Description
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"
    }
  ]
}
```

4.2.4. 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 <i>DescribeVulConfig</i> .
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"
    }
  ]
}
```

4.2.5. 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 <i>DescribeAutoDelConfig</i> .

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
}
```

4.2.6. 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 <i>DescribeVulLevel</i> .

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"]
}
```

4.2.7. 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 <i>DescribeVulWhitelist</i> .
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
}
```

4.2.8. 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 <i>DescribeGroupedVul</i> .
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: <i>20</i> .
CurrentPage	Integer	No	The current page number. Default value: <i>1</i> .
Dealed	String	No	Indicates whether the vulnerability has been handled. Valid values: • <i>Y</i>: indicates that the vulnerability has been handled. • <i>N</i>: indicates that the vulnerability has not been handled.
Direction	String	No	The sorting mode of vulnerabilities in the vulnerability group. Valid values: • <i>asc</i>: indicates sorting in ascending order. • <i>desc</i>: 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.

Name	Type	Required	Description
Level	String	No	The severity of the vulnerability. Valid values: • <i>serious</i>: critical • <i>high</i>: important • <i>medium</i>: moderate • <i>low</i>: low
Name	String	No	The name of the vulnerability.
Necessity	String	No	The necessity for fixing the vulnerability. Valid values: • <i>asap</i>: indicates that the vulnerability must be fixed as soon as possible. • <i>later</i>: indicates that the vulnerability can be fixed later. • <i>nntf</i>: 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
}
```

4.2.9. 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 <i>DescribeVulList</i> .
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: <i>20</i> .
CurrentPage	Integer	No	The current page number. Default value: <i>1</i> .
Dealed	String	No	Indicates whether the vulnerability has been handled. Valid values: • <i>Y</i>: indicates that the vulnerability has been handled. • <i>N</i>: indicates that the vulnerability has not been handled.
Level	String	No	The severity of the vulnerability. Valid values: • <i>serious</i>: critical • <i>high</i>: important • <i>medium</i>: moderate • <i>low</i>: low
Name	String	No	The name of the vulnerability.
Necessity	String	No	The necessity for fixing the vulnerability. Valid values: • <i>asap</i>: indicates that the vulnerability must be fixed as soon as possible. • <i>later</i>: indicates that the vulnerability can be fixed later. • <i>nntf</i>: 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
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: <i>asap</i>: indicates that the vulnerability must be fixed as soon as possible. <i>later</i>: indicates that the vulnerability can be fixed later. <i>nntf</i>: 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.
ResultCode	String	The code of the vulnerability handling result.

Name	Type	Description
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":"normal","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-minimal","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"
    }
  ]
}
```

4.2.10. DescribeVulDetails

Description

You can call this operation to query detailed information about a vulnerability.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeVulDetails</i> .
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).
Cveld	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.
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.

Name	Type	Description
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 operating 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"
}
```

4.2.11. 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 <i>DescribeVulNumStatistics</i> .
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
}
```

4.2.12. 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 <i>DescribeVulLevelStatistics</i> .
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"
}
```

4.2.13. 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 <i>DescribeVulMachineList</i> .

Name	Type	Required	Description
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.
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"
}
```

4.3. Baseline check

4.3.1. DescribeStratetyDetail

Description

You can call this operation to query the details of a specified baseline check policy.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeStrategyDetail</i> .
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.
SubTypes	Array	The list of risk subcategories. For more information, see the following parameter descriptions.
Alias	String	The name of the risk subcategory.

Name	Type	Description
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"
          }
        ]
      }
    ]
  }
}

```

4.3.2. 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

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeStrategyTarget</i> .
Config	String	No	The policy configuration information. The baseline check policy ID is specified in JSON format, for example, <pre>{"strategyId":15161}</pre> .
Type	String	No	The configuration type. Set the value to <i>hc_strategy</i> .
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.
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: <i>add</i>: indicates the whitelist mode, that is, the policy applies to the asset group. <i>del</i>: 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 <i>groupId</i> , indicating that the value of the <i>Target</i> 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"
}
```

4.3.3. 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 <i>DescribeUuidConfig</i> .
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: <i>add</i>: indicates enabled. <i>del</i>: 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",
}
```

4.3.4. 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 <i>DescribeUserSetting</i> .

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"
}
```

4.3.5. 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 <i>DescribeRiskWhiteList</i> .
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query output. Default value: <i>20</i> .
CurrentPage	Integer	No	The current page number. Default value: <i>1</i> .
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.

Name	Type	Description
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
}
```

4.3.6. DescribeStrategy

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 <i>DescribeStrategy</i> .

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.
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: <i>add</i>: indicates the whitelist mode, that is, the policy applies to the asset group. <i>del</i>: 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.

Name	Type	Description
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=DescribeStrategy
&<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
    }
  ]
}
```

4.3.7. 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 <i>DescribeStrategyExecDetail</i> .
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,
}
```

4.3.8. 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 <i>DescribeRiskType</i> .
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.
WarnCount	String	The number of risks that have been detected.

Name	Type	Description
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,
}
```

4.3.9. Describeshummary

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 <i>Describeshummary</i> .
PageSize	Integer	No	The number of records displayed on a page. Default value: 20.
CurrentPage	Integer	No	The current page number. Default value: 7.
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.

Name	Type	Required	Description
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.

Name	Type	Description
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":"38AAFEFE-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 the SSH V1 protocol is used\n4. Checks whether the RSH protocol is used\n5. Checks whether authentication-based logon is performed\n Solution: \n Edit /etc/ssh/sshd_config\n1. Port (not 22)\n2. PermitRootLogin (no)\n3. Protocol (2)\n4. Ignore Rhosts (yes)\n5. e) HostbasedAuthentication (no)
      "Level":"low",
      "TypeAlias":"System",
      "SubTypeAlias":"Baseline check policy",
      "RiskName":"SSH logon baseline check"
    }
  ]
}
```

4.4. Unusual logon detection

4.4.1. 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 <i>DescribeBaseConfigs</i> .
Type	String	Yes	The type of the logon security configuration record. Valid values: <i>login_common_location</i>: indicates an approved logon location. <i>login_common_ip</i>: indicates an approved logon IP address. <i>login_common_time</i>: indicates an approved logon time period. <i>login_common_account</i>: indicates an approved logon account.

Name	Type	Required	Description
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.
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.

Name	Type	Description
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: <i>groupid</i>: indicates an asset group ID. <i>uuid</i>: 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
}
```

4.4.2. 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 <i>DescribeSwitchConfigs</i> .

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: <i>login_common_location</i>: indicates an approved logon location. <i>login_common_ip</i>: indicates an approved logon IP address. <i>login_common_time</i>: indicates an approved logon time range. <i>login_common_account</i>: indicates an approved logon account.
Status	Integer	The status of the configuration item. Valid values: <i>1</i>: indicates enabled. <i>0</i>: 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-4AE4-8604-58BDEC873F4",
  "ConfigList":[
    {
      "Status":1,
      "Item":"login_common_ip"
    },
    {
      "Status":0,
      "Item":"login_common_account"
    },
    {
      "Status":0,"Item":"login_common_time"
    }
  ]
}
```

4.4.3. 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 <i>DescribeConfigTarget</i> .
Type	String	Yes	The logon security configuration record used to identify a valid logon to a server. Valid values: <i>login_common_location</i>: indicates an approved logon location. <i>login_common_ip</i>: indicates an approved logon IP address. <i>login_common_time</i>: indicates an approved logon time range. <i>login_common_account</i>: indicates an approved logon account.

Name	Type	Required	Description
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.
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: <i>groupId</i>: indicates an asset group ID. <i>uuid</i>: 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",
}
```

4.5. Webshell detection

4.5.1. 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 <i>DescribeCategoryCount</i> .

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
}
```

4.5.2. 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 <i>DescribeWebshell</i> .
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: <i>n</i>: indicates that the event is pending. <i>y</i>: 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.

Parameter	Type	Description
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.
Instanceld	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.
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-bp15xtqydmbugep****",
    "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-bp15xtqydmbugepdbev",
    "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"
}
```

4.5.3. 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 <i>DescribeQuaraFile</i> .
PageSize	Integer	No	The maximum number of records to be displayed on each page of the query result. Default value: <i>20</i> .
CurrentPage	Integer	No	The current page number. Default value: <i>1</i> .

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.
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: <i>quaraFailed("0")</i>: indicates that the file failed to be quarantined. <i>rollbackFailed("1")</i>: indicates that the file failed to be rolled back to a previous version. <i>quaraDone("2")</i>: indicates that the file has been quarantined. <i>rollbackDone("3")</i>: indicates that the file has been rolled back to a previous version. <i>quaraing("4")</i>: indicates that the file is being quarantined. <i>rollbacking("5")</i>: indicates that the file is being rolled back to a previous version.
Md5	String	The MD5 value of the file.

Name	Type	Description
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"
    }
  ]
}
```

4.6. Exception detection on hosts

4.6.1. 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 <i>DescribeSuspEventTypes</i> .

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
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"
    }
  ]
}
```

4.6.2. 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
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeSuspTrendStatistics</i> .

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": [ ]
}
```

4.6.3. 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 <i>DescribeSuspiciousExportInfo</i> .
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.
ExportStatus	String	The status of the export task. Valid values: <i>init</i>: indicates that the export task is being initialized. <i>pending</i>: indicates that the export task is pending. <i>exporting</i>: indicates that the export task is being executed. <i>success</i>: indicates that the export task has been completed. <i>fail</i>: 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_1518071576098.zip?Expires=1518075176&OSSAccessKeyId=<yourAccessKeyId>&Signature=xxxx%xxxx%3D"
}
```

4.7. Retrieval of host logs

4.7.1. 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
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeFilterFields</i> .
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.

Name	Type	Description
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", "fieldName": "default"
    }
  ],
  "Total": "20",
  "RequestID": "883e1e3d-4443-4206-871c-6c0625c01332"
}
```

4.7.2. 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 <i>DescribeHistogram</i> .
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,
        0
      ]
    }
  ]
}
```


4.7.3. 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 <i>DescribeLogInfo</i> .
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.

Name	Type	Description
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"
    },
  ]
}
```

4.7.4. 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 <i>DescribeLogItems</i> .
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.
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.

Name	Type	Description
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.
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
}
```

5. Sensitive Data Discovery and Protection

5.1. APIs

5.1.1. DescribeDataAssets

Description

Queries data assets globally based on the specified conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeDataAssets</i> .
Rangeld	Integer	Yes	The type of the assets to query. Valid values: 1: MaxCompute project 2: MaxCompute table 3: MaxCompute package 27: Object Storage Service (OSS) bucket 22: OSS object 37: Tablestore instance 32: Tablestore table 57: ApsaraDB RDS database 52: ApsaraDB RDS table
CurrentPage	Integer	Yes	The page number of the current page.
PageSize	Integer	Yes	The number of entries to return on each page.
Name	String	No	The keyword. Fuzzy match is supported.
RuleId	Long	No	The ID of the rule.
RiskLevels	String	No	The ID of the risk level. Separate multiple IDs with commas (,).

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The total number of returned pages.
CurrentPage	Integer	The page number of the current page.
PageSize	Integer	The number of entries returned per page.
Items	Array	The assets.
Owner	String	The account that owns the asset.
ProductCode	String	The code of the service. Example: RDS or OSS.
Acl	String	The access control list (ACL) for the OSS bucket.
RiskLevelId	Long	The ID of the risk level.
RiskLevelName	String	The name of the risk level.
DepartName	String	The name of the department.
Name	String	The name of the asset.
Labelsec	Boolean	The label security tag of the MaxCompute asset.
CreationTime	Long	The creation time. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	The ID of the primary key.
Protection	Boolean	The protection flag of the MaxCompute asset.
RuleName	String	The name of the hit rule.
ObjectKey	String	The key of the OSS object.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://sddp-api.[RegionId].example.com/?Action=DescribeDataAssets
&RangeId=1
&CurrentPage=1
&PageSize=10
&<Common request parameters>
```


- Sample success responses in JSON format

```
{
  "RequestId": "71064826-726F-4ADA-B879-05D8055476FB",
  "TotalCount": 4,
  "PageSize": 10,
  "CurrentPage": 1,
  "Items": [
    {
      "Owner": "dtdep-239-153536994****",
      "ProductCode": "ODPS",
      "ProductId": 1,
      "Acl": "",
      "RiskLevelId": 2,
      "RiskLevelName": "Internal",
      "DepartName": "DemoCenter",
      "Name": "****data",
      "Labelsec": false,
      "CreationTime": 1536751124000,
      "Sensitive": true,
      "Id": 268,
      "Protection": false,
      "RuleName": "Hit rule",
      "ObjectKey": "Internal"
    }
  ]
}
```

5.1.2. DescribeInstances

Description

You can call this operation to query instances, databases, projects, or buckets based on the specified conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeInstances</i> .
ProductCode	String	Yes	The code of the big data service, for example, RDS or OSS.
CurrentPage	Integer	Yes	The number of the page to return.
PageSize	Integer	Yes	The number of entries to return on each page.
Name	String	No	The search keyword. Fuzzy match is supported.

Parameter	Type	Required	Description
RuleId	Long	No	The ID of the rule.
RiskLevelId	Long	No	The ID of the risk level.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The total number of returned pages.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
Items	Array	The list of instances.
Owner	String	The account of the instance owner.
ProductCode	String	The code of the big data service, for example, RDS or OSS.
Acl	String	The access control list (ACL) for the OSS bucket.
RiskLevelId	Long	The ID of the risk level.
RiskLevelName	String	The name of the risk level.
DepartName	String	The name of the department.
Name	String	The name of the asset.
Labelsec	Boolean	The label security flag of the MaxCompute asset.
CreationTime	Long	The time when the instance was created. Unit: milliseconds.
Id	Long	The ID of the primary key.
Protection	Boolean	The protection flag of the MaxCompute asset.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=DescribeInstances
&CurrentPage=1
&PageSize=10
&ProductCode=ODPS
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "71064826-726F-4ADA-B879-05D8055476FB",
  "TotalCount": 4,
  "PageSize": 10,
  "CurrentPage": 1,
  "Items": [
    {
      "Owner": "dtdep-239-153536994****",
      "ProductCode": "ODPS",
      "ProductId": 1,
      "Acl": "",
      "RiskLevelId": 2,
      "RiskLevelName": "Internal",
      "DepartName": "DemoCenter",
      "Name": "****data",
      "Labelsec": false,
      "CreationTime": 1536751124000,
      "Sensitive": true,
      "Id": 268,
      "Protection": false
    }
  ]
}
```

5.1.3. DescribeTables

Description

Queries data asset tables of MaxCompute, ApsaraDB RDS, and Tablestore that SDDP is authorized to scan.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeTables</i> .
InstanceId	Long	Yes	The ID of the instance.
CurrentPage	Integer	Yes	The page number of the current page.
PageSize	Integer	Yes	The number of entries to return on each page.

Parameter	Type	Required	Description
Name	String	No	The keyword. Fuzzy match is supported.
RuleId	Long	No	The ID of the rule.
RiskLevelId	Long	No	The ID of the risk level.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The total number of returned pages.
CurrentPage	Integer	The page number of the current page.
PageSize	Integer	The number of entries returned per page.
Items	Array	The instances.
Owner	String	The account that owns the instance.
ProductCode	String	The code of the big data service. Example: RDS or OSS.
Acl	String	The access control list (ACL) for the OSS bucket.
RiskLevelId	Long	The ID of the risk level.
RiskLevelName	String	The name of the risk level.
DepartName	String	The name of the department.
Name	String	The name of the asset.
Labelsec	Boolean	The label security tag of the MaxCompute asset.
CreationTime	Long	The creation time. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	The ID of the primary key.
Protection	Boolean	The protection tag of the MaxCompute asset.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://sddp-api.[RegionId].example.com/?Action=DescribeInstances
&CurrentPage=1
&PageSize=10
&ProductCode=ODPS
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "71064826-726F-4ADA-B879-05D8055476FB",
  "TotalCount": 4,
  "PageSize": 10,
  "CurrentPage": 1,
  "Items": [
    {
      "Owner": "dtdep-239-153536994****",
      "ProductCode": "ODPS",
      "ProductId": 1,
      "Acl": "",
      "RiskLevelId": 2,
      "RiskLevelName": "Internal",
      "DepartName": "DemoCenter",
      "Name": "****data",
      "Labelsec": false,
      "CreationTime": 1536751124000,
      "Sensitive": true,
      "Id": 268,
      "Protection": false
    }
  ]
}
```

5.1.4. DescribePackages

Description

You can call this operation to query MaxCompute packages based on the specified conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribePackages</i> .
InstanceId	Long	Yes	The ID of the instance.
CurrentPage	Integer	Yes	The number of the page to return.
PageSize	Integer	Yes	The number of entries to return on each page.

Parameter	Type	Required	Description
Name	String	No	The search keyword. Fuzzy match is supported.
RuleId	Long	No	The ID of the rule.
RiskLevelId	Long	No	The ID of the risk level.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The total number of returned pages.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
Items	Array	The list of packages.
Owner	String	The account of the package owner.
RiskLevelId	Long	The ID of the risk level.
RiskLevelName	String	The name of the risk level.
DepartName	String	The name of the department.
Name	String	The name of the asset.
CreationTime	Long	The time when the package was created. Unit: milliseconds.
Id	Long	The ID of the primary key.
InstanceId	Long	The ID of the instance.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[ RegionId ].example.com/?Action=DescribePackages
&CurrentPage=1
&PageSize=20
&InstanceId=1
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "TotalCount": 4,
  "PageSize": 10,
  "CurrentPage": 1,
  "Items": [
    {
      "Owner": "dtdep-239-153536994****",
      "ProductCode": "ODPS",
      "ProductId": 1,
      "Acl": "",
      "RiskLevelId": 2,
      "RiskLevelName": "Internal",
      "DepartName": "DemoCenter",
      "Name": "****data",
      "CreationTime": 1536751124000,
      "Sensitive": true,
      "Id": 268,
      "InstanceId": 1
    }
  ]
}
```

5.1.5. DescribeColumns

Description

Queries columns in tables of MaxCompute, ApsaraDB RDS, and Tablestore that SDDP is authorized to scan.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeColumns</i> .
InstanceId	Long	Yes	The ID of the instance.
TableId	Long	Yes	The ID of the table.
CurrentPage	Integer	Yes	The page number of the current page.
PageSize	Integer	Yes	The number of entries to return on each page.
Name	String	No	The keyword. Fuzzy match is supported.
RuleId	Long	No	The ID of the rule.

Parameter	Type	Required	Description
RiskLevelId	Long	No	The ID of the risk level.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The total number of returned pages.
CurrentPage	Integer	The page number of the current page.
PageSize	Integer	The number of entries returned per page.
Items	Array	The packages.
Owner	String	The account that owns the package.
RiskLevelId	Long	The ID of the risk level.
RiskLevelName	String	The name of the risk level.
DepartName	String	The name of the department.
Name	String	The name of the asset.
CreationTime	Long	The creation time. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
Id	Long	The ID of the primary key.
RuleId	Long	The ID of the hit rule.
RuleName	String	The name of the hit rule.
TableId	Long	The ID of the table.
InstanceId	Long	The ID of the instance.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests


```
https://sddp-api.[RegionId].example.com/?Action=DescribeColumns
&CurrentPage=1
&PageSize=20
&InstanceId=1
&TableId=1
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "TotalCount": 4,
  "PageSize": 10,
  "CurrentPage": 1,
  "Items": [
    {
      "Owner": "dtdep-239-153536994****",
      "ProductCode": "ODPS",
      "ProductId": 1,
      "Acl": "",
      "RiskLevelId": 2,
      "RiskLevelName": "Internal",
      "DepartName": "DemoCenter",
      "Name": "****data",
      "CreationTime": 1536751124000,
      "Sensitive": true,
      "Id": 268,
      "RuleId": 1,
      "RuleName": "Hit rule",
      "InstanceId": 1,
      "TableId": 1
    }
  ]
}
```

5.1.6. DescribeOssObjects

Description

You can call this operation to query Object Storage Service (OSS) objects based on the specified conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeOssObjects</i> .
InstanceId	Long	Yes	The ID of the instance.
CurrentPage	Integer	Yes	The number of the page to return.

Parameter	Type	Required	Description
PageSize	Integer	Yes	The number of entries to return on each page.
Name	String	No	The search keyword. Fuzzy match is supported.
RuleId	Long	No	The ID of the rule.
RiskLevelId	Long	No	The ID of the risk level.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
TotalCount	Integer	The total number of returned pages.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
Items	Array	The list of packages.
RiskLevelId	Long	The ID of the risk level.
RiskLevelName	String	The name of the risk level.
DepartName	String	The name of the department.
Name	String	The name of the asset.
Id	Long	The ID of the primary key.
RegionId	String	The ID of the region.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[ RegionId ].example.com/?Action=DescribeOssObjects
&CurrentPage=1
&PageSize=20
&InstanceId=1
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "TotalCount": 4,
  "PageSize": 10,
  "CurrentPage": 1,
  "Items": [
    {
      "RiskLevelName": "Internal",
      "Id": 17383,
      "RiskLevelId": 2,
      "RegionId": "cn-hangzhou",
      "Name": "obj****"
    }
  ]
}
```

5.1.7. DescribeOssObjectDetail

Description

You can call this operation to query the details of an Object Storage Service (OSS) object that SDDP is authorized to access.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeOssObjectDetail</i> .
Id	Long	Yes	The ID of the OSS object.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
OssObjectDetail	Object	The details of the OSS object.
RiskLevelId	Long	The ID of the risk level.
RiskLevelName	String	The name of the risk level.
Name	String	The name of the asset.
Id	Long	The ID of the primary key.
RegionId	String	The ID of the region.
CategoryName	String	The type of the OSS object.

Parameter	Type	Description
RuleList	Array	A list of the matched rules.
RuleName	String	The name of the matched rule.
Count	Integer	The number of matches.

Error codes

For a list of error codes, visit the [Error codes](#).

Examples

- Sample requests

```
https://sddp-api.[ RegionId ].example.com/?Action=DescribeOssObjectDetail
&Id=12
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "OssObjectDetail": {
    "RegionId": "cn-hangzhou",
    "BucketName": "",
    "RiskLevelName": "Internal",
    "Id": 17383,
    "RiskLevelId": 2,
    "CategoryName": "MAC address",
    "Name": "obj_id",
    "RuleList": [
      {
        "RuleName": "ID card number",
        "Count": 10
      }
    ]
  }
}
```

5.1.8. DescribeDeparts

Description

You can call this operation to query departments based on the specified conditions.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeDeparts</i> .
CurrentPage	Integer	Yes	The number of the page to return.
PageSize	Integer	Yes	The number of entries to return on each page.
Key	String	No	The search keyword. Fuzzy match is supported.
AccountType	Integer	No	The type of the query. Valid values: 1: department query. 2: account query.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
TotalCount	Integer	The total number of returned pages.
Items	Array	The list of departments.
Id	Long	The ID of the primary key.
DepartName	String	The name of the department.
DepartId	Long	The ID of the department.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[ RegionId ].example.com/?Action=DescribeDeparts
&CurrentPage=1
&PageSize=10
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "PageSize": 10,
  "CurrentPage": 1
  "TotalCount": 1,
  "Items": [
    {
      "Id": 283,
      "DepartId": 2,
      "DepartName": "Development"
    }
  ]
}
```

5.1.9. DescribeAccounts

Description

Queries accounts based on the specific conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeAccounts</i> .
CurrentPage	Integer	Yes	The number of the page to return.
PageSize	Integer	Yes	The number of entries to return on each page.
Key	String	No	The search keyword. Fuzzy match is supported.
DepartId	Long	No	The ID of the department.
QueryType	Integer	No	The type of the resource. Valid values: 1: instances 2: tables 3: packages 4: columns 5: tables in a package
ProductCode	String	No	The code of the service. Valid values: - MaxCompute - RDS - OTS

Parameter	Type	Required	Description
OperationId	Integer	No	The type of the operation. For more information, see Operation type definition .
InstanceId	Long	No	The ID of the instance.
TableId	Long	No	The ID of the table.
PackageId	Long	No	The ID of the package.
ColumnId	Long	No	The ID of the column.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
TotalCount	Integer	The total number of returned pages.
Items	Array	The list of accounts.
Id	Long	The ID of the primary key.
LongName	String	The name of the account.
Email	String	The email address.
CreateTime	Long	The time when the account was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
LoginDataTime	Long	The last logon time of the account. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
UserId	Long	The ID of the account.
FullName	String	The display name.
CellphoneNum	String	The mobile phone number.
TelephoneNum	String	The landline phone number.

Parameter	Type	Description
AccountTypeId	Integer	The type of the account. Valid values: 1: an Apsara Stack tenant account of a department 2: a platform account 3: a RAM user 4: an ApsaraDB RDS account

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://sddp-api.[RegionId].example.com/?Action=DescribeAccounts
&CurrentPage=1
&PageSize=10
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "PageSize": 10,
  "CurrentPage": 1,
  "TotalCount": 1,
  "Items": [
    {
      "LoginName": "sddp_****",
      "Email": "test@example.com",
      "CreateTime": 1543300900000,
      "LoginDataTime": 1544493748000,
      "UserId": 10****,
      "FullName": "sddp****",
      "Id": 1091,
      "CellphoneNum": "1300000****",
      "TelephoneNum": "0571-6000****",
      "AccountTypeId": 1
    }
  ]
}
```

5.1.10. DescribeAccountDetail

Description

Queries the details of an account based on its ID and type.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeAccountDetail</i> .
UserId	Long	Yes	The ID of the account.
AccountTypeid	Integer	Yes	The type of the account. Valid values: • 1: an Apsara Stack tenant account of a department • 2: a platform account • 3: a RAM user • 4: an ApsaraDB RDS account

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request
Account	Object	The details of the account.
Id	Long	The ID of the primary key.
LongName	String	The name of the account.
Email	String	The email address.
CreateTime	Long	The time when the account was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
LoginDataTime	Long	The last logon time of the account. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
UserId	Long	The ID of the account.
FullName	String	The display name.
CellphoneNum	String	The mobile phone number.
TelephoneNum	String	The landline phone number.
PrivilegeList	Array	The accounts that can be used.
ProdcutName	String	The service on which the account has operation permissions. Multiple services are separated with forward slashes (/).

Parameter	Type	Description
UseAccountName	String	The name of the account that can be used.
UseAccountId	Long	The ID of the account that can be used.
UseAccountType	Integer	The type of the account that can be used.
UseAccountCreateTime	Long	The time when the account was created. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://sddp-api.[ RegionId ].example.com/?Action=DescribeAccountDetail
&UserId=1
&AccountTypeId=2
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "Account": {
    "LoginName": "yundun****",
    "Email": "kf@example.com",
    "CreateTime": 1543384996000,
    "LoginDataTime": 1543385065000,
    "UserId": 1045,
    "FullName": "yundun****",
    "Id": 882,
    "CellphoneNum": "1300000****",
    "TelephoneNum": "0571-6000****",
    "PrivilegeList": [
      {
        "UseAccountType": 2,
        "ProductName": "OSS/ODPS",
        "UseAccountCreateTime": 1546413235000,
        "UseAccountName": "ram_****",
        "UseAccountId": 259
      }
    ]
  }
}
```

5.1.11. DescribePrivileges

Description

Queries permissions of an account based on its ID and other specific conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribePrivileges</i> .
CurrentPage	Integer	Yes	The number of the page to return.
PageSize	Integer	Yes	The number of entries to return on each page.
AccountId	Long	Yes	The ID of the account.
UseAccountId	Long	No	The ID of the account that is granted the permissions.
Key	String	No	The search keyword. Fuzzy match is supported.
DataTypelds	String	No	The type of the resource. For more information about the resource types, see Resource type definition .

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
TotalCount	Integer	The total number of returned pages.
Items	Array	The permissions.
Id	Long	The ID of the primary key.
AccountId	Long	The ID of the account.

Parameter	Type	Description
AccountType	Integer	The type of the account. Valid values: 1: an Apsara Stack tenant account of a department 2: a platform account 3: a RAM user 4: an ApsaraDB RDS account
UseAccountId	Long	The ID of the account that is granted the permissions.
UseAccountType	Long	The type of the account that is granted the permissions. Valid values: 1: an Apsara Stack tenant account of a department 2: a platform account 3: a RAM user 4: an ApsaraDB RDS account
DataType	String	The type of the resource. For more information about the resource types, see Resource type definition .
DataTypeId	Integer	The ID of the resource. For more information about the resource types, see Resource type definition .
DataInstance	String	The instance. An asterisk (*) indicates all instances.
DataTable	String	The table. An asterisk (*) indicates all tables.
DataColumn	String	The column. An asterisk (*) indicates all columns.
DataPackage	String	The package. An asterisk (*) indicates all packages.
ResourceName	String	The name of the resource.
ResourcePath	String	The path of the resource.
Operation	String	The operation permission. Multiple permissions are separated by semicolons (;).
PolicyCondition	String	The usage conditions.
Sensitive	Boolean	Indicates whether the permission is sensitive.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://sddp-api.[ RegionId].example.com/?Action=DescribePrivileges
&CurrentPage=1
&PageSize=20
&AccountId=1
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "PageSize": 10,
  "CurrentPage": 1,
  "TotalCount": 1,
  "Items": [
    {
      "UseAccountType": 2,
      "DataInstance": "341",
      "AccountId": 259,
      "ResourceName": "bucket****",
      "Operation": "GET;OPEARETE",
      "AccountType": 2,
      "ResourcePath": "kf",
      "DataTypeId": 21,
      "Sensitive": false,
      "DataType": "OSS_BUCKET",
      "Id": 1,
      "UseAccountId": 259
    }
  ]
}
```

5.1.12. DescribeEventTypes

Description

You can call this operation to query types of anomalous activities based on the specified conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeEventTypes</i> .
ParentTypeId	Long	No	The ID of the type.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
EventTypeList	Array	The list of types.  Note If you do not set the ParentTypeId parameter, the system returns the type list. Otherwise, the system returns the list of subtypes under the specified type.
Id	Long	The ID of the type.
Code	String	The code of the type.
Name	String	The name of the type.
SubTypeList	Array	The list of subtypes.
Id	Long	The ID of the subtype.
Code	String	The code of the subtype.
Name	String	The name of the subtype.
Status	String	The status of the subtype. Valid values: 1: enabled. 2: disabled.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=DescribeEventTypes
&ParentTypeId=1
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId":"769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "EventTypeList":[
    {
      "SubTypeList":[
        {
          "Id":1,
          "Code":"010001",
          "Name":"Incorrect configuration - Sensitive MaxCompute projects are not protected",
          "Status":1
        }
      ],
      "Id":1,
      "Code":"01",
      "Name":"Anomalous permission access"
    }
  ]
}
```

5.1.13. DescribeEvents

Description

You can call this operation to query anomalous activities based on the specified conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeEvents</i> .
CurrentPage	Integer	Yes	The number of the page to return.
PageSize	Integer	Yes	The number of entries to return on each page.
TypeCode	String	No	The ID of the type of the anomalous activity.
UserId	Long	No	The account ID of the operator of the anomalous activity.
DealUserId	Long	No	The account ID of the handler of the anomalous activity.

Parameter	Type	Required	Description
Status	Integer	No	The status of the anomalous activity. Valid values: 0: unprocessed. 1: confirmed as a violation. 2: excluded as a false positive.
SubTypeCode	String	No	The ID of the subtype of the anomalous activity.
StartTime	Long	No	The beginning of the time range to query. Unit: milliseconds.
EndTime	Long	No	The end of the time range to query. Unit: milliseconds.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
TotalCount	Integer	The total number of returned pages.
Items	Array	The list of anomalous activities.
Id	Long	The ID of the anomalous activity.
UserId	Long	The account ID of the operator.
LoginName	String	The account name of the operator.
DisplayName	String	The account display name of the operator.
ProductCode	String	The code of the service where the anomalous activity occurred.
TypeCode	String	The ID of the type.
TypeName	String	The name of the type.
SubTypeCode	String	The ID of the subtype.
SubTypeName	String	The name of the subtype.
AlertTime	Long	The time when the anomalous activity occurred.

Parameter	Type	Description
EventTime	Long	The time when the alert was reported.
Status	Integer	The status of the anomalous activity. Valid values: 0: unprocessed. 1: confirmed as a violation. 2: excluded as a false positive.
DealUserId	Long	The account ID of the handler.
DealLoginName	String	The account name of the handler.
DealDisplayName	String	The account display name of the handler.
DealTime	Long	The time when the anomalous activity was processed. Unit: milliseconds.
Backed	Boolean	Indicates whether the processing result of the anomalous activity was returned as a feedback to the detection algorithm.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=DescribeEvents
&CurrentPage=1
&TypeCode=01
&PageSize=10
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "PageSize": 10,
  "CurrentPage": 1,
  "TotalCount": 1,
  "Items": [
    {
      "Status": 0,
      "TypeName": "Anomalous data flow",
      "Backed": false,
      "TypeCode": "02",
      "ProductCode": "ODPS",
      "SubTypeName": "Download sensitive data in an abnormal geographical location",
      "EventTime": 1545829129000,
      "UserId": "22915744338501****",
      "LoginName": "det****",
      "DisplayName": "yundun****",
      "Id": 4,
      "SubTypeCode": "020001",
      "AlertTime": 1545829129000,
      "StatusName": "To be processed",
      "DealUserId": "229157443385014132",
      "DealLoginName": "det****",
      "DeaulDisplayName": "yundun****",
      "DepartName": "kf"
    }
  ]
}
```

5.1.14. DescribeEventDetail

Description

You can call this operation to query the details of an anomalous activity based on the specified ID.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeEventDetail</i> .
Id	Long	Yes	The ID of the anomalous activity.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
Event	Object	The details of the anomalous activity.

Parameter	Type	Description
Id	Long	The ID of the anomalous activity.
UserId	Long	The account ID of the operator.
LoginName	String	The account name of the operator.
DisplayName	String	The account display name of the operator.
ProductCode	String	The code of the service where the anomalous activity occurred.
TypeCode	String	The ID of the type.
TypeName	String	The name of the type.
SubTypeCode	String	The ID of the subtype.
SubTypeName	String	The name of the subtype.
AlertTime	Long	The time when the anomalous activity occurred.
EventTime	Long	The time when the alert was reported.
Status	Integer	The status of the anomalous activity. Valid values: 0: unprocessed. 1: confirmed as a violation. 2: excluded as a false positive.
DealUserId	Long	The account ID of the handler.
DealLoginName	String	The account name of the handler.
DealDisplayName	String	The account display name of the handler.
DealTime	Long	The time when the anomalous activity was processed. Unit: milliseconds.
Backed	Boolean	Indicates whether the processing result of the anomalous activity was returned as a feedback to the detection algorithm.
Detail	Object	The detailed content of the anomalous activity.
Content	Array	The content.
Label	String	The title.
Value	String	The description.
Chart	Array	The baseline.

Parameter	Type	Description
XLabel	String	The X-axis title.
YLabel	String	The Y-axis title.
Data	Object	The content of the baseline.
X	Array	The array of data along the X-axis.
Y	Array	The array of data along the Y-axis.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=DescribeEventDetail
&Id=1
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "Event": {
    "Status": 0,
    "TypeName": "Anomalous data flow",
    "Backed": false,
    "TypeCode": "02",
    "ProductCode": "ODPS",
    "SubTypeName": "Download sensitive data in an abnormal geographical location",
    "EventTime": 1545829129000,
    "UserId": 22915744338501****,
    "LoginName": "det****",
    "DisplayName": "yundun****",
    "Id": 4,
    "SubTypeCode": "020001",
    "AlertTime": 1545829129000,
    "StatusName": "To be processed",
    "DealUserId": 22915744338501****,
    "DealLoginName": "det****",
    "DealDisplayName": "yundun****",
    "DepartName": "kf",
    "Detail": {
      "Content": [
        {
          "Value": "This anomalous activity may cause exposure of sensitive data to risks and damage to the security baseline.",
          "Label": "Risk exposure"
        }
      ]
    }
  },
}
```

```
    "Chart": [
      {
        "YLabel": "Value",
        "Label": "Event baseline",
        "Data": {
          "X": [
            1,
            2,
            3,
            4,
            5,
            6
          ],
          "Y": [
            1,
            2,
            3,
            4,
            5,
            6
          ]
        },
        "XLabel": "Days"
      }
    ],
    "DealReason": "Confirmed violation"
  }
}
```

5.1.15. ModifyEventStatus

Description

You can call this operation to process an anomalous activity.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>ModifyEventStatus</i> .
Id	Long	Yes	The ID of the anomalous activity.
Status	Integer	Yes	The status of the anomalous activity. Valid values: 1: confirmed as a violation. 2: excluded as a false positive.
DealReason	String	Yes	The processing comments.

Parameter	Type	Required	Description
Backed	Boolean	No	Specifies whether to return the processing result of the anomalous activity as a feedback to the detection algorithm.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=ModifyEventStatus
&Id=1
&Status=1
&DealReason=Confirmed violation
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "8491DBFD-48C0-4E11-B6FC-6F38921244A9"
}
```

5.1.16. ModifyEventTypeStatus

Description

Enables detection of exceptions of subtypes.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>ModifyEventTypeStatus</i> .
SubTypeIds	String	Yes	The subtype IDs of exceptions. Separate multiple IDs with commas (,).

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://sddp-api.[ RegionId ].example.com/?Action=ModifyEventTypeStatus
&SubTypeIds=1,2,3,4
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

5.1.17. ModifyDefaultLevel

Description

You can call this operation to set the default risk level or modify the risk levels of sensitive data.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>ModifyDefaultLevel</i> .
DefaultId	Long	No	The ID of the default risk level.
SensitiveIds	String	No	The ID of the risk level of sensitive data. Separate multiple IDs with commas (,).

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=ModifyDefaultLevel
&Type=15
&DefaultId=2
&SensitiveIds=3,4
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

5.1.18. DescribeRules

Description

You can call this operation to query rules based on the specified conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeRules</i> .
Name	String	No	The search keyword. Fuzzy match is supported.
RiskLevelId	Long	No	The ID of the risk level.
Category	Integer	No	The type of the rule. Valid values: • 0: keyword. • 2: regular expression.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
TotalCount	Integer	The total number of returned pages.
Items	Array	The list of rules.
Id	Long	The ID of the rule.

Parameter	Type	Description
Name	String	The name of the rule.
Content	String	The content of the rule.
Description	String	The description of the rule.
RiskLevelId	Long	The ID of the risk level.
Status	Integer	The status of the rule. Valid values: 0: disabled. 1: enabled.
Category	Integer	The type of the rule. Valid values: 0: keyword. 2: regular expression.
CategoryName	String	The name of the rule type.
UserId	Long	The account ID of the rule creator.
LoginName	String	The account name of the rule creator.
DisplayName	String	The account display name of the rule creator.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=DescribeRules
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "Items": [
    {
      "Description": "IP address",
      "Category": 2,
      "GmtModified": 1545277010000,
      "RiskLevelId": 2,
      "Name": "IP address",
      "GmtCreate": 1545277010000,
      "UserId": 0,
      "Status": 1, //0: disabled. 1: enabled.
      "Content": "(?:\\D|^)((?:(:25[0-4]|2[0-4]\\d|1\\d{2}|[1-9]\\d{1})\\.)(?:(:25[0-5]|2[0-4]\\d|1\\d{0-9}\\d|[1-9]\\d|[1-9]))(?:\\D|$))",
      "CategoryName": "Regular expression",
      "RiskLevelName": "Internal",
      "DepartName": "KF",
      "LoginName": "det****",
      "Id": 2000
    }
  ],
  "TotalCount": 18,
  "PageSize": 10,
  "CurrentPage": 1
}
```

5.1.19. CreateRule

Description

You can call this operation to create a custom rule.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>CreateRule</i> .
Name	String	Yes	The name of the rule.
Content	String	Yes	The content of the rule.
Category	Integer	Yes	The type of the rule. Valid values: 0: keyword. 2: regular expression.
RiskLevelId	Long	Yes	The ID of the risk level.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].aliyuncs.com/?Action=CreateRule
&Name=Mobile phone number
&Category=0
&Content=1300000****
&RiskLevelId=4
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

5.1.20. ModifyRule

Description

You can call this operation to modify a custom rule.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>ModifyRule</i> .
Id	Long	Yes	The ID of the rule.
Name	String	Yes	The name of the rule.
Content	String	Yes	The content of the rule.
Category	Integer	Yes	The type of the rule. Valid values: 0: keyword. 2: regular expression.
RiskLevelId	Long	Yes	The ID of the risk level.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=ModifyRule
&Id=1
&Name=Mobile phone number
&Category=0
&Content=1300000****
&RiskLevelId=4
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

5.1.21. ModifyRuleStatus

Description

You can call this operation to enable or disable a rule.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>ModifyRuleStatus</i> .
Id	Long	Yes	The ID of the rule.
Status	Integer	Yes	The status of the rule. Valid values: 0: disabled. 1: enabled.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=ModifyRuleStatus
&Id=1
&Status=1
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

5.1.22. DeleteRule

Description

You can call this operation to delete a custom rule.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DeleteRule</i> .
Id	Long	Yes	The ID of the rule.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=DeleteRule
&Id=1
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

5.1.23. DescribeDataLimitSet

Description

You can call this operation to query the instances, databases, or buckets of a specified service that Sensitive Data Discovery and Protection (SDDP) is authorized to scan.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeDataLimitSet</i> .
ResourceType	Integer	Yes	The ID of the service. Valid values: • 1: MaxCompute. • 2: Object Storage Service (OSS). • 5: Relational Database Service (RDS).

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
DataLimitList	Array	The list of instances that SDDP is authorized to scan.
Id	Long	The ID of the primary key.
RegionId	String	The ID of the region.
LocalName	String	The name of the region.
ParentId	String	The name of the instance.
UserName	String	The username.
Password	String	The password.
Connector	String	The connection string of the database.

Parameter	Type	Description
OssBucketList	Array	The list of existing OSS buckets.
RegionId	String	The ID of the region.
BucketName	String	The name of the OSS bucket.
RegionList	Array	The list of regions.
RegionId	String	The ID of the region.
LocalName	String	The name of the region.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample request

```
https://sddp-api.[RegionId].example.com/?Action=DescribeDataLimitSet
&ResourceType=1
&<Common request parameters>
```

- Sample success response in JSON format

```
{
  "RequestId": "769FB3C1-F4C9-42DF-9B72-7077A8989C13",
  "DataLimitSet": {
    "ResourceType": 1,
    "DataLimitList": [
      {
        "Id": 1,
        "RegionId": "cn-hangzhou",
        "LocalName": "China (Hangzhou)",
        "ParentId": "oss-bucket",
        "UserName": "Username",
        "Password": "Password",
        "Connector": "Connection string"
      }
    ],
    "OssBucketList": [
      {
        "RegionId": "cn-hangzhou",
        "BucketName": "oss-bucket"
      }
    ],
    "RegionList": [
      {
        "RegionId": "cn-hangzhou",
        "LocalName": "Hangzhou"
      }
    ]
  }
}
```

5.1.24. CreateDataLimit

Description

Authorizes SDDP to scan instances, databases, or buckets of a specified service.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>CreateDataLimit</i> .
ResourceType	Integer	Yes	The ID of the service. Valid values: 1: MaxCompute 2: OSS 5: RDS
RegionId	String	Yes	The ID of the region.

Parameter	Type	Required	Description
ParentId	String	Yes	The name of the instance.
UserName	String	Yes	The username.
Password	String	Yes	The password.
Connector	String	Yes	The connection string of the database.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://sddp-api.[ RegionId ].example.com/?Action=CreateDataLimit
&ResourceType=1
&ServiceRegionId=cn-hangzhou
&ParentId=test
&UserName=<userName>
&Password=<passWord>
@Connector=jdbc:mysql://localhost:3306/test
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "7C3AC882-E5A8-4855-BE77-B6837B695EF1"
}
```

5.1.25. DeleteDataLimit

Description

Revokes permissions granted to SDDP for scanning instances, databases, or buckets of a specified service.

Request parameters

Parameter	Type	Required	Description

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DeleteDataLimit</i> .
Id	Long	Yes	The authorization ID.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://sddp-api.[ RegionId].example.com/?Action=DeleteDataLimit
&Id=1
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "208B016D-4CB9-4A85-96A5-0B8ED1EBF271"
}
```

6.Container Protection

6.1. DescribelmageInfoList

Queries the information about images.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribelmageInfoList	The operation that you want to perform. Set the value to DescribelmageInfoList .
Uuids	String	Yes	UUID1,UUID2,UUID3	The UUIDs of the images. Separate multiple UUIDs with commas (,).

Response parameters

Parameter	Type	Example	Description
ImageInfos	Array of ImageInfo		An array that consists of the information about the images.
AlarmCount	Integer	1	The number of exceptions.
AlarmStatus	String	NO	Indicates whether alerts are triggered. Valid values: • YES • NO
Digest	String	6a5e1031a5858617f7d8a179ead6***	The digest of the image.
Endpoints	String	[]	The endpoint of the image.
ImageCreate	Long	1639236844747	The time when the image was created. The value is a UNIX timestamp. Unit: milliseconds.
ImageId	String	asdaSdasd*****	The ID of the image.

Parameter	Type	Example	Description
ImageSize	Long	100	The size of the image.
ImageUpdate	Long	1639236844747	The time when the image was updated. The value is a UNIX timestamp. Unit: milliseconds.
InstanceId	String	i-km100o6qy8gid*****	The ID of the instance.
RegionId	String	cn-wu***-env***-d01***	The region ID.
RegistryType	String	defaultAcr	The type of the registration.
RepodId	String	crr-vridcl4****	The ID of the image repository.
RepoName	String	centos	The name of the image repository.
RepoNamespace	String	hang***-namespace	The namespace to which the image repository belongs.
RepoType	String	PRIVATE	The type of the image repository. The value is fixed as PRIVATE .
RiskStatus	String	YES	Indicates whether risks are detected. Valid values: • YES • NO
Status	String	NORMAL	The status of the image.
Tag	String	0.2	The tag that is added to the image.
TagImmutable	Integer	1	The label that cannot be changed.
Uuid	String	B41B****-337A-472D-B82E-9FD3642B8***	The UUID of the image.

Parameter	Type	Example	Description
VulCount	Integer	1	The number of vulnerabilities that are detected in the image.
VulStatus	String	YES	Indicates whether vulnerabilities are detected. Valid values: - YES - NO
RequestId	String	B41B****-337A-472D-B82E-9FD3642B****	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageInfoList
&Uuids=UUID1,UUID2,UUID3
&<Common request parameters>
```

Sample success responses

XML format

```
<ImageInfos>
  <Status>NORMAL</Status>
  <RepoNamespace>hang***-namespace</RepoNamespace>
  <RegistryType>defaultAcr</RegistryType>
  <VulStatus>YES</VulStatus>
  <ImageSize>100</ImageSize>
  <Digest>6a5e1031a5858617f7d8a179ead6***</Digest>
  <InstanceId>i-km100o6qy8gid*****</InstanceId>
  <TagImmutable>1</TagImmutable>
  <RepoName>centos</RepoName>
  <RiskStatus>YES</RiskStatus>
  <VulCount>1</VulCount>
  <Endpoints>[]</Endpoints>
  <Uuid>B41B****-337A-472D-B82E-9FD3642B8****</Uuid>
  <ImageCreate>1639236844747</ImageCreate>
  <RepoType>PRIVATE</RepoType>
  <AlarmStatus>NO</AlarmStatus>
  <ImageId>asdaSdasd*****</ImageId>
  <ImageUpdate>1639236844747</ImageUpdate>
  <Tag>0.2</Tag>
  <RegionId>cn-wu***-env***-d01***</RegionId>
  <RepoId>crr-vridcl4****</RepoId>
  <AlarmCount>1</AlarmCount>
</ImageInfos>
<RequestId>B41B****-337A-472D-B82E-9FD3642B****</RequestId>
```

JSON format

```
{
  "ImageInfos": {
    "Status": "NORMAL",
    "RepoNamespace": "hang***-namespace",
    "RegistryType": "defaultAcr",
    "VulStatus": "YES",
    "ImageSize": 100,
    "Digest": "6a5e1031a5858617f7d8a179ead6***",
    "InstanceId": "i-km100o6qy8gid*****",
    "TagImmutable": 1,
    "RepoName": "centos",
    "RiskStatus": "YES",
    "VulCount": 1,
    "Endpoints": "[]",
    "Uuid": "B41B****-337A-472D-B82E-9FD3642B8****",
    "ImageCreate": 1639236844747,
    "RepoType": "PRIVATE",
    "AlarmStatus": "NO",
    "ImageId": "asdaSdasd*****",
    "ImageUpdate": 1639236844747,
    "Tag": 0.2,
    "RegionId": "cn-wu***-env***-d01***",
    "RepoId": "crr-vridcl4****",
    "AlarmCount": 1
  },
  "RequestId": "B41B****-337A-472D-B82E-9FD3642B8****"
}
```

6.2. DescribeImageBaselineCheckSummary

Queries image baseline check results.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeImageBaselineCheckSummary	The operation that you want to perform. Set the value to DescribeImageBaselineCheckSummary .

Parameter	Type	Required	Example	Description
RiskLevel	String	No	high,medium,low	The severity of the image baseline risk. Separate multiple severities with commas (,). Valid values: • high • medium • low
Criteria	String	No	<pre>[{"name\\":\\"risk Status\\",\\"value\\":\\"YES\\"}, {"name\\":\\"internetIp\\",\\"value\\":\\"1.2.3.4\\"}]</pre>	The search conditions for assets. Set the value in the following format: <pre>[{"name\\":\\"Name of Condition 1\\",\\"value\\":\\"Value of Condition 1\\"}, {"name\\":\\"Name of Condition 2\\",\\"value\\":\\"Value of Condition 2\\"},{},...]</pre>
CriteriaType	String	No	BaselineClassAlias	The type of the query condition. Valid values: • BaselineClassAlias: baseline category • BaselineNameAlias: baseline name
PageSize	Integer	No	20	The number of entries to return on each page.
CurrentPage	Integer	No	1	The number of the page to return.
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English

Response parameters

Parameter	Type	Example	Description
BaselineResultSummary	Array of BaselineResultSummary		An array that consists of the image baseline check results.

Parameter	Type	Example	Description
BaselineClassAlias	String	Identity authentication	The category of the baseline.
BaselineClassKey	String	identification	The key of the baseline category.
BaselineNameAlias	String	Identity authentication	The name of the baseline.
BaselineNameKey	String	identification	The key of the baseline name.
BaselineNameLevel	String	high	The severity of the baseline.
FirstScanTime	Long	1639236844747	The time when the first image baseline check was performed. The value is a UNIX timestamp. Unit: milliseconds.
HighRiskImage	Integer	1	The number of images on which high baseline risks are detected.
LastScanTime	Long	1639236844747	The time when the last image baseline check was performed. The value is a UNIX timestamp. Unit: milliseconds.
LowRiskImage	Integer	2	The number of images on which low baseline risks are detected.
MiddleRiskImage	Integer	3	The number of images on which medium baseline risks are detected.
Status	Integer	0	The status of the baseline. Valid values: 0: normal 1: abnormal
PageInfo	Struct		The pagination information.
Count	Integer	18	The total number of returned pages.
CurrentPage	Integer	1	The page number of the returned page.

Parameter	Type	Example	Description
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	18	The total number of entries returned.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageBaselineCheckSummary
&<Common request parameters>
```

Sample success responses

XML format

```
<PageInfo>
  <TotalCount>18</TotalCount>
  <PageSize>20</PageSize>
  <CurrentPage>1</CurrentPage>
  <Count>18</Count>
</PageInfo>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<BaselineResultSummary>
  <Status>0</Status>
  <BaselineClassKey>identification</BaselineClassKey>
  <FirstScanTime>1639236844747</FirstScanTime>
  <LowRiskImage>2</LowRiskImage>
  <BaselineClassAlias>Identity authentication</BaselineClassAlias>
  <BaselineNameAlias>Identity authentication</BaselineNameAlias>
  <MiddleRiskImage>3</MiddleRiskImage>
  <HighRiskImage>1</HighRiskImage>
  <BaselineNameLevel>high</BaselineNameLevel>
  <LastScanTime>1639236844747</LastScanTime>
  <BaselineNameKey>identification</BaselineNameKey>
</BaselineResultSummary>
```

JSON format

```
{
  "PageInfo": {
    "TotalCount": 18,
    "PageSize": 20,
    "CurrentPage": 1,
    "Count": 18
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "BaselineResultSummary": {
    "Status": 0,
    "BaselineClassKey": "identification",
    "FirstScanTime": 1639236844747,
    "LowRiskImage": 2,
    "BaselineClassAlias": "Identity authentication",
    "BaselineNameAlias": "Identity authentication",
    "MiddleRiskImage": 3,
    "HighRiskImage": 1,
    "BaselineNameLevel": "high",
    "LastScanTime": 1639236844747,
    "BaselineNameKey": "identification"
  }
}
```

6.3. DescribeImageBaselineItem

Queries the baseline check items of an image.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeImageBaselineItem	The operation that you want to perform. Set the value to DescribeImageBaselineItem .
ImageUuid	String	Yes	e05c0de798217637868ef4****	The UUID of the image.
Status	String	No	1	The status of the baseline check item.
BaselineClassKey	String	No	identification	The key of the baseline type.
BaselineNameKey	String	No	identification	The key of the baseline name.
PageSize	Integer	No	20	The number of entries to return on each page.

Parameter	Type	Required	Example	Description
CurrentPage	Integer	No	1	The number of the page to return.
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English

Response parameters

Parameter	Type	Example	Description
BaselineItemInfos	Array of BaselineItemInfos		An array that consists of the baseline check items.
BaselineClassAlias	String	Identity authentication	The type of the baseline.
BaselineClassKey	String	identification	The key of the baseline type.
BaselineItemAlias	String	Make sure that no accounts in the system use blank passwords	The baseline check item.
BaselineItemKey	String	non_pwd_user	The key of the baseline check item.
BaselineNameAlias	String	Identity authentication	The name of the baseline.
BaselineNameKey	String	identification	The key of the baseline name.
Status	Integer	0	The status of the baseline check item. Valid values: • 0: normal • 1: abnormal
WhiteList	Integer	0	The whitelist.
PageInfo	Struct		The pagination information.

Parameter	Type	Example	Description
Count	Integer	18	The total number of returned pages.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	200	The total number of entries returned.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageBaselineItemList
&ImageUuid=e05c0de798217637868ef4****
&<Common request parameters>
```

Sample success responses

XML format

```
<BaselineItemInfos>
  <Status>0</Status>
  <BaselineClassKey>identification</BaselineClassKey>
  <BaselineItemAlias>Make sure that no accounts in the system use blank passwords</BaselineItemAlias>
  <BaselineClassAlias>Identity authentication</BaselineClassAlias>
  <BaselineItemKey>non_pwd_user</BaselineItemKey>
  <BaselineNameAlias>Identity authentication</BaselineNameAlias>
  <WhiteList>0</WhiteList>
  <BaselineNameKey>identification</BaselineNameKey>
</BaselineItemInfos>
<PageInfo>
  <TotalCount>200</TotalCount>
  <PageSize>20</PageSize>
  <CurrentPage>1</CurrentPage>
  <Count>18</Count>
</PageInfo>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
```

JSON format

```
{
  "BaselineItemInfos": {
    "Status": 0,
    "BaselineClassKey": "identification",
    "BaselineItemAlias": "Make sure that no accounts in the system use blank passwords"
  },
  "BaselineClassAlias": "Identity authentication",
  "BaselineItemKey": "non_pwd_user",
  "BaselineNameAlias": "Identity authentication",
  "WhiteList": 0,
  "BaselineNameKey": "identification"
},
"PageInfo": {
  "TotalCount": 200,
  "PageSize": 20,
  "CurrentPage": 1,
  "Count": 18
},
"RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.4. DescribeImageListWithBaselineName

Queries baseline check results.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeImageListWithBaselineName	The operation that you want to perform. Set the value to DescribeImageListWithBaselineName .
BaselineNameKey	String	Yes	identification	The key of the baseline name.

Parameter	Type	Required	Example	Description
Criteria	String	No	<pre>[{"name\":"risk Status\","\value\":"YES\"}, {"name\":"internetIp\","\value\":"1.2.3.4\"}]</pre>	The search conditions for assets. Set the value in the following format: <pre>[{"name\":"Name of Condition 1\","\value\":"Value of Condition 1\"}, {"name\":"Name of Condition 2\","\value\":"Value of Condition 2\"},{},...]</pre>
CriteriaType	String	No	BaselineNameAlias	The type of the query condition. Valid values: • BaselineClassAlias: baseline category • BaselineNameAlias: baseline name
RepoInstanceId	String	No	cri-datvailb****	The ID of the Container Registry instance.
RepoName	String	No	centos	The name of the image repository.
RepoNamespace	String	No	hanghai-namespace	The namespace to which the image repository belongs.
ImageDigest	String	No	6a5e103187b31a94592a47a5858617f7a179ead61df7606****	The digest of the image.
PageSize	Integer	No	20	The number of entries to return on each page.
CurrentPage	Integer	No	1	The number of the page to return.
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English

Response parameters

Parameter	Type	Example	Description
ImageInfos	Array of ImageInfos		An array that consists of the information about the image.
Digest	String	6a5e1031a5858617f7d8a179ead6****	The digest of the image.
Endpoints	String	[]	The endpoint of the image.
HighRiskImage	Integer	1	The number of images on which high baseline risks are detected.
ImageCreate	Long	1639236844747	The time when the image was created. The value is a UNIX timestamp. Unit: milliseconds.
ImageId	String	asdaSdasd***	The ID of the image.
ImageSize	Integer	212	The size of the image.
ImageUpdate	Long	1639236844747	The time when the image was updated. The value is a UNIX timestamp. Unit: milliseconds.
InstanceId	String	i-km100o6qy8gidwn3****	The ID of the instance.
LowRiskImage	Integer	2	The number of images on which low baseline risks are detected.
MiddleRiskImage	Integer	3	The number of images on which medium baseline risks are detected.
NoRiskImage	Integer	3	The number of images on which no baseline risks are detected.
RegionId	String	cn-wulan-env116-d01***	The region ID.
Repold	String	crr-vridcl4****	The ID of the image repository.

Parameter	Type	Example	Description
RepoName	String	centos1	The name of the image repository.
RepoNamespace	String	hanghai-namespace	The namespace to which the image repository belongs.
RepoType	String	PRIVATE	The type of the image repository. The value is fixed as PRIVATE.
RiskStatus	String	YES	Indicates whether risks are detected. Valid values: • YES • NO
Tag	String	0.2	The tag that is added to the image.
TotalItemCount	Integer	1	The total number of images.
Uuid	String	B41B3780-337A-472D-B82E-9FD36*****	The UUID of the image.
PageInfo	Struct		The pagination information.
Count	Integer	18	The total number of returned pages.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	18	The total number of entries returned.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B935	The ID of the request.

Examples

Sample requests


```
http(s)://[Endpoint]/?Action=DescribeImageListWithBaselineName
&BaselineNameKey=identification
&<Common request parameters>
```

Sample success responses

XML format

```
<ImageInfos>
  <NoRiskImage>3</NoRiskImage>
  <RepoNamespace>hanghai-namespace</RepoNamespace>
  <ImageSize>212</ImageSize>
  <Digest>6a5e1031a5858617f7d8a179ead6****</Digest>
  <InstanceId>i-km100o6qy8gidwn3****</InstanceId>
  <TotalItemCount>1</TotalItemCount>
  <RepoName>centos1</RepoName>
  <RiskStatus>YES</RiskStatus>
  <Endpoints>[]</Endpoints>
  <Uuid>B41B3780-337A-472D-B82E-9FD36*****</Uuid>
  <LowRiskImage>2</LowRiskImage>
  <ImageCreate>1639236844747</ImageCreate>
  <RepoType>PRIVATE</RepoType>
  <MiddleRiskImage>3</MiddleRiskImage>
  <HighRiskImage>1</HighRiskImage>
  <ImageId>asdaSdasd***</ImageId>
  <ImageUpdate>1639236844747</ImageUpdate>
  <Tag>0.2</Tag>
  <RegionId>cn-wulan-env116-d01***</RegionId>
  <RepoId>crr-vridcl4****</RepoId>
</ImageInfos>
<PageInfo>
  <TotalCount>18</TotalCount>
  <PageSize>20</PageSize>
  <CurrentPage>1</CurrentPage>
  <Count>18</Count>
</PageInfo>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B935</RequestId>
```

JSON format

```
{
  "ImageInfos": {
    "NoRiskImage": 3,
    "RepoNamespace": "hanghai-namespace",
    "ImageSize": 212,
    "Digest": "6a5e1031a5858617f7d8a179ead6****",
    "InstanceId": "i-km100o6qy8gidwn3****",
    "TotalItemCount": 1,
    "RepoName": "centos1",
    "RiskStatus": "YES",
    "Endpoints": "[]",
    "Uuid": "B41B3780-337A-472D-B82E-9FD36*****",
    "LowRiskImage": 2,
    "ImageCreate": 1639236844747,
    "RepoType": "PRIVATE",
    "MiddleRiskImage": 3,
    "HighRiskImage": 1,
    "ImageId": "asdaSdasd***",
    "ImageUpdate": 1639236844747,
    "Tag": 0.2,
    "RegionId": "cn-wulan-env116-d01***",
    "RepoId": "crr-vridcl4****"
  },
  "PageInfo": {
    "TotalCount": 18,
    "PageSize": 20,
    "CurrentPage": 1,
    "Count": 18
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B935"
}
```

6.5. DescribeCycleTaskList

Queries image scan tasks.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCycleTaskList	The operation that you want to perform. Set the value to DescribeCycleTaskList .
TaskType	String	Yes	IMAGE_SCAN	The type of the task. Set the value to IMAGE_SCAN .

Parameter	Type	Required	Example	Description
TaskName	String	No	IMAGE_SCAN	The name of the task. Set the value to IMAGE_SCAN .
CurrentPage	Integer	No	1	The number of the page to return.
PageSize	Integer	No	20	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
CycleSchedulerResponseList	Array of CycleSchedulerResponse		An array that consists of scheduled tasks.
ConfigId	String	60846e06a516e91ce1665a8b50****	The ID of the configuration.
Enable	Integer	1	Indicates whether the task is enabled. 0: no 1: yes
FirstDateStr	Long	1639236844747	The time of the first scan. The value is a UNIX timestamp. Unit: milliseconds.
IntervalPeriod	Integer	3	The scan interval.
LastTaskId	String	c619d978da536af2532ea45501ef****	The ID of the latest task.
NextStartTimeStr	Long	1639236844747	The time when the next scan will be performed. The value is a UNIX timestamp. Unit: milliseconds.
Param	String	null	The parameters of the task.
PeriodUnit	String	day	The unit of the scan cycle. The value is fixed as day .
TargetEndTime	Integer	24	The end time of the task. Unit: hours.

Parameter	Type	Example	Description
TargetStartTime	Integer	0	The start time of the task. Unit: hours.
TaskName	String	IMAGE_SCAN	The name of the task. The value is fixed as IMAGE_SCAN .
TaskType	String	IMAGE_SCAN	The type of the task. The value is fixed as IMAGE_SCAN .
PageInfo	Struct		The pagination information.
Count	Integer	15	The total number of returned pages.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	15	The total number of entries returned.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCycleTaskList
&TaskType=IMAGE_SCAN
&<Common request parameters>
```

Sample success responses

`XML` format

```
<CycleScheduleResponseList>
  <TargetEndTime>24</TargetEndTime>
  <TaskName>IMAGE_SCAN</TaskName>
  <TaskType>IMAGE_SCAN</TaskType>
  <Param>{}</Param>
  <Enable>1</Enable>
  <FirstDateStr>1639236844747</FirstDateStr>
  <IntervalPeriod>3</IntervalPeriod>
  <TargetStartTime>0</TargetStartTime>
  <NextStartTimeStr>1639236844747</NextStartTimeStr>
  <ConfigId>60846e06a516e91ce1665a8b50*****</ConfigId>
  <LastTaskId>c619d978da536af2532ea45501ef*****</LastTaskId>
  <PeriodUnit>day</PeriodUnit>
</CycleScheduleResponseList>
<PageInfo>
  <TotalCount>15</TotalCount>
  <PageSize>20</PageSize>
  <CurrentPage>1</CurrentPage>
  <Count>15</Count>
</PageInfo>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
```

JSON format

```
{
  "CycleScheduleResponseList": {
    "TargetEndTime": 24,
    "TaskName": "IMAGE_SCAN",
    "TaskType": "IMAGE_SCAN",
    "Param": "{}",
    "Enable": 1,
    "FirstDateStr": 1639236844747,
    "IntervalPeriod": 3,
    "TargetStartTime": 0,
    "NextStartTimeStr": 1639236844747,
    "ConfigId": "60846e06a516e91ce1665a8b50*****",
    "LastTaskId": "c619d978da536af2532ea45501ef*****",
    "PeriodUnit": "day"
  },
  "PageInfo": {
    "TotalCount": 15,
    "PageSize": 20,
    "CurrentPage": 1,
    "Count": 15
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.6. DescribeContainerCriteria

Queries the conditions that are used to query containers.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeContainerCriteria	The operation that you want to perform. Set the value to DescribeContainerCriteria .
GroupField	String	No	pod	The type of the group that you want to query. Valid values: • pod • appName • namespace • clusterId
Value	String	No	test	The fuzzy search conditions that can be automatically matched.

Response parameters

Parameter	Type	Example	Description
CriteriaList	Array of Criteria		An array that consists of the query conditions.
Name	String	demoKey	The key of the parameter.
Type	String	select	The type of the parameter. Valid values: • input: input box • select: drop-down list
Values	String	value1,value2,value3	The values of the parameter. Multiple values are separated by commas (,).
RequestId	String	clusterTypeB41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeContainerCriteria
&<Common request parameters>
```

Sample success responses

XML format

```
<CriteriaList>
  <Type>select</Type>
  <Values>value1,value2,value3</Values>
  <Name>demoKey</Name>
</CriteriaList>
<RequestId>clusterTypeB41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
```

JSON format

```
{
  "CriteriaList": {
    "Type": "select",
    "Values": "value1,value2,value3",
    "Name": "demoKey"
  },
  "RequestId": "clusterTypeB41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.7. DescribeContainerFieldStatistics

Queries statistics of container risks.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeContainerFieldStatistics	The operation that you want to perform. Set the value to DescribeContainerFieldStatistics .

Response parameters

Parameter	Type	Example	Description
ContainerGroupedFields	Struct		The information about the pod.
AlarmContainerCount	Integer	2	The number of containers on which alerts are generated.
AlarmInstanceCount	Integer	3	The number of instances on which alerts are generated.
AppCount	Integer	1	The number of applications.

Parameter	Type	Example	Description
ClusterCount	Integer	3	The number of clusters.
ContainerCount	Integer	4	The number of containers.
ImageCount	Integer	5	The number of images.
InstanceCount	Integer	2	The number of instances.
NamespaceCount	Integer	1	The number of namespaces.
PodCount	Integer	2	The number of pods.
RiskAppCount	Integer	3	The number of applications on which risks are detected.
RiskContainerCount	Integer	4	The number of containers on which risks are detected.
RiskImageCount	Integer	1	The number of images on which risks are detected.
RiskInstanceCount	Integer	2	The number of instances on which risks are detected.
RiskPodCount	Integer	3	The number of pods on which risks are detected.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeContainerFieldStatistics
&<Common request parameters>
```

Sample success responses

XML format


```
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<ContainerGroupedFields>
  <RiskContainerCount>4</RiskContainerCount>
  <AlarmInstanceCount>3</AlarmInstanceCount>
  <AppCount>1</AppCount>
  <ClusterCount>3</ClusterCount>
  <RiskInstanceCount>2</RiskInstanceCount>
  <RiskAppCount>3</RiskAppCount>
  <NamespaceCount>1</NamespaceCount>
  <PodCount>2</PodCount>
  <InstanceCount>2</InstanceCount>
  <RiskImageCount>1</RiskImageCount>
  <ImageCount>5</ImageCount>
  <ContainerCount>4</ContainerCount>
  <AlarmContainerCount>2</AlarmContainerCount>
  <RiskPodCount>3</RiskPodCount>
</ContainerGroupedFields>
```

JSON format

```
{
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "ContainerGroupedFields": {
    "RiskContainerCount": 4,
    "AlarmInstanceCount": 3,
    "AppCount": 1,
    "ClusterCount": 3,
    "RiskInstanceCount": 2,
    "RiskAppCount": 3,
    "NamespaceCount": 1,
    "PodCount": 2,
    "InstanceCount": 2,
    "RiskImageCount": 1,
    "ImageCount": 5,
    "ContainerCount": 4,
    "AlarmContainerCount": 2,
    "RiskPodCount": 3
  }
}
```

6.8. DescribeContainerGroupedFieldDetail

Queries the details of pods.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeContainerGroupFieldDetail	The operation that you want to perform. Set the value to DescribeContainerGroupFieldDetail .
Criteria	String	Yes	<pre>[{"name\":\"riskStatus\",\"value\":\"YES\"}, {"name\":\"internetIp\",\"value\":\"1.2.3.4\"}]</pre>	The search conditions for assets. Set the value in the following format: <pre>[{"name\":\"Name of Condition 1\",\"value\":\"Value of Condition 1\"}, {"name\":\"Name of Condition 2\",\"value\":\"Value of Condition 2\"},{},...]</pre> Supported search conditions include the instance ID, instance name, virtual private cloud (VPC) ID, region, and public IP address. You can call the DescribeCriteria operation to query the supported search conditions.
GroupField	String	Yes	pod	The group type that you want to use for query. Valid values: • pod • appName • namespace • clusterId

Response parameters

Parameter	Type	Example	Description
Data	Struct		The details of the pod.
AlarmCount	Integer	1	The statistics of alerts.
AppName	String	csi-provisioner	The name of the application.
ClusterCurrentVersion	String	None	This parameter is deprecated.

Parameter	Type	Example	Description
ClusterId	String	Cccfd68c474454665ace07efce924****	The ID of the cluster.
ClusterName	String	test****	The name of the cluster.
ClusterState	String	None	This parameter is deprecated.
ClusterType	String	None	This parameter is deprecated.
ContainerCount	Integer	1	The number of containers.
CreateTime	Long	1639236844747	The creation time. The value is a UNIX timestamp. Unit: milliseconds.
InstanceCount	Integer	1	The number of instances.
Namespace	String	*****-namespace	The namespace to which the image repository belongs.
NodeName	String	cn-****-env116-d01.i-km100o6qw4bhyq** ****	The name of the node.
Pod	String	csi-provisioner-564c7989c4-9t8z8	The pod.
PodCount	Integer	2	The number of pods.
PodIp	String	172.29.0.130	The IP address of the pod.
RegionId	String	cn-wulan-env116-d01	The region ID.
VulCount	Integer	2	The number of vulnerabilities.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeContainerGroupedFieldDetail
&Criteria=[{"name\":\"riskStatus\",\"value\":\"YES\"},{\"name\":\"internetIp\",\"value\":\"1.2.3.4\"}]
&GroupField=pod
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<Data>
  <ClusterState>None</ClusterState>
  <Pod>csi-provisioner-564c7989c4-9t8z8</Pod>
  <ClusterId>Cccfd68c474454665ace07efce924****</ClusterId>
  <NodeName>cn-****-env116-d01.i-km100o6qw4bhyq*****</NodeName>
  <CreateTime>1639236844747</CreateTime>
  <ClusterType>None</ClusterType>
  <Namespace>*****-namespace</Namespace>
  <VulCount>2</VulCount>
  <AppName>csi-provisioner</AppName>
  <PodCount>2</PodCount>
  <InstanceCount>1</InstanceCount>
  <ClusterCurrentVersion>None</ClusterCurrentVersion>
  <ContainerCount>1</ContainerCount>
  <PodIp>172.29.0.130</PodIp>
  <ClusterName>test****</ClusterName>
  <RegionId>cn-wulan-env116-d01</RegionId>
  <AlarmCount>1</AlarmCount>
</Data>
```

JSON format

```
{
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "Data": {
    "ClusterState": "None",
    "Pod": "csi-provisioner-564c7989c4-9t8z8",
    "ClusterId": "Cccfd68c474454665ace07efce924****",
    "NodeName": "cn-****-env116-d01.i-km100o6qw4bhyq*****",
    "CreateTime": 1639236844747,
    "ClusterType": "None",
    "Namespace": "*****-namespace",
    "VulCount": 2,
    "AppName": "csi-provisioner",
    "PodCount": 2,
    "InstanceCount": 1,
    "ClusterCurrentVersion": "None",
    "ContainerCount": 1,
    "PodIp": "172.29.0.130",
    "ClusterName": "test****",
    "RegionId": "cn-wulan-env116-d01",
    "AlarmCount": 1
  }
}
```

6.9. DescribeContainerInstances

Queries containers.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeContainerInstances	The operation that you want to perform. Set the value to DescribeContainerInstances .

Parameter	Type	Required	Example	Description
Criteria	String	No	<code>[{"name\":"risk Status\","value\":"YES\"}, {"name\":"internetIp\","value\":"1.2.3.4\"}]</code>	The search conditions for assets. Set the value in the following format: <pre>[{"name\":"Name of Condition 1\","value\":"Value of Condition 1\"}, {"name\":"Name of Condition 2\","value\":"Value of Condition 2\"}, {}, ...]</pre> Supported search conditions include the instance ID, instance name, virtual private cloud (VPC) ID, region, and public IP address. You can call the DescribeCriteria operation to query the supported search conditions.
LogicalExp	String	No	OR	The logical relationship among the search conditions. Valid values: OR: The logical relationship among the search conditions is OR. AND: The logical relationship among the search conditions is AND.
PageSize	Integer	No	20	The number of entries to return on each page.
CurrentPage	Integer	No	1	The number of the page to return.

Response parameters

Parameter	Type	Example	Description
ContainerInstanceList	Array of ContainerInstance		An array that consists of the containers.
AlarmCount	Integer	1	The statistics of alerts.
AlarmStatus	String	NO	Indicates whether alerts were triggered. Valid values: YES NO

Parameter	Type	Example	Description
AppName	String	csi-provisioner	The name of the application.
ClusterId	String	Cccfd68c474454665 ace07efce924****	The ID of the cluster to which the container belongs.
ClusterName	String	test****	The name of the cluster to which the container belongs.
ContainerId	String	B41B3780-337A- 472D-B82E- 9FD3*****	The ID of the container.
CreateTimestamp	Long	1639236844747	The timestamp when the container was created. Unit: milliseconds.
HcCount	Integer	1	The number of baseline risks.
HcStatus	String	NO	Indicates whether baseline risks were detected. Valid values: • YES • NO
HostIp	String	47.100.XX.XX	The IP address.
Image	String	registry.acs.intra.env 116.shuguang.com/ acs/log- controller:0.2.7.0- 68ada84-aliyun	The image.
ImageDigest	String	6a5e103187b31a945 92a47a5858617f7a1 79ead61df7606****	The digest of the image.
ImageId	String	asdaSdasd*****	The ID of the image.
ImageRepoName	String	centos1	The image repository.
ImageRepoNamespace	String	shanghai- namespace	The namespace to which the image repository belongs.

Parameter	Type	Example	Description
ImageRepoTag	String	0.2.7.0-68ada84-aliyun	The tag that is added to the image repository.
ImageUuid	String	e05c0de798217637868ef4****	The UUID of the image.
InstanceId	String	i-km100o6qy8g***** **	The ID of the instance.
Namespace	String	shanghai-namespace	The namespace to which the image repository belongs.
NodeInfo	String	None	This parameter is deprecated.
NodeName	String	cn-wulan-env116-d01.i-km100o6qw4bhyqo7pbvb	The name of the node.
Pod	String	csi-provisioner-564c7989c4-9****	The pod.
PodIp	String	172.29.0.130	The IP address of the pod.
RegionId	String	cn-***-env116-d01	The region ID.
RiskCount	String	1	The number of risks.
RiskStatus	String	YES	Indicates whether risks were detected. Valid values: • YES • NO
UpdateMark	String	None	This parameter is deprecated.
VulCount	Integer	0	The number of vulnerabilities.

Parameter	Type	Example	Description
VulStatus	String	NO	Indicates whether vulnerabilities were detected. Valid values: • YES • NO
PageInfo	Struct		The pagination information.
Count	Integer	20	The total number of returned pages.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	50	The total number of entries returned.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeContainerInstances
&<Common request parameters>
```

Sample success responses

`XML` format

```

<ContainerInstanceList>
  <VulStatus>NO</VulStatus>
  <ImageDigest>6a5e103187b31a94592a47a5858617f7a179ead61df7606****</ImageDigest>
  <NodeName>cn-wulan-env116-d01.i-km100o6qw4bhyqo7pbvb</NodeName>
  <ImageRepoNamespace>shanghai-namespace</ImageRepoNamespace>
  <Image>registry.acs.intra.env116.shuguang.com/acs/log-controller:0.2.7.0-68ada84-aliyun
</Image>
  <ImageUuid>e05c0de798217637868ef4****</ImageUuid>
  <RiskCount>1</RiskCount>
  <AppName>csi-provisioner</AppName>
  <ContainerId>B41B3780-337A-472D-B82E-9FD3*****</ContainerId>
  <ImageId>asdaSdasd</ImageId>
  <ClusterName>test****</ClusterName>
  <CreateTimestamp>1639236844747</CreateTimestamp>
  <AlarmCount>1</AlarmCount>
  <HcCount>1</HcCount>
  <HostIp>192.1.1.130</HostIp>
  <Pod>csi-provisioner-564c7989c4-9****</Pod>
  <InstanceId>i-km100o6qy8g*****</InstanceId>
  <ClusterId>Cccfd68c474454665ace07efce924****</ClusterId>
  <RiskStatus>YES</RiskStatus>
  <Namespace>shanghai-namespace</Namespace>
  <VulCount>0</VulCount>
  <ImageRepoName>centos1</ImageRepoName>
  <NodeInfo>None</NodeInfo>
  <PodIp>172.29.0.130</PodIp>
  <AlarmStatus>NO</AlarmStatus>
  <RegionId>cn-***-env116-d01</RegionId>
  <ImageRepoTag>0.2.7.0-68ada84-aliyun</ImageRepoTag>
  <HcStatus>NO</HcStatus>
  <UpdateMark>None</UpdateMark>
</ContainerInstanceList>
<PageInfo>
  <TotalCount>50</TotalCount>
  <PageSize>20</PageSize>
  <CurrentPage>1</CurrentPage>
  <Count>20</Count>
</PageInfo>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>

```

JSON format

```
{
  "ContainerInstanceList": {
    "VulStatus": "NO",
    "ImageDigest": "6a5e103187b31a94592a47a5858617f7a179ead61df7606****",
    "NodeName": "cn-wulan-env116-d01.i-km100o6qw4bhyqo7pbvb",
    "ImageRepoNamespace": "shanghai-namespace",
    "Image": "registry.acs.intra.env116.shuguang.com/acs/log-controller:0.2.7.0-68ada84-aliyun",
    "ImageUuid": "e05c0de798217637868ef4****",
    "RiskCount": 1,
    "AppName": "csi-provisioner",
    "ContainerId": "B41B3780-337A-472D-B82E-9FD3*****",
    "ImageId": "asdaSdasd",
    "ClusterName": "test****",
    "CreateTimestamp": 1639236844747,
    "AlarmCount": 1,
    "HcCount": 1,
    "HostIp": "192.1.1.130",
    "Pod": "csi-provisioner-564c7989c4-9****",
    "InstanceId": "i-km100o6qy8g*****",
    "ClusterId": "Cccfd68c474454665ace07efce924****",
    "RiskStatus": "YES",
    "Namespace": "shanghai-namespace",
    "VulCount": 0,
    "ImageRepoName": "centos1",
    "NodeInfo": "None",
    "PodIp": "172.29.0.130",
    "AlarmStatus": "NO",
    "RegionId": "cn-***-env116-d01",
    "ImageRepoTag": "0.2.7.0-68ada84-aliyun",
    "HcStatus": "NO",
    "UpdateMark": "None"
  },
  "PageInfo": {
    "TotalCount": 50,
    "PageSize": 20,
    "CurrentPage": 1,
    "Count": 20
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.10. DescribeGroupedContainerInstances

Queries the details about containers by group, such as application, cluster, namespace, or pod.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeGroupedContainerInstances	The operation that you want to perform. Set the value to DescribeGroupedContainerInstances .
Criteria	String	No	[{"name": "riskStatus", "value": "YES"}, {"name": "internetIp", "value": "1.2.3.4"}]	The search conditions for assets. Set the value in the following format: <pre>[{"name": "Name of Condition 1", "value": "Value of Condition 1"}, {"name": "Name of Condition 2", "value": "Value of Condition 2"}, {}, ...]</pre> Supported search conditions include the instance ID, instance name, virtual private cloud (VPC) ID, region, and public IP address. You can call the DescribeCriteria operation to query the supported search conditions.
LogicalExp	String	No	OR	The logical relationship among the search conditions. OR: The logical relationship among the search conditions is OR. AND: The logical relationship among the search conditions is AND.
GroupField	String	No	pod	The type of the container group that you want to query. Valid values: pod appName namespace clusterId

Parameter	Type	Required	Example	Description
FieldValue	String	No	pod	The keyword that is used to search for containers based on the specified group type. The value is automatically identified as a parameter. You must specify this parameter based on the value of the GroupField parameter. • pod: the name of the pod that you want to query. • appName: the name of the application that you want to query. • namespace: the namespace that you want to query. • clusterId: the ID of the cluster that you want to query.
PageSize	Integer	No	20	The number of entries to return on each page.
CurrentPage	Integer	No	1	The number of the page to return.

Response parameters

Parameter	Type	Example	Description
GroupedContainerInstanceList	Array of GroupedContainerInstance		An array that consists of the details about the containers of the specified group.
AlarmCount	Integer	1	The number of alerts.
AppName	String	csi-provisioner	The name of the application.
ClusterId	String	Cccfd68c474454665ace07efce924****	The ID of the cluster to which the container belongs.
ClusterName	String	test***	The name of the cluster to which the container belongs.
ClusterType	String	NotManagedKubernetes	The type of the cluster. Valid values: • ManagedKubernetes • NotManagedKubernetes • PrivateKubernetes

Parameter	Type	Example	Description
CreateTime	Long	1639236844747	The creation time. The value is a UNIX timestamp. Unit: milliseconds.
CusterState	String	running	The status of the cluster.
HostIp	String	47.100.XX.XX	The IP address of the server.
InstanceCount	Integer	2	The number of instances.
Instanceld	String	i- km100o6qy8gidw*** ***	The ID of the instance.
Namespace	String	hangzhou- namespace	The namespace.
Pod	String	csi-provisioner- 564c7989c4-9****	The pod.
PodIp	String	47.100.XX.XX	The IP address of the pod.
RegionId	String	cn-*****-env116-d01	The region ID.
RiskInstanceCount	Integer	5	The number of at-risk instances.
RiskLevel	String	medium	The risk level. Valid values: • high • medium • low
RiskStatus	String	YES	Indicates whether risks were detected. Valid values: • YES • NO

Parameter	Type	Example	Description
VulCount	Integer	2	The number of vulnerabilities.
PageInfo	Struct		The pagination information.
Count	Integer	20	The total number of returned pages.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	35	The total number of entries returned.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeGroupedContainerInstances
&<Common request parameters>
```

Sample success responses

`XML` format

```
<GroupedContainerInstanceList>
  <HostIp>47.100.XX.XX</HostIp>
  <Pod>csi-provisioner-564c7989c4-9****</Pod>
  <InstanceId>i-km100o6qy8gidw*****</InstanceId>
  <ClusterId>Cccfd68c474454665ace07efce924****</ClusterId>
  <ClusterState>running</ClusterState>
  <CreateTime>1639236844747</CreateTime>
  <RiskInstanceCount>5</RiskInstanceCount>
  <ClusterType>NotManagedKubernetes</ClusterType>
  <RiskStatus>YES</RiskStatus>
  <Namespace>hangzhou-namespace</Namespace>
  <AppName>csi-provisioner</AppName>
  <VulCount>2</VulCount>
  <InstanceCount>2</InstanceCount>
  <PodIp>47.100.XX.XX</PodIp>
  <ClusterName>test***</ClusterName>
  <RegionId>cn-****-env116-d01</RegionId>
  <RiskLevel>medium</RiskLevel>
  <AlarmCount>1</AlarmCount>
</GroupedContainerInstanceList>
<PageInfo>
  <TotalCount>35</TotalCount>
  <PageSize>20</PageSize>
  <CurrentPage>1</CurrentPage>
  <Count>20</Count>
</PageInfo>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
```

JSON **format**


```
{
  "GroupedContainerInstanceList": {
    "HostIp": "47.100.XX.XX",
    "Pod": "csi-provisioner-564c7989c4-9****",
    "InstanceId": "i-km100o6qy8gidw*****",
    "ClusterId": "Cccfd68c474454665ace07efce924****",
    "CusterState": "running",
    "CreateTime": 1639236844747,
    "RiskInstanceCount": 5,
    "ClusterType": "NotManagedKubernetes",
    "RiskStatus": "YES",
    "Namespace": "hangzhou-namespace",
    "AppName": "csi-provisioner",
    "VulCount": 2,
    "InstanceCount": 2,
    "PodIp": "47.100.XX.XX",
    "ClusterName": "test****",
    "RegionId": "cn-*****-env116-d01",
    "RiskLevel": "medium",
    "AlarmCount": 1
  },
  "PageInfo": {
    "TotalCount": 35,
    "PageSize": 20,
    "CurrentPage": 1,
    "Count": 20
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.11. DescribeImageCriteria

Queries the search conditions that can be used to obtain images.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeImageCriteria	The operation that you want to perform. Set the value to DescribeImageCriteria .
Value	String	No	demo	The search conditions. Fuzzy match is supported.

Response parameters

Parameter	Type	Example	Description
CriteriaList	Array of Criteria		An array that consists of the search conditions.
Name	String	riskStatus	The name of the search condition.
Type	String	select	The type of the search condition. • input: text box • select: drop-down list
Values	String	NO	The value of the search condition.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageCriteria
&<Common request parameters>
```

Sample success responses

XML format

```
<CriteriaList>
  <Type>select</Type>
  <Values>NO</Values>
  <Name>riskStatus</Name>
</CriteriaList>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
```

JSON format

```
{
  "CriteriaList": {
    "Type": "select",
    "Values": "NO",
    "Name": "riskStatus"
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.12. DescribeImageInstances

Queries the information of images.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeImageInstances	The operation that you want to perform. Set the value to DescribeImageInstances .
Criteria	String	No	<pre>[{"name": "riskStatus", "value": "YES"}, {"name": "internetIp", "value": "1.2.3.4"}]</pre>	The search conditions for assets. Set the value in the following format: [{"name": "Name of Condition 1", "value": "Value of Condition 1"}, {"name": "Name of Condition 2", "value": "Value of Condition 2"}]. Supported search conditions include the instance ID, instance name, virtual private cloud (VPC) ID, region, and public IP address.
LogicalExp	String	No	OR	The logical relationship among the search conditions. Valid values: • OR: The logical relationship among the search conditions is OR. • AND: The logical relationship among the search conditions is AND.
PageSize	Integer	No	20	The number of entries to return on each page.
CurrentPage	Integer	No	1	The number of the page to return.

Response parameters

Parameter	Type	Example	Description
ImageInstanceList	Array of responses		An array that consists of the images.
AlarmCount	Integer	1	The number of alerts.
AlarmStatus	String	YES	Indicates whether alerts were triggered. Valid values: • YES • NO

Parameter	Type	Example	Description
Digest	String	6a5e1031a5858617f7d8a179ead6***	The digest of the image.
Endpoints	String	[]	The endpoint of the image.
HcCount	Integer	0	The number of baseline checks.
HcStatus	String	NO	Indicates whether baseline risks were detected. Valid values: • YES • NO
ImageCreate	String	1234567890123	The timestamp when the image was created. Unit: milliseconds.
ImageId	String	asdaSdasd	The ID of the image.
ImageSize	String	101	The size of the image.
ImageUpdate	String	1639236844747	The timestamp when the image was updated. Unit: milliseconds.
InstanceId	String	i-km100o6qy8gidwn3****	The ID of the instance.
RegionId	String	cn-wulan-env116-d01	The region ID.
RegistryType	String	defaultAcr	The registration type of the image.
Repold	String	crr-vridcl4****	The ID of the image repository.
RepoName	String	centos1	The name of the image repository.
RepoNamespace	String	hangzhou-namespace	The namespace to which the image repository belongs.
RepoType	String	PRIVATE	The type of the image repository.

Parameter	Type	Example	Description
RiskStatus	String	NO	Indicates whether risks were detected. Valid values: • YES • NO
ScaProgress	Integer	1	This parameter is deprecated.
ScaResult	String	None	This parameter is deprecated.
ScaStatus	String	YES	Indicates whether Software Composition Analysis (SCA) vulnerabilities were detected. • YES • NO
Status	String	NORMAL	The status.
Tag	String	0.1	The tag that is added to the image.
Uuid	String	B41B****-337A-472D-B82E-9FD3642B****	The UUID of the asset.
VulCount	Integer	1	The number of vulnerabilities.
VulStatus	String	YES	Indicates whether vulnerabilities were detected. Valid values: • YES • NO
PageInfo	Struct		The pagination information.
Count	Integer	15	The total number of returned pages.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	15	The total number of entries returned.

Parameter	Type	Example	Description
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageInstances
&<Common request parameters>
```

Sample success responses

XML format

```
<ImageInstanceList>
  <VulStatus>YES</VulStatus>
  <ImageSize>101</ImageSize>
  <Endpoints>[]</Endpoints>
  <ScaProgress>1</ScaProgress>
  <ImageId>asdaSdasd</ImageId>
  <ImageUpdate>1639236844747</ImageUpdate>
  <ScaResult>None</ScaResult>
  <AlarmCount>1</AlarmCount>
  <HcCount>0</HcCount>
  <Status>NORMAL</Status>
  <RepoNamespace>hangzhou-namespace</RepoNamespace>
  <RegistryType>defaultAcr</RegistryType>
  <InstanceId>i-km100o6qy8gidwn3****</InstanceId>
  <Digest>6a5e1031a5858617f7d8a179ead6***</Digest>
  <RepoName>centos1</RepoName>
  <RiskStatus>NO</RiskStatus>
  <VulCount>1</VulCount>
  <ScaStatus>YES</ScaStatus>
  <Uuid>B41B***-337A-472D-B82E-9FD3642B****</Uuid>
  <ImageCreate>1234567890123</ImageCreate>
  <RepoType>PRIVATE</RepoType>
  <AlarmStatus>YES</AlarmStatus>
  <Tag>0.1</Tag>
  <RegionId>cn-wulan-env116-d01</RegionId>
  <RepoId>crr-vridcl4****</RepoId>
  <HcStatus>NO</HcStatus>
</ImageInstanceList>
<PageInfo>
  <TotalCount>15</TotalCount>
  <PageSize>20</PageSize>
  <CurrentPage>1</CurrentPage>
  <Count>15</Count>
</PageInfo>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
```

JSON format

```
{
  "ImageInstanceList": {
    "VulStatus": "YES",
    "ImageSize": 101,
    "Endpoints": "[]",
    "ScaProgress": 1,
    "ImageId": "asdaSdasd",
    "ImageUpdate": 1639236844747,
    "ScaResult": "None",
    "AlarmCount": 1,
    "HcCount": 0,
    "Status": "NORMAL",
    "RepoNamespace": "hangzhou-namespace",
    "RegistryType": "defaultAcr",
    "InstanceId": "i-kml00o6qy8gidwn3****",
    "Digest": "6a5e1031a5858617f7d8a179ead6****",
    "RepoName": "centos1",
    "RiskStatus": "NO",
    "VulCount": 1,
    "ScaStatus": "YES",
    "Uuid": "B41B****-337A-472D-B82E-9FD3642B****",
    "ImageCreate": 1234567890123,
    "RepoType": "PRIVATE",
    "AlarmStatus": "YES",
    "Tag": 0.1,
    "RegionId": "cn-wulan-env116-d01",
    "RepoId": "crr-vridcl4****",
    "HcStatus": "NO"
  },
  "PageInfo": {
    "TotalCount": 15,
    "PageSize": 20,
    "CurrentPage": 1,
    "Count": 15
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.13. DescribeImageSecurityScanCount

Queries the results of an image scan.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeImageSecurityScanCount	The operation that you want to perform. Set the value to DescribeImageSecurityScanCount .
RepoRegionId	String	No	cn-*****	The region ID of the image repository.
RepoInstanceId	String	No	cri-datvailb****	The ID of the Container Registry instance.
RepoId	String	No	crr-vridcl4****	The ID of the image repository.
ImageTag	String	No	0.2	The tag that is added to the image.
ImageDigest	String	No	6a5e103187b31a94592a47a5858617f7a179ead61df7606****	The digest of the image.
Dealed	String	No	N	The status of the vulnerabilities that are detected. Valid values: - Y: handled - N: unhandled
ImageUuid	String	No	e05c0de798217637868ef4****	The ID of the image.

Response parameters

Parameter	Type	Example	Description
Data	Struct		The information of image.
ImageBaselineCount	Integer	1	The number of image baselines.
ImageCveVulCount	Integer	2	The number of image system vulnerabilities.
ImageMaliciousFileCount	Integer	3	The number of alerts that are generated for suspicious file changes.

Parameter	Type	Example	Description
ImageScaVulCount	Integer	1	The number of Software Composition Analysis (SCA) vulnerabilities.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageSecurityScanCount
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<Data>
  <ImageBaselineCount>1</ImageBaselineCount>
  <ImageCveVulCount>2</ImageCveVulCount>
  <ImageMaliciousFileCount>3</ImageMaliciousFileCount>
  <ImageScaVulCount>1</ImageScaVulCount>
</Data>
```

JSON format

```
{
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "Data": {
    "ImageBaselineCount": 1,
    "ImageCveVulCount": 2,
    "ImageMaliciousFileCount": 3,
    "ImageScaVulCount": 1
  }
}
```

6.14. GetRegistryScanDayNum

Queries the time setting for image scans.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	GetRegistryScanDayNum	The operation that you want to perform. Set the value to GetRegistryScanDayNum .

Response parameters

Parameter	Type	Example	Description
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.
ScanDayNumConfig	Struct		The settings for image scans.
DayNumList	String	1,3,7,15,30,90,180,365	The valid values of the time setting for image scans.
ScanDayNum	Integer	90	The time setting for scanning images.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=GetRegistryScanDayNum
&<Common request parameters>
```

Sample success responses

XML format

```
<ScanDayNumConfig>
  <DayNumList>1,3,7,15,30,90,180,365</DayNumList>
  <ScanDayNum>90</ScanDayNum>
</ScanDayNumConfig>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
```

JSON format

```
{
  "ScanDayNumConfig": {
    "DayNumList": "1,3,7,15,30,90,180,365",
    "ScanDayNum": 90
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.15. ListPrivateRegistryList

Queries third-party image repositories.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListPrivateRegistryList	The operation that you want to perform. Set the value to ListPrivateRegistryList .
RegistryType	String	No	defaultAcr	The type of the repository. Set the value to defaultAcr .

Response parameters

Parameter	Type	Example	Description
ImageRegistryInfos	Array of ImageRegistryInfo		An array that consists of image repositories.
AliUid	Long	1	The Apsara Stack tenant account.
DomainName	String	192.168.0.1	The domain name of the repository.  Note An IP address is returned only in an internal network.
Id	Long	1	The ID of the image repository.
NetType	Long	1	The type of the network.
ProtocolType	Long	1	The type of the protocol.
RegionId	String	cn-*****-env116-d01	The region ID.
RegistryHostIp	String	47.100.XX.XX	The IP address of the host on which the repository is deployed.

Parameter	Type	Example	Description
RegistryType	String	defaultAcr	The type of the repository. The value is fixed as defaultAcr .
RegistryVersion	String	1	The version of the repository.
Token	String	3fa33eb3-16f9-4ee8-921f-fb558*****	The token.
VpcId	String	112***	The ID of the virtual private cloud (VPC).
WhiteList	String	47.100.XX.XX/24	The whitelist.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ListPrivateRegistryList
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<ImageRegistryInfos>
  <VpcId>112***</VpcId>
  <RegistryType>defaultAcr</RegistryType>
  <DomainName>http://192.168.0.1</DomainName>
  <RegistryHostIp>47.100.XX.XX</RegistryHostIp>
  <ProtocolType>1</ProtocolType>
  <WhiteList>47.100.XX.XX/24</WhiteList>
  <Token>3fa33eb3-16f9-4ee8-921f-fb558*****</Token>
  <RegionId>cn-****-env116-d01</RegionId>
  <Id>1</Id>
  <NetType>1</NetType>
  <RegistryVersion>1</RegistryVersion>
  <AliUid>1</AliUid>
</ImageRegistryInfos>
```

JSON format

```
{
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "ImageRegistryInfos": {
    "VpcId": "112***",
    "RegistryType": "defaultAcr",
    "DomainName": "http://192.168.0.1",
    "RegistryHostIp": "47.100.XX.XX",
    "ProtocolType": 1,
    "WhiteList": "47.100.XX.XX/24",
    "Token": "3fa33eb3-16f9-4ee8-921f-fb558*****",
    "RegionId": "cn-****-env116-d01",
    "Id": 1,
    "NetType": 1,
    "RegistryVersion": 1,
    "AliUid": 1
  }
}
```

6.16. ListPrivateRegistryType

Queries the types of image repositories.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ListPrivateRegistryType	The operation that you want to perform. Set the value to ListPrivateRegistryType .

Response parameters

Parameter	Type	Example	Description
RegistryTypeInfo	Array of RegistryTypeInfo		An array that consists of the information about repository types.
Count	Long	2	The number of repositories of the type.
RegistryType	String	defaultAcr	The type of the repository.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ListPrivateRegistryType
&<Common request parameters>
```

Sample success responses

XML format

```
<RegistryTypeInfo>
  <RegistryType>defaultAcr</RegistryType>
  <Count>2</Count>
</RegistryTypeInfo>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
```

JSON format

```
{
  "RegistryTypeInfo": {
    "RegistryType": "defaultAcr",
    "Count": 2
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.17. DescribeAlarmEventDetail

Queries the details of an exception.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeAlarmEventDetail	The operation that you want to perform. Set the value to DescribeAlarmEventDetail .
AlarmUniqueInfo	String	Yes	asdsafasdfsfa sdf*****	The unique value that identifies the exception.
From	String	Yes	css	The code of the service. Set the value to css .
SourceIp	String	No	47.100.XX.XX	The source IP address of the request.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English

Response parameters

Parameter	Type	Example	Description
Data	Struct		The details of the exception.
AccessCode	String	None	This parameter is deprecated.
AlarmEventAliasName	String	Webshell - Webshell file	The alias of the alert type.
AlarmEventDesc	String	After an attacker accesses a server, the attacker may import malicious shell scripts into scheduled tasks to keep malicious programs running. The scheduled tasks include crontab and systemd.	The description of the alert event.
AlarmUniqueInfo	String	asdajshdklahsdj*****	The unique value that identifies the alert event.
CanBeDealOnline	Boolean	false	Indicates whether the online processing of alert events is supported, such as blocking an alert, adding an alert to the whitelist, and ignoring an alert. Valid values: • true: yes • false: no
CanCancelFault	Boolean	false	Indicates whether you can cancel marking the alert as a false positive. Valid values: • true: yes • false: no

Parameter	Type	Example	Description
CauseDetails	Array of CauseDetail		An array that consists of the details about the exception.
Key	String	html	The format in the exception details. Valid values: text html
Value	Array of Value		An array that consists of exception details.
Name	String	Solution	The name of the field that displays tracing information.
Type	String	html	The format of the field that displays tracing information. Valid values: text html
Value	String	[]	The value of the field that displays tracing information.
DataSource	String	console	The source of data.
Dealed	Boolean	false	The status of the exception. Valid values: true: handled false: unhandled
EndTime	Long	1639236844747	The end of the time range during which the exception was handled. The value is a UNIX timestamp. Unit: milliseconds.
HasTraceInfo	Boolean	false	This parameter is deprecated.
InstanceName	String	worker-k8s-for-cs-cb9218d50728c470fb7dfbc16577a2673	The name of the instance.
InternetIp	String	47.100.XX.XX	The public IP address.

Parameter	Type	Example	Description
IntranetIp	String	192.168.0.1	The private IP address.
Level	String	suspicious	The severity of the exception. Valid values: • serious • suspicious • remind
Solution	String	Check the malicious URLs that are listed in the alert. Check the directory for malicious file downloads. Stop the malicious processes that are running. If you trust the processes, mark the alert as a false positive in the console, and submit a ticket to notify security engineers.	The solution to the exception.
StartTime	Long	1234567890123	The start of the time range during which the exception was handled. The value is a UNIX timestamp. Unit: milliseconds.

Parameter	Type	Example	Description
Type	String	Webshell	The type of the alert event. Valid values: • Suspicious process • Webshell • Unusual logon • Exception • Sensitive file tampering • Malicious process • Suspicious network connection • Other. • Abnormal account. • Application intrusion event • Cloud threat detection • Precise defense • Application whitelist. • Persistent webshell • Web application threat detection • Malicious script • Threat intelligence. • Malicious network activity
Uuid	String	B41B3780-337A-472D-B82E-9FD364*****	The UUID of the asset.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAlarmEventDetail
&AlarmUniqueInfo=asdsafasdfsfasdf*****
&From=css
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<Data>
  <CanCancelFault>false</CanCancelFault>
  <EndTime>1639236844747</EndTime>
  <StartTime>1234567890123</StartTime>
  <AccessCode>None</AccessCode>
  <Dealed>false</Dealed>
  <HasTraceInfo>false</HasTraceInfo>
  <IntranetIp>1.1.1.1</IntranetIp>
  <DataSource>console</DataSource>
  <InstanceName>worker-k8s-for-cs-cb9218d50728c470fb7dfbc16577a2673</InstanceName>
  <CanBeDealOnLine>false</CanBeDealOnLine>
  <Type>Webshell</Type>
  <Uuid>B41B3780-337A-472D-B82E-9FD3642B9350</Uuid>
  <InternetIp>1.1.1.1</InternetIp>
  <AlarmUniqueInfo>asdajshdklahsdjka</AlarmUniqueInfo>
  <AlarmEventDesc>After an attacker accesses a server, the attacker may import malicious
  shell scripts into scheduled tasks to keep malicious programs running. The scheduled tasks
  include crontab and systemd. </AlarmEventDesc>
  <AlarmEventAliasName>Webshell - Webshell file</AlarmEventAliasName>
  <Level>suspicious</Level>
  <Solution>Check the malicious URLs that are listed in the alert. Check the directory fo
  r malicious file downloads. Stop the malicious processes that are running. If you trust the
  processes, mark the alert as a false positive in the console, and submit a ticket to notify
  security engineers. </Solution>
  <CauseDetails>
    <Key>html</Key>
    <Value>
      <Type>html</Type>
      <Value>[]</Value>
      <Name>Solution</Name>
    </Value>
  </CauseDetails>
</Data>
```

JSON format

```
{
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "Data": {
    "CanCancelFault": false,
    "EndTime": 1639236844747,
    "StartTime": 1234567890123,
    "AccessCode": "None",
    "Dealed": false,
    "HasTraceInfo": false,
    "IntranetIp": "1.1.1.1",
    "DataSource": "console",
    "InstanceName": "worker-k8s-for-cs-cb9218d50728c470fb7dfbc16577a2673",
    "CanBeDealOnLine": false,
    "Type": "Webshell",
    "Uuid": "B41B3780-337A-472D-B82E-9FD3642B9350",
    "InternetIp": "1.1.1.1",
    "AlarmUniqueInfo": "asdajshdklahsdjkashdjka",
    "AlarmEventDesc": "After an attacker accesses a server, the attacker may import malicious shell scripts into scheduled tasks to keep malicious programs running. The scheduled tasks include crontab and systemd.",
    "AlarmEventAliasName": "Webshell - Webshell file",
    "Level": "suspicious",
    "Solution": "Check the malicious URLs that are listed in the alert. Check the directory for malicious file downloads. Stop the malicious processes that are running. If you trust the processes, mark the alert as a false positive in the console, and submit a ticket to notify security engineers.",
    "CauseDetails": {
      "Key": "html",
      "Value": {
        "Type": "html",
        "Value": "[]",
        "Name": "Solution"
      }
    }
  }
}
```

6.18. DescribeNsasSuspEventType

Queries the types of alert events.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeNsasSuspEventType	The operation that you want to perform. Set the value to DescribeNsasSuspEventType .
SourceIp	String	No	47.100.XX.XX	The source IP address of the request.

Parameter	Type	Required	Example	Description
Remark	String	No	test	The conditions for fuzzy search.
Name	String	No	Threat Intelligence	The name of the alert event.
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English
From	String	No	css	The code of the service. Set the value to css .
Uuids	String	No	4b092975242bea7fa4af*****,07282975242bea7fa4af*****	The UUIDs . Separate multiple UUIDs with commas (,).
ClusterId	String	No	cb9218d50728c470fb7dfbc1657****	The ID of the cluster.
ContainerFieldName	String	No	containerId	The type of the search condition that is used to query containers.
ContainerFieldValue	String	No	4b092975242bea7fa4af8515057f660faf2b285bc1693fd4cb0e7bfac****	The search term that is used to query containers.
TargetType	String	No	containerId	The information that is used to query the types of alert events.

Response parameters

Parameter	Type	Example	Description
EventTypes	Array of Data		An array that consists of the types of alert events.
Name	String	Threat Intelligence	The name of the exception.

Parameter	Type	Example	Description
SuspEventCount	Integer	12	The number of exceptions.
Type	String	Threat Intelligence	The type of the exception.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeNsasSuspEventType
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<EventTypes>
  <Type>Threat Intelligence</Type>
  <SuspEventCount>12</SuspEventCount>
  <Name>Threat Intelligence</Name>
</EventTypes>
```

JSON format

```
{
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "EventTypes": {
    "Type": "Threat Intelligence",
    "SuspEventCount": 12,
    "Name": "Threat Intelligence"
  }
}
```

6.19. DescribeSecurityEventOperations

Queries the operations that are performed on alert events.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSecurityEventOperations	The operation that you want to perform. Set the value to DescribeSecurityEventOperations .
SourceIp	String	No	47.100.XX.XX	The source IP address of the request.
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English
SecurityEventId	Long	No	1	The ID of the alert event.

Response parameters

Parameter	Type	Example	Description
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.
SecurityEventOperationsResponse	Array of SecurityEventOperation		An array that consists of the operations performed on alert events.
MarkField	Array of MarkField		This parameter is deprecated.
FiledAliasName	String	None	This parameter is deprecated.
FiledName	String	None	This parameter is deprecated.
MarkMisType	String	None	This parameter is deprecated.
MarkMisValue	String	None	This parameter is deprecated.
SupportedMisType	List	None	This parameter is deprecated.
MarkFieldsSource	Array of SecurityEventOperation		An array that consists of the information of the alert events.

Parameter	Type	Example	Description
FiledAliasName	String	Process path	The name of the alert.
FiledName	String	proc_path	The key of the field.
MarkMisValue	String	/usr/bin/ps	The operation instruction.
SupportedMisType	List	["contains", "notContains", "regex", "strEqual", "strNotEqual"]	The operations that can be performed.
OperationCode	String	ignore	The operation performed on the alert event. Valid values: • ignore: ignores the alerts. • advance_mark_mis_info: adds the alert to the whitelist. • manual_handled: manually handled.
OperationParams	String	demo	The parameters of the operation.
UserCanOperate	Boolean	false	Indicates whether you can handle the alert. Valid values: • true: yes • false: no

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSecurityEventOperations
&<Common request parameters>
```

Sample success responses

XML format


```
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<SecurityEventOperationsResponse>
  <OperationParams>demo</OperationParams>
  <OperationCode>ignore</OperationCode>
  <UserCanOperate>false</UserCanOperate>
  <MarkField>
    <FileName>None</FileName>
    <MarkMisValue>None</MarkMisValue>
    <MarkMisType>None</MarkMisType>
    <FiledAliasName>None</FiledAliasName>
    <SupportedMisType>None</SupportedMisType>
  </MarkField>
  <MarkFieldsSource>
    <FileName>proc_path</FileName>
    <MarkMisValue>/usr/bin/ps</MarkMisValue>
    <FiledAliasName>Process path</FiledAliasName>
    <SupportedMisType>["contains", "notContains", "regex", "strEqual", "strNotEqual"]</SupportedMisType>
  </MarkFieldsSource>
</SecurityEventOperationsResponse>
```

JSON format

```
{
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "SecurityEventOperationsResponse": {
    "OperationParams": "demo",
    "OperationCode": "ignore",
    "UserCanOperate": false,
    "MarkField": {
      "FileName": "None",
      "MarkMisValue": "None",
      "MarkMisType": "None",
      "FiledAliasName": "None",
      "SupportedMisType": "None"
    },
    "MarkFieldsSource": {
      "FileName": "proc_path",
      "MarkMisValue": "/usr/bin/ps",
      "FiledAliasName": "Process path",
      "SupportedMisType": "[\"contains\", \"notContains\", \"regex\", \"strEqual\", \"strNotEqual\"]"
    }
  }
}
```

6.20. DescribeSuspEvents

Queries exceptions.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSuspEvents	The operation that you want to perform. Set the value to DescribeSuspEvents .
SourceIp	String	No	47.100.XX.XX	The source IP address of the request.
Dealed	String	No	Y	The status of the exception. Valid values: N: unhandled Y: handled
Name	String	No	ecs-xxx	The name of the exception or the hostname of the server.
Levels	String	No	serious	The severity of the exception. Separate multiple severities with commas (,). Valid values: serious suspicious remind
ParentEventTypes	String	No	Webshell	The type of the alert with which the exception is associated.
Remark	String	No	test	The IP address or hostname of the server.
Status	String	No	None	This parameter is deprecated.
PageSize	String	No	20	The number of entries to return on each page.
CurrentPage	String	No	1	The number of the page to return.
Lang	String	No	zh	The language of the content within the request and response. Valid values: zh: Chinese en: English

Parameter	Type	Required	Example	Description
AlarmUniqueInfo	String	No	asdhlashdlkah*** ****	The unique identifier of the alert event.
UniqueInfo	String	No	a097975445d891 ddf86a3f56*****	The unique information.
From	String	No	css	The code of the service. Set the value to css .
Source	String	No	None	This parameter is deprecated.
GroupId	Long	No	1	This parameter is deprecated.
Uuids	String	No	None	This parameter is deprecated.
OperateErrorCodeList.N	RepeatList	No	[]	The error codes.
ClusterId	String	No	asdjashdkashdkj* ***	The ID of the cluster to which the container belongs.
ContainerFieldName	String	No	appName	The key that is used to query the container.
ContainerFieldValue	String	No	nginx-ingress-controller	The value that is used to query the container.
TargetType	String	No	containerId	The container that matches both the value of ContainerFieldValue and the value of ContainerFieldName .

Response parameters

Parameter	Type	Example	Description
Count	Integer	20	The total number of returned pages.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.

Parameter	Type	Example	Description
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.
SuspEvents	Array of WarningSummary		The content of the exception.
Advanced	Boolean	false	Indicates whether the Advanced edition is used. • true: yes • false: no
AlarmEventName	String	DDoS trojan	The name of the exception.
AlarmEventNameDisplay	String	None	This parameter is deprecated.
AlarmEventType	String	Malicious process	The type of the alert event. Valid values: • Suspicious process • Webshell • Unusual logon • Exception • Sensitive file tampering • Malicious process • Suspicious network connection • Other • Abnormal account • Application intrusion event • Cloud threat detection • Precise defense • Application whitelist • Persistent webshell • Web application threat detection • Malicious script • Threat intelligence • Malicious network activity
AlarmEventTypeDisplay	String	None	This parameter is deprecated.
AlarmUniqueInfo	String	asdhkashdkash****	The unique identifier of the alert event.

Parameter	Type	Example	Description
AppName	String	app1	The name of the application.
AssetType	Integer	0	The type of the asset. Valid values: • 0: Elastic Compute Service (ECS) instance • 1: Server Load Balancer (SLB) instance • 2: NAT gateway • 3: ApsaraDB RDS database • 4: ApsaraDB for MongoDB database • 6: container image • 7: container
AutoBreaking	Boolean	false	Indicates whether the exception is automatically blocked. • true: yes • false: no
CanBeDealOnline	Boolean	false	Indicates whether the online processing of alert events is supported, such as blocking an alert, adding an alert to the whitelist, and ignoring an alert. Valid values: • true: yes • false: no
CanCancelFault	Boolean	false	Indicates whether you can cancel marking the alert as a false positive. Valid values: • true: yes • false: no
ContainHwMode	Boolean	false	This parameter is deprecated.
ContainerId	String	asdaksDaksh*****	The ID of the container.
ContainerImageId	String	asdalsdka*****	The ID of the image to which the container belongs.
ContainerImageName	String	name1	The name of the image to which the container belongs.

Parameter	Type	Example	Description
DataSource	String	aegis_suspicious_***	The data source on which the exception is detected.
Desc	String	The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.	The description of the exception.
Details	Array of QuaraFile		The details of the exception.
InfoType	String	None	This parameter is deprecated.
Name	String	\${suspicious.sp.rs.description}	The keyword that identifies the exception for internationalization.
NameDisplay	String	Event description	The display name of the exception.
Type	String	text	The format in which the details of the exception are displayed. Valid values: • text • html
Value	String	The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.	The detailed content of the exception.

Parameter	Type	Example	Description
ValueDisplay	String	The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.	The detailed content that is displayed.
EventNotes	Array of EventNote		This parameter is deprecated.
Note	String	None	This parameter is deprecated.
Noteld	Long	1	This parameter is deprecated.
NoteTime	String	None	This parameter is deprecated.
EventStatus	Integer	1	The status of the alert event. Valid values: • 1: pending handling • 2: ignored • 4: confirmed • 8: marked as a false positive • 16: handling • 32: handled • 64: expired

Parameter	Type	Example	Description
EventSubType	String	Suspicious process	The type of the alert event. Valid values: • Suspicious process • Webshell • Unusual logon • Exception • Sensitive file tampering • Malicious process • Suspicious network connection • Other • Abnormal account • Application intrusion event • Cloud threat detection • Precise defense • Application whitelist • Persistent webshell • Web application threat detection • Malicious script • Threat intelligence • Malicious network activity
HasTraceInfo	Boolean	false	This parameter is deprecated.
Id	Long	1	The ID.
InstanceId	String	i-asdasdjhkh*****	The ID of the instance.
InstanceName	String	worker-k8s-for-cs-cb9218d50728c470fb7dfbc16577a2673	The name of the instance.
InternetIp	String	47.100.XX.XX	The public IP address.
IntranetIp	String	192.168.0.1	The private IP address.
K8sClusterId	String	asdasdkah*****	The ID of the Kubernetes cluster.
K8sClusterName	String	cqqtesttest	The name of the Kubernetes cluster.

Parameter	Type	Example	Description
K8sNamespace	String	hangzhou-namespace	The namespace of the Kubernetes cluster.
K8sNodeId	String	nod*****	The ID of the node in the Kubernetes cluster.
K8sNodeName	String	nodeName1	The name of the node in the Kubernetes cluster.
K8sPodName	String	PodName1	The name of the pod in the Kubernetes cluster.
LastTime	String	2022-01-06 18:41:24	The time when the exception was last updated. The time is in the yyyy-MM-dd HH:mm:ss format.
LastTimeStamp	Long	1234567890123	The timestamp when the exception was last updated. The value is a UNIX timestamp. Unit: milliseconds.
Level	String	serious	The severity of the exception. • serious • suspicious • remind
LogAnalysis	String	None	This parameter is deprecated.
LogFromTime	Long	1	This parameter is deprecated.
LogToTime	Long	1	This parameter is deprecated.
MarkMisRules	String	None	This parameter is deprecated.
Name	String	\${suspicious.sp.rs.description}	The keyword that identifies the exception for internationalization.
OccurrenceTime	String	2022-01-06 18:41:24	The time when the exception was detected. The time is in the yyyy-MM-dd HH:mm:ss format.

Parameter	Type	Example	Description
OccurrenceTimeStamp	Long	1234567890123	The timestamp when the exception was detected. The value is a UNIX timestamp. Unit: milliseconds.
OperateErrorCode	String	quara.Succes	The handling result of the exception.
OperateMsg	String	succes	The message that describes the handling result of the exception.
OperateTime	Long	1234567890123	The time when the exception was handled. The value is a UNIX timestamp. Unit: milliseconds.
RegionId	String	cn-*****-env116-d01	The region ID.
SaleVersion	String	None	This parameter is deprecated.
SecurityEventIds	String	1212***	The ID of the exception.
Stages	String	None	This parameter is deprecated.
TraceBackInfo	String	None	This parameter is deprecated.
UniqueInfo	String	asdlykhaskl*****	The unique information.
Uuid	String	B41B3780-337A-472D-B82E-9FD364*****	The UUID of the asset.
TotalCount	Integer	35	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSusEvents
&<Common request parameters>
```

Sample success responses

XML format

```

<TotalCount>35</TotalCount>
<PageSize>20</PageSize>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<CurrentPage>1</CurrentPage>
<Count>20</Count>
<SuspEvents>
  <K8sNodeId>nod*****</K8sNodeId>
  <K8sNodeName>nodeName1</K8sNodeName>
  <ContainHwMode>false</ContainHwMode>
  <HasTraceInfo>false</HasTraceInfo>
  <IntranetIp>192.168.0.1</IntranetIp>
  <K8sClusterId>asdasdkah*****</K8sClusterId>
  <Name>${suspicious.sp.rs.description}</Name>
  <K8sNamespace>hangzhou-namespace</K8sNamespace>
  <Desc>The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers. </Desc>
  <TraceBackInfo>None</TraceBackInfo>
  <InternetIp>47.100.XX.XX</InternetIp>
  <ContainerId>asdaksDaksh*****</ContainerId>
  <AlarmEventType>Malicious process</AlarmEventType>
  <LogToTime>1</LogToTime>
  <AlarmEventNameDisplay>None</AlarmEventNameDisplay>
  <UniqueInfo>asdIjkhaskl*****</UniqueInfo>
  <CanCancelFault>false</CanCancelFault>
  <InstanceId>i-asdasdjhkh*****</InstanceId>
  <LogFromTime>1</LogFromTime>
  <SaleVersion>None</SaleVersion>
  <ContainerImageId>asdalsdka*****</ContainerImageId>
  <DataSource>aegis_suspicious_***</DataSource>
  <LogAnalysis>None</LogAnalysis>
  <InstanceName>worker-k8s-for-cs-cb9218d50728c470fb7dfbc16577a2673</InstanceName>
  <OccurrenceTime>2022-01-06 18:41:24</OccurrenceTime>
  <OperateTime>1234567890123</OperateTime>
  <CanBeDealOnLine>false</CanBeDealOnLine>
  <K8sClusterName>cqqttesttest</K8sClusterName>
  <ContainerImageName>name1</ContainerImageName>
  <AlarmUniqueInfo>asdhkashdkash****</AlarmUniqueInfo>
  <OccurrenceTimeStamp>1234567890123</OccurrenceTimeStamp>
  <Level>serious</Level>
  <Id>1</Id>
  <Advanced>false</Advanced>
  <OperateErrorCode>quara.Succes</OperateErrorCode>
  <AlarmEventName>DDoS trojan</AlarmEventName>
  <SecurityEventIds>1212***</SecurityEventIds>
  <EventStatus>1</EventStatus>
  <EventSubType>Suspicious process</EventSubType>
  <AppName>app1</AppName>
  <LastTimeStamp>1234567890123</LastTimeStamp>
  <AlarmEventTypeDisplay>None</AlarmEventTypeDisplay>
  <Stages>None</Stages>

```

```

<MarkMisRules>None</MarkMisRules>
<K8sPodName>PodName1</K8sPodName>
<OperateMsg>succes</OperateMsg>
<AssetType>0</AssetType>
<Uuid>B41B3780-337A-472D-B82E-9FD364*****</Uuid>
<AutoBreaking>>false</AutoBreaking>
<RegionId>cn-*****-env116-d01</RegionId>
<LastTime>2022-01-06 18:41:24</LastTime>
<Details>
  <Type>text</Type>
  <Value>The threat detection model detected that the command line data of a process
on your server was highly suspicious. This may be related to trojans, viruses, or attackers
. </Value>
  <ValueDisplay>The threat detection model detected that the command line data of a p
rocess on your server was highly suspicious. This may be related to trojans, viruses, or at
tackers. </ValueDisplay>
  <InfoType>None</InfoType>
  <NameDisplay>Event description</NameDisplay>
  <Name>${suspicious.sp.rs.description}</Name>
</Details>
<EventNotes>
  <NoteId>1</NoteId>
  <Note>None</Note>
  <NoteTime>None</NoteTime>
</EventNotes>
</SuspEvents>

```

JSON format

```

{
  "TotalCount": 35,
  "PageSize": 20,
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "CurrentPage": 1,
  "Count": 20,
  "SuspEvents": {
    "K8sNodeId": "nod*****",
    "K8sNodeName": "nodeName1",
    "ContainHwMode": false,
    "HasTraceInfo": false,
    "IntranetIp": "192.168.0.1",
    "K8sClusterId": "asdasdkah*****",
    "Name": "${suspicious.sp.rs.description}",
    "K8sNamespace": "hangzhou-namesapce",
    "Desc": "The threat detection model detected that the command line data of a proces
s on your server was highly suspicious. This may be related to trojans, viruses, or attacke
rs.",
    "TraceBackInfo": "None",
    "InternetIp": "47.100.XX.XX",
    "ContainerId": "asdaksDaksh*****",
    "AlarmEventType": "Malicious process",
    "LogToTime": 1,
    "AlarmEventNameDisplay": "None",
    ...
  }
}

```

```

    "UniqueInfo": "asdljkhaskl*****",
    "CanCancelFault": false,
    "InstanceId": "i-asdasdjhkh*****",
    "LogFromTime": 1,
    "SaleVersion": "None",
    "ContainerImageId": "asdalsdka*****",
    "DataSource": "aegis_suspicious_***",
    "LogAnalysis": "None",
    "InstanceName": "worker-k8s-for-cs-cb9218d50728c470fb7dfbc16577a2673",
    "OccurrenceTime": "2022-01-06 18:41:24",
    "OperateTime": 1234567890123,
    "CanBeDealOnLine": false,
    "K8sClusterName": "cqqttesttest",
    "ContainerImageName": "name1",
    "AlarmUniqueInfo": "asdhkashdkash****",
    "OccurrenceTimeStamp": 1234567890123,
    "Level": "serious",
    "Id": 1,
    "Advanced": false,
    "OperateErrorCode": "quara.Succes",
    "AlarmEventName": "DDoS trojan",
    "SecurityEventIds": "1212****",
    "EventStatus": 1,
    "EventSubType": "Suspicious process",
    "AppName": "appl",
    "LastTimeStamp": 1234567890123,
    "AlarmEventTypeDisplay": "None",
    "Stages": "None",
    "MarkMisRules": "None",
    "K8sPodName": "PodName1",
    "OperateMsg": "succes",
    "AssetType": 0,
    "Uuid": "B41B3780-337A-472D-B82E-9FD364*****",
    "AutoBreaking": false,
    "RegionId": "cn-****-env116-d01",
    "LastTime": "2022-01-06 18:41:24",
    "Details": {
      "Type": "text",
      "Value": "The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.",
      "ValueDisplay": "The threat detection model detected that the command line data of a process on your server was highly suspicious. This may be related to trojans, viruses, or attackers.",
      "InfoType": "None",
      "NameDisplay": "Event description",
      "Name": "${suspicious.sp.rs.description}"
    },
    "EventNotes": {
      "NoteId": 1,
      "Note": "None",
      "NoteTime": "None"
    }
  }
}

```

6.21. DescribeEventLevelCount

Queries the severities of alerts.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeEventLevelCount	The operation that you want to perform. Set the value to DescribeEventLevelCount .
SourceIp	String	No	47.100.XX.XX	The source IP address of the request.
Type	String	No	alarm	The type of the query. Set the value to alarm .
From	String	No	css	The code of the service. Set the value to css .
ClusterId	String	No	Cccfd68c474454665ace07efce924**	The ID of the cluster to which the container belongs.
ContainerFieldName	String	No	containerId	The key that is used to query the container.
ContainerFieldValue	String	No	4b092975242bea7fa4af8515057f660faf2b285bc1693fd4cb0e7bfac***	The value that is used to query the container.
TargetType	String	No	containerId	The container that matches both the value of ContainerFieldName and the value of ContainerFieldValue .

Response parameters

Parameter	Type	Example	Description
EventLevels	Struct		The alerts.

Parameter	Type	Example	Description
Remind	Integer	1	The number of alerts that have the remind severity.
Serious	Integer	2	The number of alerts that have the serious severity.
Suspicious	Integer	3	The number of alerts that have the suspicious severity.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeEventLevelCount
&<Common request parameters>
```

Sample success responses

XML format

```
<EventLevels>
  <Serious>2</Serious>
  <Suspicious>3</Suspicious>
  <Remind>1</Remind>
</EventLevels>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
```

JSON format

```
{
  "EventLevels": {
    "Serious": 2,
    "Suspicious": 3,
    "Remind": 1
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}
```

6.22. DescribeConcernNecessity

Queries the severities of alert events.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeConcernNecessity	The operation that you want to perform. Set the value to DescribeConcernNecessity .
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English

Response parameters

Parameter	Type	Example	Description
ConcernNecessity	List	["nntf", "later", "asap"]	The severities of alert events. • nntf: low • later: medium • asap: high
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeConcernNecessity
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<ConcernNecessity>["nntf", "later", "asap"]</ConcernNecessity>
```

JSON format

```
{
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "ConcernNecessity": ["nntf", "later", "asap"]
}
```

6.23. DescribeGroupedVul

Queries vulnerabilities by group.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeGroupedVul	The operation that you want to perform. Set the value to DescribeGroupedVul .
SourceIp	String	No	47.100.XX.XX	The source IP address of the request.
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English
Type	String	No	cve	The type of the vulnerability. Valid values: • CVE: image system vulnerabilities • SCA: image application vulnerabilities
GroupId	String	No	None	This parameter is deprecated.
CveId	String	No	q3w4er12***	The Common Vulnerabilities and Exposures (CVE) ID of the vulnerability.
Uuids	String	No	uuid1,uuid2	The UUID of the asset. Separate multiple UUIDs with commas (,).
Name	String	No	debian:10:CVE-2019-9893	The name of the vulnerability.
AliasName	String	No	DSA-2019 libseccomp security vulnerability	The alias of the vulnerability.
PatchId	Long	No	1	This parameter is deprecated.
Level	String	No	None	This parameter is deprecated.

Parameter	Type	Required	Example	Description
LastTsStart	Long	No	1	This parameter is deprecated.
LastTsEnd	Long	No	1	This parameter is deprecated.
StatusList	String	No	None	This parameter is deprecated.
OrderBy	String	No	None	This parameter is deprecated.
Direction	String	No	None	This parameter is deprecated.
Necessity	String	No	later,nntf,asap	The severity of the vulnerability. Separate multiple severities with commas (,). Valid values: • serious • suspicious • remind
Dealed	String	No	Y	The status of the vulnerability. Valid values: • N: unhandled • Y: handled
CreateTsStart	Long	No	1	This parameter is deprecated.
CreateTsEnd	Long	No	1	This parameter is deprecated.
CurrentPage	Integer	No	1	The number of the page to return.
PageSize	Integer	No	20	The number of entries to return on each page.
SearchTags	String	No	None	This parameter is deprecated.

Parameter	Type	Required	Example	Description
AttachTypes	String	No	sca	The type of the vulnerability. Valid values: • CVE: image system vulnerabilities • SCA: image application vulnerabilities
ContainerFieldName	String	No	containerId	The key that is used to query the container.
ContainerFieldValue	String	No	4b092975242bea7fa4af85150*****faf2b285bc1693fd4cb0e7bfac300f5c7	The value that is used to query the container.
TargetType	String	No	containerId	The container that matches both the value of ContainerFieldName and the value of ContainerFieldValue .
ClusterId	String	No	cs-adasd	The ID of the cluster to which the container belongs.
MinScore	Integer	No	1	This parameter is deprecated.
VpcInstanceId	String	No	None	This parameter is deprecated.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
GroupedVulItems	Array of GroupedVulItem		An array that consists of the vulnerabilities by group.
AliasName	String	DSA-2019 libseccomp security vulnerability	The alias of the vulnerability.
AsapCount	Integer	1	The number of vulnerabilities that have the high priority.

Parameter	Type	Example	Description
GmtLast	Long	1234567890123	The timestamp when the last scan was performed. Unit: milliseconds.
HandledCount	Integer	1	The number of handled vulnerabilities.
LaterCount	Integer	2	The number of vulnerabilities that have the medium priority.
Name	String	debian:10:CVE-2019-9893	The name of the vulnerability.
NntfCount	Integer	4	The number of vulnerabilities that have the low risks.
Status	Integer	0	The status of the vulnerability. Valid values: • 0: unhandled • 1: handled • 2: being verified • 3: added to the whitelist
Tags	String	Code execution	The tag that is added to the vulnerability. Valid values: • Restart required • Remote exploitation • Exploit exists • Exploitable • Privilege escalation • Code execution
TotalFixCount	Long	233	The total number of fixed vulnerabilities.
Type	String	cve	Valid values: • CVE: image system vulnerabilities • SCA: image application vulnerabilities
PageSize	Integer	20	The number of entries returned per page.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Parameter	Type	Example	Description
TotalCount	Integer	25	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeGroupedVul
&<Common request parameters>
```

Sample success responses

XML format

```
<TotalCount>25</TotalCount>
<PageSize>20</PageSize>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<CurrentPage>1</CurrentPage>
<GroupedVulItems>
  <Status>0</Status>
  <Type>cve</Type>
  <LaterCount>2</LaterCount>
  <GmtLast>1234567890123</GmtLast>
  <HandledCount>1</HandledCount>
  <AliasName>DSA-2019 libseccomp security vulnerability</AliasName>
  <AsapCount>1</AsapCount>
  <TotalFixCount>233</TotalFixCount>
  <NntfCount>4</NntfCount>
  <Tags>Code execution</Tags>
  <Name>debian:10:CVE-2019-9893</Name>
</GroupedVulItems>
```

JSON format

```
{
  "TotalCount": 25,
  "PageSize": 20,
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "CurrentPage": 1,
  "GroupedVulItems": {
    "Status": 0,
    "Type": "cve",
    "LaterCount": 2,
    "GmtLast": 1234567890123,
    "HandledCount": 1,
    "AliasName": "DSA-2019 libseccomp security vulnerability",
    "AsapCount": 1,
    "TotalFixCount": 233,
    "NntfCount": 4,
    "Tags": "Code execution",
    "Name": "debian:10:CVE-2019-9893"
  }
}
```

6.24. DescribeImageGroupedVulList

Queries image vulnerabilities by group.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeImageGroupedVulList	The operation that you want to perform. Set the value to DescribeImageGroupedVulList.
Type	String	No	sca	The type of the vulnerability that you want to query. Valid values: CVE: image system vulnerability SCA: image application vulnerability
GroupId	String	No	12345***	The ID of the asset group.
CveId	String	No	CVE-2017-15420	The Common Vulnerabilities and Exposures (CVE) ID of the vulnerability.
Uuids	String	No	uuid1,uuid2,uuid3	The IDs of assets. Separate multiple IDs with commas (,).

Parameter	Type	Required	Example	Description
AliasName	String	No	DSA-2019 libseccomp security vulnerability	The alias of the vulnerability.
PatchId	Long	No	1	The ID of the patch that is used to fix the vulnerability.
Necessity	String	No	later,nntf,asap	The priority to fix the vulnerability. Separate multiple priorities with commas (,). Valid values: • asap: high • later: medium • nntf: low
CurrentPage	Integer	No	1	The number of the page to return.
PageSize	Integer	No	20	The number of entries to return on each page.
RepoRegionId	String	No	cn-*****	The region ID of the image repository.
RepoInstanceId	String	No	cri-adasdadsda***	The ID of the container image.
RepoId	String	No	crr-dadsdafs****	The ID of the image repository.
RepoName	String	No	centos1	The name of the image repository.
RepoNamespace	String	No	hangzhou-namespace	The namespace to which the image repository belongs.
ImageTag	String	No	0.2	The tag that is added to the image.
ImageDigest	String	No	6a5e103187b31a94592a47a5858617f7a179ead61df7606*****	The digest of the image.
ImageLayer	String	No	27213ad375b53628dd152a5ca****	The information about the image layer.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English
IsLatest	Integer	No	0	Specifies whether to query the vulnerabilities in the latest images. If you do not specify this parameter, the vulnerabilities of all images are queried. Valid values: • 0: no • 1: yes

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
GroupedVulItems	Array of GroupedVulItem		An array that consists of the vulnerabilities by group.
AliasName	String	DSA-2019 libseccomp security vulnerability	The alias of the vulnerability.
AsapCount	Integer	1	The number of vulnerabilities that have the high priority.
GmtLast	Long	1234567890123	The time when the status of the image vulnerability is last modified. The value is a UNIX timestamp. Unit: milliseconds.
LastScanTime	Long	1234567890123	The last scan time. The value is a UNIX timestamp. Unit: milliseconds.
LaterCount	Integer	2	The number of vulnerabilities that have the medium priority.
Name	String	debian:10: CVE-2019-9893	The name of the vulnerability.

Parameter	Type	Example	Description
NntfCount	Integer	3	The number of vulnerabilities that have the low priority.
Status	Integer	0	The status of the vulnerability. Valid values: • 0: unhandled • 1: handled • 2: being verified • 3: added to the whitelist
Tags	String	Code execution	The tag that is added to the vulnerability. Valid values: • Restart required • Remote exploitation • Exploit exists • Exploitable • Privilege escalation • Code execution
Type	String	sca	The type of the vulnerability. Valid values: • CVE: image system vulnerability • SCA: image application vulnerability
PageSize	Integer	20	The number of entries returned per page.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.
TotalCount	Integer	27	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageGroupedVulList
&<Common request parameters>
```

Sample success responses

XML format

```

<TotalCount>27</TotalCount>
<PageSize>20</PageSize>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<CurrentPage>1</CurrentPage>
<GroupedVulItems>
  <Status>0</Status>
  <Type>sca</Type>
  <LaterCount>2</LaterCount>
  <GmtLast>1234567890123</GmtLast>
  <AliasName>DSA-2019 libseccomp security vulnerability</AliasName>
  <AsapCount>1</AsapCount>
  <LastScanTime>1234567890123</LastScanTime>
  <NntfCount>3</NntfCount>
  <Tags>Code execution</Tags>
  <Name>debian:10:CVE-2019-9893</Name>
</GroupedVulItems>

```

JSON **format**

```

{
  "TotalCount": 27,
  "PageSize": 20,
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "CurrentPage": 1,
  "GroupedVulItems": {
    "Status": 0,
    "Type": "sca",
    "LaterCount": 2,
    "GmtLast": 1234567890123,
    "AliasName": "DSA-2019 libseccomp security vulnerability",
    "AsapCount": 1,
    "LastScanTime": 1234567890123,
    "NntfCount": 3,
    "Tags": "Code execution",
    "Name": "debian:10:CVE-2019-9893"
  }
}

```

6.25. DescribeImageVulList

Queries image vulnerabilities.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeImageVulList	The operation that you want to perform. Set the value to DescribeImageVulList .

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English
Type	String	No	cve	The type of the vulnerability. Valid values: • CVE: image system vulnerability • SCA: image application vulnerability
Uuids	String	No	uuid1,uuid2	The IDs of assets. Separate multiple IDs with commas (,).
Name	String	No	debian:10:CVE-2019-9893	The name of the vulnerability.
AliasName	String	No	DSA-2019 libseccomp security vulnerability	The alias of the vulnerability.
StatusList	String	No	None	This parameter is deprecated.
Necessity	String	No	later,nntf,asap	The priority to fix the vulnerability. Separate multiple priorities with commas (,). Valid values: • asap: high • later: medium • nntf: low
Dealed	String	No	N	The status of the vulnerability. Valid values: • Y: handled • N: unhandled
CurrentPage	Integer	No	1	The number of the page to return.
PageSize	Integer	No	20	The number of entries to return on each page.

Parameter	Type	Required	Example	Description
RepoRegionId	String	No	cn-hangzhou	The region ID of the image repository.
RepoInstanceId	String	No	cri-datavilb****	The ID of the container image.
Repold	String	No	crr-vridcl4****	The ID of the image repository.
RepoName	String	No	centos1	The name of the image repository.
RepoNamespace	String	No	hangzhou-namespace	The namespace to which the image repository belongs.
RegionId	String	No	cn-*****	The region ID.
InstanceId	String	No	i-qeqew*****	The ID of the instance.
Tag	String	No	None	This parameter is deprecated.
Digest	String	No	None	This parameter is deprecated.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.
TotalCount	Integer	25	The total number of entries returned.
VulRecords	Array of VulRecord		An array that consists of the vulnerabilities.
AliasName	String	DSA-2019 libseccomp security vulnerability	The alias of the vulnerability.

Parameter	Type	Example	Description
CanUpdate	Boolean	false	Indicates whether the information about the vulnerability can be modified. Valid values: • true • false
ExtendContentJson	Struct		The extended information about the vulnerability.
Os	String	centos	The name of the operating system.
OsRelease	String	7	The version of the operating system.
RpmEntityList	Array of RpmEntity		An array that consists of the information about RPM Package Manager (RPM) packages.
FullVersion	String	1.4.3-12.el7_6.2	The complete version number.
Layer	String	27213ad3447f0209dd152a5cadea****	The image layer.
MatchDetail	String	libssh2 version less than 0:1.4.3-12.el7_6.3	The details about how the vulnerability was detected.
MatchList	String	libglib2.0-0 version less than 2.50.3-2+deb9u1	The rule that is used to detect the vulnerability.
Name	String	libssh2	The name of the RPM package.
Path	String	/usr/lib64/libssh2.so.1	The path of the software that has the vulnerability.
UpdateCmd	String	yum update libssh2	The command that is used to fix the vulnerability.
Version	String	1.4.3	The version number.

Parameter	Type	Example	Description
FirstTs	Long	1580808765000	The time when the vulnerability was first detected. The value is a UNIX timestamp. Unit: milliseconds.
ImageDigest	String	dsadjahksdhjasdh** **	The digest of the image.
LastTs	Long	1580808765000	The time when the vulnerability was last detected. The value is a UNIX timestamp. Unit: milliseconds.
Layers	List	["b1f5b9420803ad0657cf21566e3e20acc08581e7f22991249ef3aa80b8b1c587"]	The image layers.
ModifyTs	Long	1580808765000	The time when the vulnerability record was updated. The value is a UNIX timestamp. Unit: milliseconds.
Name	String	debian:10:CVE-2019-9893	The name of the vulnerability.
Necessity	String	asap	The priority to fix the vulnerability. Multiple priorities are separated by commas (,). Valid values: • asap: high • later: medium • nntf: low
PrimaryId	Long	2	The ID.
Related	String	CVE-2019-3862	The Common Vulnerabilities and Exposures (CVE) ID of the associated vulnerability.
RepoName	String	centos	The name of the image repository.
RepoNamespace	String	hangzhou-namespace	The namespace of the image.

Parameter	Type	Example	Description
Status	Integer	0	The status of the vulnerability. Valid values: • 0: unhandled • 1: handled • 2: being verified • 3: added to the whitelist
SupportFix	Integer	1	This parameter is deprecated.
Tag	String	0.2	The tag that is added to the image.
Type	String	cve	The type of the vulnerability. Valid values: • CVE: image system vulnerability • SCA: image application vulnerability
Uuid	String	B41B3780-337A-472D-B82E-9FD3*****	The UUID of the asset.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeImageVulList
&<Common request parameters>
```

Sample success responses

`XML` format

```

<TotalCount>25</TotalCount>
<PageSize>20</PageSize>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>
<VulRecords>
  <Status>0</Status>
  <RepoNamespace>hangzhou-namespace</RepoNamespace>
  <ImageDigest>dsadjahksdhjasdh****</ImageDigest>
  <RepoName>centos</RepoName>
  <Necessity>asap</Necessity>
  <LastTs>1580808765000</LastTs>
  <Name>debian:10:CVE-2019-9893</Name>
  <FirstTs>1580808765000</FirstTs>
  <Type>cve</Type>
  <ModifyTs>1580808765000</ModifyTs>
  <Related>CVE-2019-3862</Related>
  <Uuid>B41B3780-337A-472D-B82E-9FD3642B9350</Uuid>
  <CanUpdate>false</CanUpdate>
  <AliasName>DSA-2019 libseccomp security vulnerability</AliasName>
  <Tag>0.2</Tag>
  <SupportFix>1</SupportFix>
  <PrimaryId>2</PrimaryId>
  <Layers>["b1f5b9420803ad0657cf21566e3e20acc08581e7f22991249ef3aa80b8b1c587"]</Layers>
  <ExtendContentJson>
    <Os>centos</Os>
    <OsRelease>7</OsRelease>
    <RpmEntityList>
      <Path>/usr/lib64/libssh2.so.1</Path>
      <UpdateCmd>yum update libssh2</UpdateCmd>
      <MatchList>libglib2.0-0 version less than 2.50.3-2+deb9u1</MatchList>
      <Version>1.4.3</Version>
      <FullVersion>1.4.3-12.el7_6.2</FullVersion>
      <Layer>27213ad3447f0209dd152a5cadea****</Layer>
      <MatchDetail>libssh2 version less than 0:1.4.3-12.el7_6.3</MatchDetail>
      <Name>libssh2</Name>
    </RpmEntityList>
  </ExtendContentJson>
</VulRecords>
<CurrentPage>1</CurrentPage>

```

JSON format


```
{
  "TotalCount": 25,
  "PageSize": 20,
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350",
  "VulRecords": {
    "Status": 0,
    "RepoNamespace": "hangzhou-namespace",
    "ImageDigest": "dsadjahksdhjasdh****",
    "RepoName": "centos",
    "Necessity": "asap",
    "LastTs": 1580808765000,
    "Name": "debian:10:CVE-2019-9893",
    "FirstTs": 1580808765000,
    "Type": "cve",
    "ModifyTs": 1580808765000,
    "Related": "CVE-2019-3862",
    "Uuid": "B41B3780-337A-472D-B82E-9FD3642B9350",
    "CanUpdate": false,
    "AliasName": "DSA-2019 libseccomp security vulnerability",
    "Tag": 0.2,
    "SupportFix": 1,
    "PrimaryId": 2,
    "Layers": "[\"b1f5b9420803ad0657cf21566e3e20acc08581e7f22991249ef3aa80b8b1c587\"]",
    "ExtendContentJson": {
      "Os": "centos",
      "OsRelease": 7,
      "RpmEntityList": {
        "Path": "/usr/lib64/libssh2.so.1",
        "UpdateCmd": "yum update libssh2",
        "MatchList": "libglib2.0-0 version less than 2.50.3-2+deb9u1",
        "Version": "1.4.3",
        "FullVersion": "1.4.3-12.el7_6.2",
        "Layer": "27213ad3447f0209dd152a5cadea****",
        "MatchDetail": "libssh2 version less than 0:1.4.3-12.el7_6.3",
        "Name": "libssh2"
      }
    }
  },
  "CurrentPage": 1
}
```

6.26. DescribeVulDetails

Queries the details of a vulnerability.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVulDetails	The operation that you want to perform. Set the value to DescribeVulDetails .
Name	String	Yes	debian:10:CVE-2019-9893	The name of the vulnerability.
Type	String	Yes	cve	The type of the vulnerability. Valid values: • CVE: system vulnerability • SCA: application vulnerability
SourceIp	String	No	47.100.XX.XX	The source IP address of the request.
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English
AliasName	String	No	DSA-2019 libseccomp security vulnerability	The alias of the vulnerability.

Response parameters

Parameter	Type	Example	Description
Cves	Array of Cve		An array that consists of system vulnerabilities.
Classify	String	None	This parameter is deprecated.
Classifys	Array of Classify		This parameter is deprecated.
Classify	String	None	This parameter is deprecated.
DemoVideoUrl	String	None	This parameter is deprecated.
Description	String	None	This parameter is deprecated.

Parameter	Type	Example	Description
CnvdId	String	CNVD-2017-***	CNVD ID
Complexity	String	None	This parameter is deprecated.
Content	String	FasterXML Jackson is a Java-oriented data processing tool provided by FasterXML. The jackson-databind component of FasterXML Jackson is used to bind data. \nA vulnerability was detected in FasterXML jackson-databind 2.x versions earlier than FasterXML jackson-databind 2.9.10.5. Attacker can exploit this vulnerability to execute arbitrary code on the system by sending commands.	The description of the vulnerability.
Cveld	String	CVE-2018-**	The Common Vulnerabilities and Exposures (CVE) ID of the vulnerability.
CvssScore	String	9.3	The Common Vulnerability Scoring System (CVSS) score.
CvssVector	String	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H	The CVSS vendor.
OtherId	String	CVE-1999-**	The ID of the associated vulnerability.
Poc	String	None	This parameter is deprecated.
PocCreateTime	Long	1	This parameter is deprecated.
PocDisclosureTime	Long	1	This parameter is deprecated.

Parameter	Type	Example	Description
Product	String	None	This parameter is deprecated.
Reference	String	https://github.com/FasterXML/jackson-databind/issues/2765	The reference.
ReleaseTime	Long	1234567890123	The disclosure time of the vulnerability. The value is a UNIX timestamp. Unit: milliseconds.
Solution	String	The vendor has released a patch to fix this vulnerability. Download the patch from: https://github.com/FasterXML/jackson-databind/issues/2765	The solution.
Summary	String	FasterXML Jackson is a Java-oriented data processing tool provided by FasterXML. The jackson-databind component of FasterXML Jackson is used to bind data. A vulnerability was detected in FasterXML jackson-databind 2.x versions earlier than FasterXML jackson-databind 2.9.10.5. Attacker can exploit this vulnerability to execute arbitrary code on the system by sending commands.	The digest of the vulnerability.
Title	String	FasterXML jackson-databind Code vulnerability	The title of the vulnerability.
Vendor	String	Alibaba Cloud	The vendor that disclosed the vulnerability.

Parameter	Type	Example	Description
VulLevel	String	serious	The severity of the vulnerability.
RequestId	String	B41B3780-337A-472D-B82E-9FD3642B9350	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVulDetails
&Name=debian:10:CVE-2019-9893
&Type=cve
&<Common request parameters>
```

Sample success responses

`XML` format

```

<Cves>
  <CvssVector>CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H</CvssVector>
  <CvssScore>9.3</CvssScore>
  <Classify>None</Classify>
  <PocDisclosureTime>1</PocDisclosureTime>
  <Poc>None</Poc>
  <Reference>https://github.com/FasterXML/jackson-databind/issues/2765</Reference>
  <Product>None</Product>
  <Title>FasterXML jackson-databind Code vulnerability</Title>
  <CveId>CVE-2018-**</CveId>
  <Vendor>Alibaba Cloud</Vendor>
  <OtherId>CVE-1999-**</OtherId>
  <CnvdId>CNVD-2017-***</CnvdId>
  <Complexity>None</Complexity>
  <PocCreateTime>1</PocCreateTime>
  <ReleaseTime>1234567890123</ReleaseTime>
  <Content>FasterXML Jackson is a Java-oriented data processing tool provided by FasterXML. The jackson-databind component of FasterXML Jackson is used to bind data. \nA vulnerability was detected in FasterXML jackson-databind 2.x versions earlier than FasterXML jackson-databind 2.9.10.5. Attacker can exploit this vulnerability to execute arbitrary code on the system by sending commands. </Content>
  <Summary>FasterXML Jackson is a Java-oriented data processing tool provided by FasterXML L. The jackson-databind component of FasterXML Jackson is used to bind data. \n\nA vulnerability was detected in FasterXML jackson-databind 2.x versions earlier than FasterXML jackson-databind 2.9.10.5. Attacker can exploit this vulnerability to execute arbitrary code on the system by sending commands. \n</Summary>
  <Solution>&lt;p&gt;The vendor has released a patch to fix this vulnerability. Download the patch from:&lt;br /&gt;https://github.com/FasterXML/jackson-databind/issues/2765&lt;/p&gt;&lt;n&lt;/Solution>
  <VulLevel>serious</VulLevel>
  <Classifys>
    <DemoVideoUrl>None</DemoVideoUrl>
    <Description>None</Description>
    <Classify>None</Classify>
  </Classifys>
</Cves>
<RequestId>B41B3780-337A-472D-B82E-9FD3642B9350</RequestId>

```

JSON format

```

{
  "Cves": {
    "CvssVector": "CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H",
    "CvssScore": 9.3,
    "Classify": "None",
    "PocDisclosureTime": 1,
    "Poc": "None",
    "Reference": "https://github.com/FasterXML/jackson-databind/issues/2765",
    "Product": "None",
    "Title": "FasterXML jackson-databind Code vulnerability",
    "CveId": "CVE-2018-**",
    "Vendor": "Alibaba Cloud",
    "OtherId": "CVE-1999-**",
    "CnvdId": "CNVD-2017-***",
    "Complexity": "None",
    "PocCreateTime": 1,
    "ReleaseTime": 1234567890123,
    "Content": "FasterXML Jackson is a Java-oriented data processing tool provided by FasterXML. The jackson-databind component of FasterXML Jackson is used to bind data. \\nA vulnerability was detected in FasterXML jackson-databind 2.x versions earlier than FasterXML jackson-databind 2.9.10.5. Attacker can exploit this vulnerability to execute arbitrary code on the system by sending commands.",
    "Summary": "FasterXML Jackson is a Java-oriented data processing tool provided by FasterXML. The jackson-databind component of FasterXML Jackson is used to bind data. \\n\\nA vulnerability was detected in FasterXML jackson-databind 2.x versions earlier than FasterXML jackson-databind 2.9.10.5. Attacker can exploit this vulnerability to execute arbitrary code on the system by sending commands. \\n",
    "Solution": "<p>The vendor has released a patch to fix this vulnerability. Download the patch from:<br />https://github.com/FasterXML/jackson-databind/issues/2765</p>\\n",
    "VulLevel": "serious",
    "Classifys": {
      "DemoVideoUrl": "None",
      "Description": "None",
      "Classify": "None"
    }
  },
  "RequestId": "B41B3780-337A-472D-B82E-9FD3642B9350"
}

```

6.27. DescribeAllGroups

Queries the grouping information about servers.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeAllGroups	The operation that you want to perform. Set the value to DescribeAllGroups .

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The language of the content within the request and response. Valid values: • zh: Chinese • en: English

Response parameters

Parameter	Type	Example	Description
Count	Integer	1	The total number of groups.
Groups	Array of Group		An array that consists of the grouping information.
GroupFlag	Integer	0	The type of the server group. Valid values: • 0: default group • 1: other groups
GroupId	Integer	123	The ID of the group.
GroupName	String	abc	The name of the group.
RequestId	String	7E0618A9-D5EF-4220-9471-C42B5E92719F	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAllGroups
&<Common request parameters>
```

Sample success responses

`XML` format


```
<RequestId>7E0618A9-D5EF-4220-9471-C42B5E92719F</RequestId>
<Groups>
  <GroupName>abc</GroupName>
  <GroupFlag>0</GroupFlag>
  <GroupId>123</GroupId>
</Groups>
<Count>1</Count>
```

JSON format

```
{
  "RequestId": "7E0618A9-D5EF-4220-9471-C42B5E92719F",
  "Groups": {
    "GroupName": "abc",
    "GroupFlag": 0,
    "GroupId": 123
  },
  "Count": 1
}
```

6.28. DescribeAssetDetailByUuid

Queries the details of an asset by using the UUID of the asset.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeAssetDetailByUuid	The operation that you want to perform. Set the value to DescribeAssetDetailByUuid .
Uuid	String	Yes	9e6cad93-a379-46fd-a701-9bbf02f4****	The UUID of the asset that you want to query.
SourceIp	String	No	192.0.XX.XX	The source IP address of the request.
Lang	String	No	zh	The language of the content within the request and response. Default value: zh . Valid values: zh: Chinese en: English

Response parameters

Parameter	Type	Example	Description
AssetDetail	Struct		The details of the asset.
AssetType	String	6	The type of the asset. Valid values: • 0: Elastic Compute Service (ECS) instance • 1: Server Load Balancer (SLB) instance • 2: NAT gateway • 3: ApsaraDB RDS database • 4: ApsaraDB for MongoDB database • 5: KVStore for Redis database • 6: image • 7: container
AuthModifyTime	Long	1627974044000	The timestamp when Container Protection was authorized to scan the asset. Unit: milliseconds.
AuthVersion	Integer	1	The edition of Container Protection that is authorized to scan the asset. Valid values: • 1: Basic edition (Unauthorized) • 6: Anti-virus edition • 5: Advanced edition • 3: Enterprise edition • 7: Ultimate edition • 10: Value-added Plan edition
Bind	Boolean	true	Indicates whether Container Protection is authorized to scan the asset. Valid values: • true: yes • false: no
ClientStatus	String	online	The status of the agent. Valid values: • pause: The agent suspends protection for your asset. • online: The agent is protecting your asset. • offline: The agent does not protect your asset.
Cpu	Integer	4	The number of CPU cores.

Parameter	Type	Example	Description
CpuInfo	String	Intel(R) Xeon(R) Platinum 8163 CPU @ 2.50GHz	The details of the CPU.
CreateTime	Long	1603863599000	The timestamp when Container Protection records the details of the asset. Unit: milliseconds.
DiskInfoList	List	[{ "diskName": "/dev/vda1", "totalSize": 20, "useSize": 2 }]	The information about the disk. This parameter contains the following fields: • diskName: the name of the disk. • totalSize: the total amount of the disk space. Unit: GB. • useSize: the amount of the used disk space. Unit: GB.
GroupTrace	String	Ungrouped	The group to which the asset belongs. By default, the assets that are not grouped belong to the Ungrouped group.
HostName	String	qewrqwerqs****	The hostname of the asset.
InstanceId	String	i- uf6h7p2fgk6rkk0g** **	The instance ID of the asset.
InstanceName	String	i- fasdfasdfadfa****	The instance name of the asset.
InternetIp	String	10.18.XX.XX	The public IP address of the server.
IntranetIp	String	192.168.XX.XX	The private IP address of the server.
Ip	String	192.168.XX.XX	The IP address of the asset.
IpList	List	["192.168.XX.XX", "1 92.168.XX.XX"]	The list of IP addresses.
Kernel	String	4.18.0- 80.11.2.el8_0.x86_64	The kernel version of the operating system.
MacList	List	["00:16:3*:1*:9*:cf"]	The MAC address.

Parameter	Type	Example	Description
Mem	Integer	32	The memory size of the server. Unit: GB.
Os	String	linux	The type of the operating system.
OsDetail	String	Linux 64bit	The version of the operating system.
OsName	String	CentOS 8.0 64-bit	The name of the operating system.
Region	String	cn-hangzhou-dg-a01	The region.
RegionId	String	cn-hangzhou	The region ID.
RegionName	String	China (Hangzhou)	The region name.
SysInfo	String	CentOS Linux 8.0.1905	The details of the operating system.
Tag	String	InternetIp	The tag that is added to the asset.
Uuid	String	9e6cad93-a379-46fd-a701-9bbf02f4****	The UUID of the asset.
VpcInstanceId	String	vpc-bp1fs3bwonlfq503w****	The ID of the virtual private cloud (VPC) to which the asset belongs.
RequestId	String	39031E31-6BBA-5C99-A870-D807E78918CD	The ID of the request, which is used to locate and troubleshoot issues.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAssetDetailByUuid
&Uuid=9e6cad93-a379-46fd-a701-9bbf02f4****
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>39031E31-6BBA-5C99-A870-D807E78918CD </RequestId>
<AssetDetail>
  <GroupTrace>Ungrouped</GroupTrace>
  <Bind>true</Bind>
  <Os>linux</Os>
  <Ip>192.168.XX.XX </Ip>
  <Cpu>4</Cpu>
  <OsDetail>Linux 64bit </OsDetail>
  <IntranetIp>192.168.XX.XX </IntranetIp>
  <AuthModifyTime>1627974044000</AuthModifyTime>
  <InternetIp>10.18.XX.XX </InternetIp>
  <RegionName>China (Hangzhou)</RegionName>
  <Kernel>4.18.0-80.11.2.el8_0.x86_64 </Kernel>
  <HostName>qewrqwerqs**** </HostName>
  <ClientStatus>online</ClientStatus>
  <CpuInfo>Intel(R) Xeon(R) Platinum 8163 CPU @ 2.50GHz </CpuInfo>
  <InstanceId>i-uf6h7p2fgk6rkk0g**** </InstanceId>
  <CreateTime>1603863599000</CreateTime>
  <OsName>CentOS 8.0 64-bit</OsName>
  <SysInfo>CentOS Linux 8.0.1905 </SysInfo>
  <InstanceName>i-fasdfasdfadfafa**** </InstanceName>
  <AssetType>6</AssetType>
  <Uuid>9e6cad93-a379-46fd-a701-9bbf02f4**** </Uuid>
  <Mem>32</Mem>
  <Region>cn-hangzhou-dg-a01 </Region>
  <VpcInstanceId>vpc-bp1fs3bwonlfq503w**** </VpcInstanceId>
  <Tag>InternetIp </Tag>
  <RegionId>cn-hangzhou </RegionId>
  <AuthVersion>1</AuthVersion>
  <IpList>["192.168.XX.XX", "192.168.XX.XX"] </IpList>
  <MacList>["00:16:3*:1*:9*:cf"] </MacList>
  <DiskInfoList>[ { "diskName": "/dev/vda1", "totalSize": 20, "useSize": 2 } ]</DiskInfoList>
</AssetDetail>
```

JSON format

```
{
  "RequestId": "39031E31-6BBA-5C99-A870-D807E78918CD",
  "AssetDetail": {
    "GroupTrace": "Ungrouped",
    "Bind": true,
    "Os": "linux",
    "Ip": "192.168.XX.XX",
    "Cpu": 4,
    "OsDetail": "Linux 64bit",
    "IntranetIp": "192.168.XX.XX",
    "AuthModifyTime": 1627974044000,
    "InternetIp": "10.18.XX.XX",
    "RegionName": "China (Hangzhou)",
    "Kernel": "4.18.0-80.11.2.el8_0.x86_64",
    "HostName": "qewrqwerqs****",
    "ClientStatus": "online",
    "CpuInfo": "Intel(R) Xeon(R) Platinum 8163 CPU @ 2.50GHz",
    "InstanceId": "i-uf6h7p2fgk6rkk0g****",
    "CreateTime": 1603863599000,
    "OsName": "CentOS 8.0 64-bit",
    "SysInfo": "CentOS Linux 8.0.1905",
    "InstanceName": "i-fasdfasdfadfaf****",
    "AssetType": 6,
    "Uuid": "9e6cad93-a379-46fd-a701-9bbf02f4****",
    "Mem": 32,
    "Region": "cn-hangzhou-dg-a01",
    "VpcInstanceId": "vpc-bp1fs3bwonlfq503w****",
    "Tag": "InternetIp",
    "RegionId": "cn-hangzhou",
    "AuthVersion": 1,
    "IpList": "[\"192.168.XX.XX\", \"192.168.XX.XX\"]",
    "MacList": "[\"00:16:3*:1*:9*:cf\"]",
    "DiskInfoList": "[ { \"diskName\": \"/dev/vda1\", \"totalSize\": 20, \"useSize\": 2"
  } ]"
}
```

7. Threat Detection Service (TDS)

7.1. Asset management

7.1.1. DescribeFieldStatistics

Queries statistics of the assets.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeFieldStatistics	The operation that you want to perform. Set the value to DescribeFieldStatistics.
MachineTypes	String	No	ecs	The types of the assets. If the asset type is not specified, the statistics of all types of assets are queried. • ecs: an ECS instance • cloud_product: a cloud service

Response parameters

Parameter	Type	Example	Description
GroupedFields	-	-	The asset information.
GroupCount	Integer	20	The number of server groups.
InstanceCount	Integer	100	The total number of assets.
NewInstanceCount	Integer	10	The number of new servers.
NotRunningStatusCount	Integer	10	The number of servers that are not started.
OfflineInstanceCount	Integer	21	The number of offline servers.
RegionCount	Integer	11	The number of regions to which the servers belong.

Parameter	Type	Example	Description
RiskInstanceCount	Integer	90	The number of assets that are at risk.
UnprotectedInstanceCount	Integer	10	The number of unprotected assets.
VpcCount	Integer	5	The number of VPCs.
RequestId	String	7E0618A9-D5EF-4220-9471-C42B5E92719F	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeFieldStatistics
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeFieldStatistics>
  <RequestId>20CB6B41-0ED9-4679-BF5D-B84B8F7E70FC</RequestId>
  <GroupedFields>
    <InstanceCount>216</InstanceCount>
    <GroupCount>3</GroupCount>
    <NewInstanceCount>11</NewInstanceCount>
    <VpcCount>109</VpcCount>
    <RiskInstanceCount>121</RiskInstanceCount>
    <OfflineInstanceCount>48</OfflineInstanceCount>
    <UnprotectedInstanceCount>48</UnprotectedInstanceCount>
    <RegionCount>25</RegionCount>
    <NotRunningStatusCount>9</NotRunningStatusCount>
  </GroupedFields>
</DescribeFieldStatistics>
```

JSON format


```
{
  "RequestId": "20CB6B41-0ED9-4679-BF5D-B84B8F7E70FC",
  "GroupedFields": {
    "InstanceCount": 216,
    "NewInstanceCount": 11,
    "GroupCount": 3,
    "VpcCount": 109,
    "RiskInstanceCount": 121,
    "UnprotectedInstanceCount": 48,
    "OfflineInstanceCount": 48,
    "RegionCount": 25,
    "NotRunningStatusCount": 9
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.1.2. DescribeGroupedTags

Queries the statistics of asset tags.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeGroupedTags	The operation that you want to perform. Set the value to DescribeGroupedTags.
MachineTypes	String	No	ecs	The types of the assets. If the asset type is not specified, the statistics of all asset tags are queried. - ecs: an ECS instance - cloud_product: a cloud service

Response parameters

Parameter	Type	Example	Description
Count	Integer	2	The number of entries returned on the current page.
GroupedFields	Array		The statistics of the asset tag.

Parameter	Type	Example	Description
Count	String	2	The number of assets to which a tag attaches.
Name	String	test	The name of the tag.
TagId	Integer	8704	The ID of the tag.
HttpStatusCode	Integer	200	The HTTP status code of the returned results.
RequestId	String	7E0618A9-D5EF-4220-9471-C42B5E92719F	The ID of the request.
Success	Boolean	true	Indicates whether the request was successful. • true: successful • false: failed

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeGroupedTags
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeGroupedTags>
  <HttpStatusCode>200</HttpStatusCode>
  <Count>1</Count>
  <RequestId>DD5AFF52-0827-4FC9-B6EA-B233FF3AFF91</RequestId>
  <Success>true</Success>
  <GroupedFiles>
    <Name>test</Name>
    <Count>167</Count>
    <TagId>8704</TagId>
  </GroupedFiles>
</DescribeGroupedTags>
```

JSON format

```
{
  "HttpStatusCode":200,
  "Count":1,
  "RequestId":"DD5AFF52-0827-4FC9-B6EA-B233FF3AFF91",
  "Success":true,
  "GroupedFileds":[
    {
      "Name":"test",
      "Count":"167",
      "TagId":8704
    }
  ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.1.3. DescribeAllGroups

Queries the grouping information about servers.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeAllGroups	The operation that you want to perform. Set the value to DescribeAllGroups.
Lang	String	No	zh	The natural language of the request and response. Valid values: zh: Chinese en: English

Response parameters

Parameter	Type	Example	Description
Count	Integer	2	The number of entries returned on the current page.
Groups	Array		The grouping information about the servers.

Parameter	Type	Example	Description
GroupFlag	Integer	1	The type of the server group. • 0: default group • 1: other groups
GroupId	Integer	8834224	The ID of the server group.
GroupName	String	test	The name of the server group.
RequestId	String	"requestId": "7E0618A9-D5EF- 4220-9471- C42B5E92719F",	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAllGroups  
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeAllGroups>  
  <Groups>  
    <GroupFlag>0</GroupFlag>  
    <GroupName>Ungrouped</GroupName>  
    <GroupId>4120080</GroupId>  
  </Groups>  
  <Groups>  
    <GroupFlag>1</GroupFlag>  
    <GroupName>leaves</GroupName>  
    <GroupId>8831497</GroupId>  
  </Groups>  
  <Groups>  
    <GroupFlag>1</GroupFlag>  
    <GroupName>test</GroupName>  
    <GroupId>8834224</GroupId>  
  </Groups>  
  <Count>3</Count>  
  <RequestId>9DD4B19B-CA32-41DA-AED7-77B4F84A91D5</RequestId>  
</DescribeAllGroups>
```

JSON format

```
{
  "Groups": [
    {
      "GroupFlag": 0,
      "GroupName": "Ungrouped",
      "GroupId": 4120080
    },
    {
      "GroupFlag": 1,
      "GroupName": "leaves",
      "GroupId": 8831497
    },
    {
      "GroupFlag": 1,
      "GroupName": "test",
      "GroupId": 8834224
    }
  ],
  "Count": 3,
  "RequestId": "9DD4B19B-CA32-41DA-AED7-77B4F84A91D5"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.1.4. DescribeInstanceStatistics

Queries risk information about an asset.

Request parameters

Parameter	Type	Required	Example	Description
From	String	Yes	sas	The source of the data. Set the value to sas.
Uuid	String	Yes	a51cec37-ed73-4c53-b467-***	The IDs of the assets. Separate multiple IDs with commas (.).  Note To query the risk information about an asset, you must provide the ID of the asset. You can call the DescribeCloudCenterInstances operation to obtain the ID.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The natural language of the request and response. Valid values: zh: Chinese en: English

Response parameters

Parameter	Type	Example	Description
RequestId	String	7E0618A9-D5EF-4220-9471-C42B5E92719F	The ID of the request.
Data	Array		The risk information about the asset.
Uuid	String	us1233*****	The ID of the asset.
Account	Integer	1	The type of the asset group. Valid values: 0: default group 1: other groups
Health	Integer	1	The number of issues detected by the baseline check.
Trojan	Integer	1	The number of trojans.
Suspicious	Integer	2	The number of alerts.
Vul	Integer	4	The total number of vulnerabilities: CveNum + EmgNum + SysNum + CmsNum + AppNum.
CveNum	Integer	1	The number of Linux software vulnerabilities.
EmgNum	Integer	0	The number of emergency vulnerabilities.
SysNum	Integer	1	The number of Windows vulnerabilities.
CmsNum	Integer	2	The number of Web CMS vulnerabilities.

Parameter	Type	Example	Description
AppNum	Integer	0	The number of application vulnerabilities.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeInstanceStatistics
&From=sas
&Uuid=a51cec37-ed73-4c53-b467-***
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeInstanceStatisticsResponse>
  <Data>
    <SysNum>1</SysNum>
    <Uuid>a51cec37-ed73-4c53-b467-***</Uuid>
    <CveNum>1</CveNum>
    <Suspicious>1</Suspicious>
    <Trojan>0</Trojan>
    <Account>0</Account>
    <CmsNum>1</CmsNum>
    <EmgNum>1</EmgNum>
    <Health>0</Health>
    <AppNum>1</AppNum>
    <Vul>5</Vul>
  </Data>
  <Data>
    <SysNum>2</SysNum>
    <Uuid>33f107a3-4653-4228-a428-***</Uuid>
    <CveNum>1</CveNum>
    <Suspicious>2</Suspicious>
    <Trojan>0</Trojan>
    <Account>0</Account>
    <CmsNum>1</CmsNum>
    <EmgNum>2</EmgNum>
    <Health>0</Health>
    <AppNum>1</AppNum>
    <Vul>7</Vul>
  </Data>
  <RequestId>44AE72D4-2DDF-4CEC-9957-64C470CC90FC</RequestId>
</DescribeInstanceStatisticsResponse>
```

JSON format

```
{
  "Data": [
    {
      "SysNum": 1,
      "Uuid": "a51cec37-ed73-4c53-b467-***",
      "CveNum": 1,
      "Suspicious": 1,
      "Trojan": 0,
      "Account": 0,
      "CmsNum": 1,
      "EmgNum": 1,
      "Health": 0,
      "AppNum": 1,
      "Vul": 5
    },
    {
      "SysNum": 2,
      "Uuid": "33f107a3-4653-4228-a428-***",
      "CveNum": 1,
      "Suspicious": 2,
      "Trojan": 0,
      "Account": 0,
      "CmsNum": 1,
      "EmgNum": 2,
      "Health": 0,
      "AppNum": 1,
      "Vul": 7
    }
  ],
  "RequestId": "44AE72D4-2DDF-4CEC-9957-64C470CC90FC"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.1.5. DescribeCloudProductFieldStatistics

Queries the statistics on cloud services that are protected by Threat Detection Service.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCloudProductFieldStatistics	The operation that you want to perform. Set the value to DescribeCloudProductFieldStatistics.

Response parameters

Parameter	Type	Example	Description
RequestId	String	7E0618A9-D5EF-4220-9471-C42B5E92719F	The ID of the request.
GroupedFields	Struct		The statistics on cloud services that are protected by Threat Detection Service.
RiskInstanceCount	Integer	90	The number of assets that are at risk.
InstanceCount	Integer	100	The total number of assets.
CategoryCount	String	[{"MachineType":1,"Count":11}]	The statistics on the numbers of assets of different types. MachineType specifies the type of the asset. Count specifies the number of assets of a specific type. Valid values of MachineType: • 1: Server Load Balancer (SLB) • 2: NAT Gateway • 3: ApsaraDB RDS • 4: ApsaraDB for MongoDB

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCloudProductFieldStatistics  
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeCloudProductFieldStatistics>
  <code>200</code>
  <data>
    <GroupedFields>
      <InstanceCount>100</InstanceCount>
      <RiskInstanceCount>90</RiskInstanceCount>
      <categoryCount>
        <MachineType>1</MachineType>
        <Count>11</Count>
      </categoryCount>
    </GroupedFields>
  </data>
  <requestId>7E0618A9-D5EF-4220-9471-C42B5E92719F</requestId>
  <success>true</success>
</DescribeCloudProductFieldStatistics>
```

JSON format

```
{
  "code": 200,
  "data": {
    "GroupedFields": {
      "InstanceCount": 100,
      "RiskInstanceCount": 90,
      "categoryCount": [{"MachineType": 1, "Count": 11}]
    }
  },
  "requestId": "7E0618A9-D5EF-4220-9471-C42B5E92719F",
  "success": true
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.1.6. DescribeCloudCenterInstances

Queries the asset information on the Assets page, such as the name and region of an asset instance.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCloudCenterInstances	The operation that you want to perform. Set the value to DescribeCloudCenterInstances.

Parameter	Type	Required	Example	Description
Criteria	String	No	<pre>[{"name": "riskStatus", "value": "YES"}, {"name": "internetIp", "value": "1.2."}]</pre>	Specifies the search conditions, such as instance IDs, instance names, VPC IDs, regions, and IP addresses.
CurrentPage	Integer	No	1	The page number of the current page.
LogicalExp	String	No	OR	The logical relationship between search conditions. Valid values: • OR: The logical relationship between search conditions is OR. • AND: The logical relationship between search conditions is AND.
MachineTypes	String	No	ecs	The type of the asset. • ecs: an Elastic Compute Service (ECS) instance • cloud_product: a cloud service
NoPage	Boolean	No	true	Specifies whether to enable paged query. Valid values: • true: enables paged query. • false: disables paged query.
PageSize	Integer	No	20	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
Instances	Array		The asset details.
AlarmStatus	String	NO	Indicates whether alerts are configured for the asset instance. Valid values: • YES • NO
AssetType	String	ecs	The type of the asset.

Parameter	Type	Example	Description
ClientStatus	String	online	Indicates whether the asset instance is protected by the agent. Valid values: online: The protection status of the asset is Enabled. offline: The protection status of the asset is Disabled. pause: The protection status of the asset is Paused.
Flag	Integer	0	Indicates whether the asset instance is provided by Alibaba Cloud. Valid values: 0: The asset instance is provided by Alibaba Cloud. 1: The asset instance is not provided by Alibaba Cloud.
GroupId	String	4120080	The ID of the group to which the asset instance belongs.
HcStatus	String	YES	Indicates whether the asset instance is exposed to baseline risks. Valid values: YES NO
HealthCheckCount	Integer	1	The number of issues that are detected in baseline checks.
InstanceId	String	i-m5***	The ID of the asset instance.
InstanceName	String	yztest-l***	The name of the asset instance.
InternetIp	String	1.2.3.4	The public IP address of the asset instance.
IntranetIp	String	1.2.3.0	The private IP address of the asset instance.
Ip	String	1.2.3.4	The public IP address of the asset instance.
Os	String	Linux	The operating system of the asset instance.

Parameter	Type	Example	Description
OsName	String	CentOS 7.6 64-bit	The kernel version of the asset instance.
Region	String	cn-hangzhou-cm***-***	The region where the asset instance is deployed.
RegionId	String	cn-hangzhou	The ID of the region where the asset instance is deployed.
RegionName	String	China (Qingdao)	The name of the region where the asset instance is deployed.
RiskStatus	String	NO	Indicates whether the asset instance is exposed to security risks. Valid values: • YES • NO
SafeEventCount	Integer	5	The number of alerts detected on the asset instance.
Status	String	Running	The status of the asset instance. Valid values: • Running: The instance is running. • notRunning: The instance is not running.
Tag	String	InternetIp	The tag of the asset instance.
Uuid	String	c9107c04-942f-40c1-981a-f1c1***	The ID of the asset instance.
VpcInstanceId	String	classic	The ID of the VPC to which the asset instance belongs.
VulCount	Integer	2	The number of vulnerabilities detected on the asset instance.
VulStatus	String	YES	Indicates whether the asset instance is exposed to vulnerabilities. Valid values: • YES • NO

Parameter	Type	Example	Description
PageInfo			The page information.
Count	Integer	10	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	50	The total number of entries.
RequestId	String	32A73759-4C0F-4801-BE98-901223ACEE9A	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. • true: successful • false: failed

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCloudCenterInstances
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeCloudCenterInstances>
  <RequestId>32A73759-4C0F-4801-BE98-901223ACEE9A</RequestId>
  <PageInfo>
    <Count>0</Count>
    <TotalCount>691</TotalCount>
    <PageSize>20</PageSize>
    <CurrentPage>1</CurrentPage>
  </PageInfo>
  <Instances>
    <RiskStatus>NO</RiskStatus>
    <Uuid>88f7ce77-595e-4580-b655-3***</Uuid>
    <Ip>1.2.3.4</Ip>
    <Flag>0</Flag>
    <RegionName>China (Hangzhou)</RegionName>
    <OsName>CentOS 7.6 64-bit</OsName>
    <AssetType>0</AssetType>
```

```
<InstanceId>i-m5e50***</InstanceId>
<InternetIp>1.2.3.4</InternetIp>
<HealthCheckCount>0</HealthCheckCount>
<HcStatus>NO</HcStatus>
<Os>linux</Os>
<ClientStatus>online</ClientStatus>
<Status>Running</Status>
<Region>cn-hangzhou-cm***-***</Region>
<VpcInstanceId>classic</VpcInstanceId>
<VulStatus>NO</VulStatus>
<Tag>InternetIp</Tag>
<RegionId>cn-hangzhou</RegionId>
<IntranetIp>1.2.3.0</IntranetIp>
<AlarmStatus>NO</AlarmStatus>
<VulCount>0</VulCount>
<SafeEventCount>0</SafeEventCount>
<InstanceName>yztest-l***</InstanceName>
</Instances>
<Instances>
  <RiskStatus>NO</RiskStatus>
  <Uuid>7a4735d6-75a4-4555-a18f-b***</Uuid>
  <Ip>1.2.3.4</Ip>
  <Flag>0</Flag>
  <RegionName>China (Hangzhou)</RegionName>
  <OsName>CentOS 7.6 64-bit</OsName>
  <AssetType>0</AssetType>
  <InstanceId>i-m5e50***</InstanceId>
  <InternetIp>1.2.3.4</InternetIp>
  <HealthCheckCount>0</HealthCheckCount>
  <HcStatus>NO</HcStatus>
  <Os>linux</Os>
  <ClientStatus>online</ClientStatus>
  <Status>Running</Status>
  <Region>cn-hangzhou-cm***-***</Region>
  <VpcInstanceId>classic</VpcInstanceId>
  <VulStatus>NO</VulStatus>
  <Tag>InternetIp</Tag>
  <RegionId>cn-hangzhou</RegionId>
  <IntranetIp>1.2.3.0</IntranetIp>
  <AlarmStatus>NO</AlarmStatus>
  <VulCount>0</VulCount>
  <SafeEventCount>0</SafeEventCount>
  <InstanceName>yztest-l***</InstanceName>
</Instances>
<Success>true</Success>
</DescribeCloudCenterInstances>
```

JSON format

```
{
  "RequestId": "32A73759-4C0F-4801-BE98-901223ACEE9A",
  "Instances": [
    {
      "RiskStatus": "NO"
```

```
    "RiskStatus": "NO",
    "Uuid": "88f7ce77-595e-4580-b655-3***",
    "Ip": "1.2.3.4",
    "Flag": 0,
    "RegionName": "China (Hangzhou)",
    "OsName": "CentOS 7.6 64-bit",
    "AssetType": "0",
    "InstanceId": "i-m5e50***",
    "InternetIp": "1.2.3.4",
    "HealthCheckCount": 0,
    "HcStatus": "NO",
    "Os": "linux",
    "Status": "Running",
    "ClientStatus": "online",
    "Region": "cn-hangzhou-cm***-***",
    "VpcInstanceId": "classic",
    "Tag": "InternetIp",
    "VulStatus": "NO",
    "IntranetIp": "1.2.3.0",
    "RegionId": "cn-hangzhou",
    "AlarmStatus": "NO",
    "VulCount": 0,
    "InstanceName": "yztest-l***",
    "SafeEventCount": 0
  },
  {
    "RiskStatus": "NO",
    "Uuid": "7a4735d6-75a4-4555-a18f-b***",
    "Ip": "1.2.3.4",
    "Flag": 0,
    "RegionName": "China (Hangzhou)",
    "OsName": "CentOS 7.6 64-bit",
    "AssetType": "0",
    "InstanceId": "i-m5e5***",
    "InternetIp": "1.2.3.4",
    "HealthCheckCount": 0,
    "HcStatus": "NO",
    "Os": "linux",
    "Status": "Running",
    "ClientStatus": "online",
    "Region": "cn-hangzhou-cm***-***",
    "VpcInstanceId": "classic",
    "Tag": "InternetIp",
    "VulStatus": "NO",
    "IntranetIp": "1.2.3.0",
    "RegionId": "cn-hangzhou",
    "AlarmStatus": "NO",
    "VulCount": 0,
    "InstanceName": "yztest-l***",
    "SafeEventCount": 0
  }
],
"PageInfo": {
  "Count": 0,
  "TotalCount": 691,
```



```
"PageSize":20,  
"CurrentPage":1  
},  
"Success":true  
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.1.7. DescribeSummaryInfo

Queries the security information about an asset, such as the security score and the numbers of protected and unprotected assets.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSummaryInfo	The operation that you want to perform. Set the value to DescribeSummaryInfo.
Lang	String	No	zh	The natural language of the request and response. Valid values: zh: Chinese en: English
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
AegisClientOfflineCount	Integer	12	The number of unprotected assets.
AegisClientOnlineCount	Integer	127	The number of protected assets.
RequestId	String	D40198E1-6EA8-482E-B3C7-D9573D75C0CA	The ID of the request.

Parameter	Type	Example	Description
SecurityScore	Integer	44	The security score of assets. Valid values: 95 to 100: The assets are secure. 85 to 94: The assets are exposed to a few security risks. We recommend that you reinforce your security system as soon as possible. 70 to 84: The assets are exposed to many security risks. We recommend that you reinforce your security system as soon as possible. 69 or lower: The current security system is unable to protect the assets against attacker intrusions. We recommend that you reinforce your security system as soon as possible.
Success	Boolean	true	Indicates whether the request is successful.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSummaryInfo
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeSummaryInfo>
  <SecurityScore>44</SecurityScore>
  <AegisClientOnlineCount>127</AegisClientOnlineCount>
  <RequestId>D40198E1-6EA8-482E-B3C7-D9573D75C0CA</RequestId>
  <Success>true</Success>
  <AegisClientOfflineCount>12</AegisClientOfflineCount>
</DescribeSummaryInfo>
```

JSON format

```
{
  "AegisClientOnlineCount":127,
  "SecurityScore":44,
  "RequestId":"D40198E1-6EA8-482E-B3C7-D9573D75C0CA",
  "Success":true,
  "AegisClientOfflineCount":12
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.2. Secure score

7.2.1. DescribeSecureSuggestion

Queries suggestions about how to manage the security risks that affect the security score.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSecureSuggestion	The operation that you want to perform. Set the value to DescribeSecureSuggestion.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: zh: Chinese en: English

Response parameters

Parameter	Type	Example	Description
RequestId	String	F35F45B0-5D6B-4238-BE02-A62D0760E840	The ID of the request.
Suggestions	Array		The suggestions on risk management.
Detail	Array		The details of risk management suggestions.
Description	String	You have four ApsaraDB RDS instances at risk.	The description of the suggestion for risk management.
SubType	String	CLOUD_HC_RDS	The type of the unhandled risk.

Parameter	Type	Example	Description
Title	String	The check on security policies of ApsaraDB RDS instances has failed. The instances are at risk.	The name of the unhandled risk.
Points	Integer	40	The penalty points of each item.
SuggestType	String	SS_ALARM	The type of the unhandled risk. Valid values: SS_REINFORCE: Key features, such as the antivirus feature, are not configured. SS_ALARM: unhandled risks. SS_VUL: unhandled vulnerabilities. SS_HC: baseline check risks. SS_AK: AccessKey pair leaks. SS_CLOUD_HC: configuration risks in Alibaba Cloud services. OTHER: other risks.
TotalCount	Integer	15	The total number of unhandled risks.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSecureSuggestion
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeSecureSuggestionResponse>
  <Suggestions>
    <Points>40</Points>
    <SuggestType>SS_ALARM</SuggestType>
    <Detail>
      <Description>You have 691 security alerts, which affects 56 assets.</Description>
      <SubType>ALARM_HIGH</SubType>
      <Title>You have unhandled high-risk alerts</Title>
    </Detail>
    <Detail>
      <Description>You have 501 security alerts, which affects 119 assets.</Description>
```

```
<SubType>ALARM_MEDIUM</SubType>
<Title>You have unhandled medium-risk alerts</Title>
</Detail>
</Suggestions>
<Suggestions>
  <Points>12</Points>
  <SuggestType>SS_VUL</SuggestType>
  <Detail>
    <Description>You have five vulnerabilities.</Description>
    <SubType>VUL_CMS</SubType>
    <Title>You have unhandled CMS vulnerabilities</Title>
  </Detail>
  <Detail>
    <Description>You have 107 vulnerabilities, which affects 68 servers.</Descrip
tion>
    <SubType>VUL_WIN</SubType>
    <Title>You have unhandled Windows host vulnerabilities</Title>
  </Detail>
  <Detail>
    <Description>You have 701 vulnerabilities, which affects 87 servers.</Descrip
tion>
    <SubType>VUL_LINUX</SubType>
    <Title>You have unhandled Linux host vulnerabilities</Title>
  </Detail>
  <Detail>
    <Description>You have one unhandled urgent vulnerability.</Description>
    <SubType>VUL_EMR_UNFIX</SubType>
    <Title>You have unhandled urgent vulnerabilities</Title>
  </Detail>
</Suggestions>
<Suggestions>
  <Points>2</Points>
  <SuggestType>SS_HC</SuggestType>
  <Detail>
    <Description>You have 46 baseline check risks, which affects 260 servers.</De
scription>
    <SubType>HC_WARN</SubType>
    <Title>You have unhandled baseline check risks</Title>
  </Detail>
</Suggestions>
<Suggestions>
  <Points>30</Points>
  <SuggestType>SS_AK</SuggestType>
  <Detail>
    <Description>You have 12 AccessKey pair leaks.</Description>
    <SubType>ACCESSKEY_LEAK</SubType>
    <Title>You have potential AccessKey pair leaks</Title>
  </Detail>
</Suggestions>
<Suggestions>
  <Points>35</Points>
  <SuggestType>SS_CLOUD_HC</SuggestType>
  <Detail>
    <Description>You have four ApsaraDB RDS instances at risk.</Description>
```

```

        <SubType>CLOUD_HC_RDS</SubType>
        <Title>The check on security policies of ApsaraDB RDS instances has failed. The instances are at risk</Title>
    </Detail>
    <Detail>
        <Description>You have three high configuration risks for Alibaba Cloud services.</Description>
        <SubType>CLOUD_HC_HIGH_LEVEL</SubType>
        <Title>You have high configuration risks for Alibaba Cloud services</Title>
    </Detail>
    <Detail>
        <Description>You have 28 medium or low configuration risks for Alibaba Cloud services.</Description>
        <SubType>CLOUD_HC_OTHER_LEVEL</SubType>
        <Title>You have medium or low configuration risks for Alibaba Cloud services</Title>
    </Detail>
</Suggestions>
<Suggestions>
    <Points>5</Points>
    <SuggestType>OTHER</SuggestType>
    <Detail>
        <Description>You have been attacked 5,767 times.</Description>
        <SubType>OTHER_ATTACH</SubType>
        <Title>You are under attack</Title>
    </Detail>
</Suggestions>
<TotalCount>12</TotalCount>
<requestId>F35F45B0-5D6B-4238-BE02-A62D0760E840</requestId>
</DescribeSecureSuggestionResponse>

```

JSON format

```

{
  "Suggestions": [{
    "Points": 40,
    "SuggestType": "SS_ALARM",
    "Detail": [{
      "Description": "You have 691 security alerts, which affects 56 assets",
      "SubType": "ALARM_HIGH",
      "Title": "You have unhandled high-risk alerts"
    }, {
      "Description": "You have 501 security alerts, which affects 119 assets",
      "SubType": "ALARM_MEDIUM",
      "Title": "You have unhandled medium-risk alerts"
    }
  ]
}, {
  "Points": 12,
  "SuggestType": "SS_VUL",
  "Detail": [{
    "Description": "You have five vulnerabilities",
    "SubType": "VUL_CMS",
    "Title": "You have unhandled CMS vulnerabilities"
  }], {

```

```
    "Description": "You have 107 vulnerabilities, which affects 68 servers",
    "SubType": "VUL_WIN",
    "Title": "You have unhandled Windows host vulnerabilities"
  }, {
    "Description": "You have 701 vulnerabilities, which affects 87 servers",
    "SubType": "VUL_LINUX",
    "Title": "You have unhandled Linux host vulnerabilities"
  }, {
    "Description": "You have one unhandled urgent vulnerability",
    "SubType": "VUL_EMR_UNFIX",
    "Title": "You have unhandled urgent vulnerabilities"
  }
]
}, {
  "Points": 2,
  "SuggestType": "SS_HC",
  "Detail": [{
    "Description": "You have 46 baseline check risks, which affects 260 servers",
    "SubType": "HC_WARN",
    "Title": "You have baseline check risks"
  }]
}, {
  "Points": 30,
  "SuggestType": "SS_AK",
  "Detail": [{
    "Description": "You have 12 potential AccessKey pair leaks",
    "SubType": "ACCESSKEY_LEAK",
    "Title": "You have potential AccessKey pair leaks"
  }]
}, {
  "Points": 35,
  "SuggestType": "SS_CLOUD_HC",
  "Detail": [{
    "Description": "You have four ApsaraDB RDS instances at risk",
    "SubType": "CLOUD_HC_RDS",
    "Title": "The check on security policies of ApsaraDB RDS instances has failed.
The instances are at risk"
  }, {
    "Description": "You have three high configuration risks for Alibaba Cloud servi
ces",
    "SubType": "CLOUD_HC_HIGH_LEVEL",
    "Title": "You have high configuration risks for Alibaba Cloud services"
  }, {
    "Description": "You have 28 medium or low configuration risks for Alibaba Cloud
services",
    "SubType": "CLOUD_HC_OTHER_LEVEL",
    "Title": "You have medium or low configuration risks for Alibaba cloud services
"
  }]
}, {
  "Points": 5,
  "SuggestType": "OTHER",
  "Detail": [{
    "Description": "You have been attacked 5,767 times",
    "SubType": "OTHER_ATTACH",
```

```
        "Title": "You are under attack."
      }
    }
  },
  "TotalCount": 12,
  "requestId": "F35F45B0-5D6B-4238-BE02-A62D0760E840"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.3. Security alerts

7.3.1. DescribeAlarmEventList

Queries alert events on the Alerts page. An alert event consists of alerts and exceptions. Each alert event is related to multiple exceptions.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeAlarmEventList	The operation that you want to perform. Set the value to DescribeAlarmEventList.
CurrentPage	Integer	Yes	1	The page number of the current page. Pages start from page 1. Default value: 1.
From	String	Yes	sas	The ID of the request source. Set the value to sas.
PageSize	String	Yes	20	The number of entries to return on each page. Default value: 20.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: zh: Chinese en: English

Parameter	Type	Required	Example	Description
Dealed	String	No	Y	The status of the alert event. Valid values: • N: unhandled • Y: handled
Levels	String	No	serious	The severity levels of the alert events. Separate multiple levels with commas (.). Valid values: • serious • suspicious • remind
Remark	String	No	database_server	The name of the alert, or the asset information.
GroupId	String	No	tst***	The group ID of the affected asset.
AlarmEventName	String	No	DDoS trojans	The name of the alert event.
AlarmEventType	String	No	Malicious process (cloud threat detection)	The type of the alert event.

Parameter	Type	Required	Example	Description
OperateErrorCode List.N	RepeatList	No	ignore. Success	Alert handling result code N. The value is in the format of Operation type.Operation result code. Operation types include: • Common: performs common operations. • deal: handles the alert. • ignore: ignores the alert. • offline_handled: marks the alert as handled. • mark_mis_info: marks the alerts as false positives by adding them to the whitelist. • rm_mark_mis_info: cancels false positives by removing the alerts from the whitelist. • quara: quarantines the source file of the malicious process. • kill_and_quara: kills the malicious process and quarantines the source file. • kill_virus: deletes the source file of the malicious process. • block_ip: blocks the source IP addresses. • manual_handled: manually handles the alert. Operation result codes: • Success: The operation is successful. • Failure: The operation fails. • AgentOffline: The agent is offline.

Response parameters

Parameter	Type	Example	Description
RequestId	String	28267723-D857-4DD8-B295-013100000000	The ID of the request.
SuspEvents	Array		The information about the alert event.
AlarmUniqueInfo	String	8df914418f4211fbf756efe7a6f40cbc	The ID of the alert event.

Parameter	Type	Example	Description
Solution	String	Check the malicious URLs that have been listed in the alert. Check the directory for malicious files. Terminate the malicious processes. If you manually run the processes, you can mark them as false positives in the console.	The solution to handle the alert event.
Level	String	serious	The severity level of the alert event. Valid values: • serious • suspicious • remind
CanBeDealOnline	Boolean	true	Indicates whether the online processing of the alert event is supported, such as quarantining the source file of the malicious process, adding the alert event to the whitelist, and ignoring the alert event. • true: Online processing is supported. • false: Online processing is not supported.
Description	String	After an attacker accesses a victim server, to keep the malicious programs running, the attacker may have imported malicious shell scripts into scheduled tasks such as crontab and systemd.	The description of the alert event.
StartTime	Long	1543740301000	The time when the alert event starts. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Example	Description
EndTime	Long	1543740301000	The time when the alert event ends. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
AlarmEventType	String	Suspicious processes	The type of the alert event.
SuspiciousEventCount	Integer	1	The number of exceptions related to the alert event.
Uuid	String	47900178-885d-4fa4-9d77-***	The ID of the related asset.
InstanceName	String	Test server	The name of the affected asset.
InternetIp	String	1.2.3.4	The public IP address of the affected asset.
IntranetIp	String	1.2.3.5	The private IP address of the affected asset.
AlarmEventName	String	Running malicious commands	The name of the alert event.
SafeVersion	String	1	The version in which the alert event detection can be enabled. Valid values: • 0: Basic Edition • 1: Enterprise Edition
DataSource	String	aegis_***	The source of data.
CanCancelFault	Boolean	false	Indicates whether you can cancel marking this alert event as a false positive.
Dealed	Boolean	false	Indicates whether the alert has been handled. Valid values: • true: handled • false: unhandled

Parameter	Type	Example	Description
GmtModified	Long	1569235879000	The last time when the alert was triggered. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
HasTraceInfo	Boolean	true	Indicates whether the alert has trace information. • true: The alert has trace information. • false: The alert does not have trace information.
SecurityEventIds	String	270789	The ID of the related exception.
OperateErrorCode	String	kill_and_quara.Succss	The handling result code of the alert event.
AlarmEventNameOriginal	String	Precise defense against malicious commands	The original parent name of the alert event.
Instanceld	String	i-e***	The ID of the affected asset.
PageInfo	Struct		The page information.
Count	Integer	1	The number of entries returned on the current page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	1	The total number of the alert events.
CurrentPage	Integer	1	The page number of the current page.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAlarmEventList
&CurrentPage=1
&From=sas
&PageSize=20
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeAlarmEventList>
  <RequestId>1D7FB2DD-4B80-41F4-94CF-C484EF6A5CAC</RequestId>
  <PageInfo>
    <Count>1</Count>
    <TotalCount>58</TotalCount>
    <PageSize>1</PageSize>
    <CurrentPage>1</CurrentPage>
  </PageInfo>
  <SuspEvents>
    <Uuid>c4678332-ef35-4ad4-8358-681ebbc0ccab</Uuid>
    <Dealed>true</Dealed>
    <SecurityEventIds>261401</SecurityEventIds>
    <Description>Cloud threat detection (mining programs)</Description>
    <CanCancelFault>false</CanCancelFault>
    <InstanceId>i-bp***</InstanceId>
    <OperateErrorCode></OperateErrorCode>
    <InternetIp>1.2.3.5</InternetIp>
    <GmtModified>1572524936000</GmtModified>
    <SuspiciousEventCount>1</SuspiciousEventCount>
    <HasTraceInfo>false</HasTraceInfo>
    <AlarmUniqueInfo>8b59e7bd134797758709983c26ece2a2</AlarmUniqueInfo>
    <AlarmEventName>Mining programs</AlarmEventName>
    <AlarmEventType>Precise defense</AlarmEventType>
    <IntranetIp>1.2.3.4</IntranetIp>
    <Level>serious</Level>
    <EndTime>1572524936000</EndTime>
    <StartTime>1572524936000</StartTime>
    <AlarmEventNameOriginal>Precise defense against mining programs</AlarmEventNameOriginal>
    <SaleVersion>0</SaleVersion>
    <CanBeDealOnLine>false</CanBeDealOnLine>
    <InstanceName>cit***</InstanceName>
  </SuspEvents>
</DescribeAlarmEventList>
```

JSON format

```
{
  "RequestId": "1D7FB2DD-4B80-41F4-94CF-C484EF6A5CAC",
  "PageInfo": {
    "Count": 1,
    "TotalCount": 58,
    "PageSize": 1,
    "CurrentPage": 1
  },
  "SuspEvents": [
    {
      "Uuid": "c4678332-ef35-4ad4-8358-681ebbc0ccab",
      "Dealed": true,
      "SecurityEventIds": "261401",
      "Description": "Cloud threat detection (mining programs)",
      "CanCancelFault": false,
      "InstanceId": "i-bp***",
      "OperateErrorCode": "",
      "InternetIp": "1.2.3.5",
      "GmtModified": 1572524936000,
      "SuspiciousEventCount": 1,
      "HasTraceInfo": false,
      "AlarmUniqueInfo": "8b59e7bd134797758709983c26ece2a2",
      "AlarmEventName": "Mining programs",
      "AlarmEventType": "Precise defense",
      "IntranetIp": "1.2.3.4",
      "Level": "serious",
      "EndTime": 1572524936000,
      "StartTime": 1572524936000,
      "AlarmEventNameOriginal": "Precise defense against mining programs",
      "SaleVersion": "0",
      "CanBeDealOnLine": false,
      "InstanceName": "cit***"
    }
  ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.3.2. DescribeAlarmEventDetail

Queries details of an alert event. An alert event consists of alerts and exceptions. Each alert event contains multiple exceptions.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeAlarmEventDetail	The operation that you want to perform. Set the value to DescribeAlarmEventDetail .
AlarmUniqueInfo	String	Yes	8df914418f4211fbf756efe7a6f40cbc	The ID of the alert event.  Note To query details of an alert event, you must specify the ID of the alert event. You can call the DescribeAlarmEventList operation to obtain the ID.
From	String	Yes	sas	The ID of the request source. Set the value to sas.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English

Response parameters

Parameter	Type	Example	Description
Data	Struct		The details of the alert event.
AlarmEventAliasName	String	Suspicious process behavior-execution of suspicious commands in scheduled Linux tasks	The complete name of the alert event.

Parameter	Type	Example	Description
AlarmEventDesc	String	After an attacker accesses a victim server, to keep the malicious programs running, the attacker may have imported malicious shell scripts into scheduled tasks such as crontab and systemd.	The description of the alert event.
AlarmUniqueInfo	String	8df914418f4211fbf756efe700000000	The ID of the alert event.
CanBeDealOnline	Boolean	false	Indicates whether processing alert events online is supported, such as blocking an alert, adding an alert to the whitelist, and ignoring an alert. Valid values: • true: Online processing is supported. • false: Online processing is not supported.
CanCancelFault	Boolean	false	Indicates whether you can cancel labelling this alert event as a false positive. Valid values: • true: You can cancel labeling this alert event as a false positive. • false: You cannot cancel labeling this alert event as a false positive.
CauseDetails	Array		The cause of the alert event (the information used to trace the alert).
Key	String	item	The format of the text. Valid values: • text • html
Value	Array		The value of the field displaying the information used to trace alerts.
Name	String	Solutions	The key of the field displaying the information used to trace alerts.

Parameter	Type	Example	Description
Type	String	html	The format of the field displaying the information used to trace alerts.
Value	String	Check for the exploited pages of your Web services and vulnerabilities in parameter configuration, and resolve these issues.	The value of the field displaying the information used to trace alerts.
DataSource	String	aegis_***	The source of data.
EndTime	Long	1542366542000	The end time of the alert event.
InstanceName	String	Test server	The name of the associated instance.
InternetIp	String	1.2.3.1	The public IP address of the associated instance.
IntranetIp	String	1.2.3.5	The private IP address of the associated instance.
Level	String	serious	The level of the alert event. Valid values: • serious • suspicious • remind
Solution	String	Check the malicious URLs that have been listed in the alert. Check the directory for malicious file downloads. Stop the malicious processes that are running. If you trust the processes, mark the alert as a false positive in the console, and submit a ticket to security engineers.	The solution to the alert event.

Parameter	Type	Example	Description
StartTime	Long	1542378601000	The timestamp when the alert event was detected.
Type	String	Suspicious network connections	The type of the alert event.
Uuid	String	47900178-885d-4fa4-9d77-XXXXXXXXXXXX	The ID of the related instance.
RequestId	String	5A1DDB3C-798C-4A84-BF6E-3DC700000000	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeAlarmEventDetail
&AlarmUniqueInfo=8df914418f4211fbf756efe7a6f40cbc
&From=sas
&<Common request parameters>
```

Sample success responses

`XML` format

```

<DescribeAlarmEventDetailResponse>
  <Data>
    <Uuid>47900178-885d-4fa4-9d77-XXXXXXXXXXXX</Uuid>
    <AlarmEventAliasName>Suspicious Process - Command Exceptions in Scheduled Linux Tasks</AlarmEventAliasName>
    <Type>Suspicious process behavior</Type>
    <InternetIp>1.2.3.1</InternetIp>
    <AlarmEventDesc>After accessing a victim server, the attacker may have imported malicious shell scripts into scheduled tasks such as crontab and systemd, to enable persistent execution of malicious backdoor programs. </AlarmEventDesc>
    <IntranetIp>1.2.3.5</IntranetIp>
    <CauseDetails>
      <Value>
        <Type>text</Type>
        <Value>An attacker has logged on to your server and has written webshells by editing the configuration file.</Value>
        <Name>Intrusion cause</Name>
      </Value>
      <Value>
        <Type>text</Type>
        <Value>2018-11-16 19:09:02</Value>
        <Name>Attack time</Name>
      </Value>
      <Value>
        <Type>text</Type>
        <Value>N/A</Value>
        <Name>Source IP of attack</Name>
      </Value>
      <Value>
        <Type>text</Type>
        <Value>N/A</Value>
        <Name>Payload of attack</Name>
      </Value>
      <Value>
        <Type>text</Type>
        <Value>Check for the exploited pages of your Web services and vulnerabilities in parameter configuration, and resolve these issues. </Value>
        <Name>Solutions</Name>
      </Value>
    </CauseDetails>
    <Level>serious</Level>
    <EndTime>1543741201000</EndTime>
    <StartTime>1543312803000</StartTime>
    <CanBeDealOnLine>false</CanBeDealOnLine>
    <InstanceName>serve***</InstanceName>
  </Data>
  <RequestId>5A1DDB3C-798C-4A84-BF6E-3DC7F7D7EB4A</RequestId>
</DescribeAlarmEventDetailResponse>

```

JSON format

```
{
  "Data": {
    "Uuid": "47900178-885d-4fa4-9d77-XXXXXXXXXXXX",
    "AlarmEventAliasName": "Suspicious process behavior-execution of suspicious commands in scheduled Linux tasks",
    "Type": "Suspicious process behavior",
    "InternetIp": "1.2.3.1",
    "AlarmEventDesc": "After an attacker accesses a victim server, to keep the malicious programs running, the attacker may have imported malicious shell scripts into scheduled tasks such as crontab and systemd.",
    "IntranetIp": "1.2.3.5",
    "CauseDetails": [
      {
        "Value": [
          {
            "Type": "text",
            "Value": "An attacker has logged on to your ECS instance and has written webshells by editing files.",
            "Name": "Intrusion cause"
          },
          {
            "Type": "text",
            "Value": "2018-11-16 19:09:02",
            "Name": "Time of attack"
          },
          {
            "Type": "text",
            "Value": "N/A",
            "Name": "Source IP of attack"
          },
          {
            "Type": "text",
            "Value": "N/A",
            "Name": "Payload of attack"
          },
          {
            "Type": "text",
            "Value": "Check for the exploited pages of your Web services and vulnerabilities in parameter configuration, and resolve these issues.",
            "Name": "Solutions"
          }
        ],
        "Key": "item"
      }
    ],
    "Level": "serious",
    "EndTime": 1543741201000,
    "StartTime": 1543312803000,
    "CanBeDealOnline": false,
    "InstanceName": "serve***"
  },
  "RequestId": "5A1DDB3C-798C-4A84-BF6E-3DC7F7D7EB4A"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.3.3. DescribeSuspEvents

Queries information about exceptions. An alert event consists of alerts and exceptions. Each alert event is related to multiple exceptions.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSuspEvents	The operation that you want to perform. Set the value to DescribeSuspEvents .
From	String	Yes	sas	The data source on which the exception is detected. Set the value to sas.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Dealed	String	No	N	The status of the exception. Valid values: • N: unhandled • Y: handled
Name	String	No	ecs-xxx	The name of the exception or the affected server. Fuzzy match is supported.
Levels	String	No	serious	The severity levels of the alert events. Separate multiple levels with commas (.). The following levels are listed in descending order. • serious • suspicious • remind
ParentEventTypes	String	No	Webshells	The type of the alert event to which the exception is related.
Remark	String	No	Test server	The IP address or name of the server.

Parameter	Type	Required	Example	Description
PageSize	String	No	20	The number of entries to return on each page. Default value: 20.
CurrentPage	String	No	1	The page number of the current page.
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
AlarmUniqueInfo	String	No	8df914418f4211f bf***	The alert event to which the exception is related.  Note To query details about exceptions of an alert event, you must provide the ID of the alert event. You can call the DescribeAlarmEventList operation to obtain the ID.

Response parameters

Parameter	Type	Example	Description
RequestId	String	43F670F3-AB40-4E91-BC7D-C57400000000	The ID of the request.
Count	Integer	1	The number of entries returned on the current page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	100	The total number of the exceptions.
CurrentPage	Integer	1	The page number of the current page.
SuspEvents	Array		The details of the exception.
LastTime	String	2018-09-26 01:51:01	The last time when the exception occurred.

Parameter	Type	Example	Description
OccurrenceTime	String	2018-09-26 01:51:01	The first time when the exception occurred.
Id	Long	1000	The ID of the exception to query.
UniqueInfo	String	e17e***	The ID of the exception.
InstanceName	String	nginx	The name of the related asset.
InternetIp	String	1.2.3.1	The public IP address of the related asset.
IntranetIp	String	1.2.3.5	The private IP address of the related asset.
Uuid	String	bf6b30d3-eea8-4924-9f0a-***	The ID of the related asset.
Name	String	Malicious processes (cloud threat detection) - XOR DDoS trojan	The complete name of the exception.
EventSubType	String	XorDDoS trojan	The name of the exception.
Level	String	serious	The severity level of the exception. Valid values: • serious • suspicious • remind
EventStatus	Integer	1	The status of the exception. Valid values: • 1: unhandled • 2: ignored • 4: confirmed • 8: marked as false positive • 16: handling • 32: handled • 64: expired
Desc	String	webshell	The impact of the exception.

Parameter	Type	Example	Description
OperateMsg	String	success	The operation remarks of the exception.
DataSource	String	aegis_suspicious_***	The data source.
CanBeDealOnline	Boolean	true	Indicates whether the online processing of the exception is supported. The processing includes quarantining the exception. Valid values: • true: Online processing is supported. • false: Online processing is not supported.
SaleVersion	String	1	The version in which the exception detection can be enabled. Valid values: • 0: Basic Edition • 1: Enterprise Edition
AlarmEventType	String	Suspicious processes	The type of the alert event.
AlarmEventName	String	Suspicious command running in scheduled Linux tasks	The name of the alert event.
AlarmUniqueInfo	String	8df914418f***	The ID of the alert event.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSuspEvents
&From=saas
&<Common request parameters>
```

Sample success responses

XML format

```

<DescribeSuspEvents>
  <TotalCount>3</TotalCount>
  <Count>2</Count>
  <PageSize>20</PageSize>
  <RequestId>0C7FAD74-83FA-4671-9250-A5F2A64F437A</RequestId>
  <CurrentPage>1</CurrentPage>
  <SuspEvents>
    <EventStatus>1</EventStatus>
    <SaleVersion>1</SaleVersion>
    <IntranetIp>1.2.3.4</IntranetIp>
    <EventSubType>XOR DDoS trojan</EventSubType>
    <Name>Malicious processes (cloud threat detection) - XOR DDoS trojan</Name>
    <DataSource>aegis_suspiciou***</DataSource>
    <OccurrenceTime>2018-09-26 01:51:01</OccurrenceTime>
    <InstanceName>server01</InstanceName>
    <Desc>After accessing the server, XOR DDoS trojan may have injected malicious code
into Linux scheduled tasks. </Desc>
    <CanBeDealOnLine>>false</CanBeDealOnLine>
    <Uuid>bf6b30d3-eea8-4924***</Uuid>
    <InternetIp>1.2.3.4</InternetIp>
    <Level>serious</Level>
    <Id>3682</Id>
    <LastTime>2018-10-24 21:06:01</LastTime>
  </SuspEvents>
  <SuspEvents>
    <EventStatus>1</EventStatus>
    <SaleVersion>1</SaleVersion>
    <IntranetIp>1.2.3.5</IntranetIp>
    <EventSubType>XOR DDoS trojan</EventSubType>
    <Name>Malicious processes (cloud threat detection) - XOR DDoS trojan</Name>
    <DataSource>aegis_suspiciou***</DataSource>
    <OccurrenceTime>2018-09-26 02:01:01</OccurrenceTime>
    <InstanceName>server01</InstanceName>
    <Desc>After accessing the server, XOR DDoS trojan may have injected malicious code
into Linux scheduled tasks. </Desc>
    <CanBeDealOnLine>>false</CanBeDealOnLine>
    <Uuid>bf6b30d3-eea8-4924***</Uuid>
    <InternetIp>1.2.3.4</InternetIp>
    <Level>serious</Level>
    <Id>3683</Id>
    <LastTime>2018-10-24 21:01:01</LastTime>
  </SuspEvents>
</DescribeSuspEvents>

```

JSON **format**

```
{
  "TotalCount": 3,
  "Count": 2,
  "PageSize": 20,
  "RequestId": "0C7FAD74-83FA-4671-9250-A5F2A64F437A",
  "CurrentPage": 1,
  "SuspEvents": [
    {
      "EventStatus": 1,
      "SaleVersion": "1",
      "IntranetIp": "1.2.3.4",
      "EventSubType": "XOR DDoS trojan"
      "Name": "Malicious processes (cloud threat detection) - XOR DDoS trojan",
      "DataSource": "aegis suspiciou***",
      "OccurrenceTime": "2018-09-26 01:51:01",
      "InstanceName": "server01",
      "Desc": "After accessing the server, XOR DDoS trojan may have injected maliciou
s code into Linux scheduled tasks.",
      "CanBeDealOnLine": false,
      "Uuid": "bf6b30d3-eea8-4924***",
      "InternetIp": "1.2.3.4",
      "Level": "serious",
      "Id": 3682,
      "LastTime": "2018-10-24 21:06:01"
    },
    {
      "EventStatus": 1,
      "SaleVersion": "1",
      "IntranetIp": "1.2.3.5",
      "EventSubType": "XOR DDoS trojan"
      "Name": "Malicious processes (cloud threat detection) - XOR DDoS trojan",
      "DataSource": "aegis_suspiciou***",
      "OccurrenceTime": "2018-09-26 02:01:01",
      "InstanceName": "server01",
      "Desc": "After accessing the server, XOR DDoS trojan may have injected maliciou
s code into Linux scheduled tasks.",
      "CanBeDealOnLine": false,
      "Uuid": "bf6b30d3-eea8-4924-***",
      "InternetIp": "1.2.3.4",
      "Level": "serious",
      "Id": 3683,
      "LastTime": "2018-10-24 21:01:01"
    }
  ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.3.4. DescribeSuspEventDetail

Queries details of a specific exception. An alert event consists of alerts and exceptions. Each alert event is related to multiple exceptions.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSuspEventDetail	The operation that you want to perform. Set the value to DescribeSuspEventDetail .
From	String	Yes	sas	The data source on which the exception is detected. Set the value to sas.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
SuspiciousEventId	Integer	No	1	The ID of the exception to query.  Note To query the details of an exception, you must provide the ID of the exception. You can call the DescribeSuspEvents operation to obtain the ID.

Response parameters

Parameter	Type	Example	Description
RequestId	String	1	The ID of the request.
LastTime	String	2018-10-30 11:43:46	The last time when the exception occurred.
Id	Integer	1991	The ID of the exception to query.
InstanceName	String	ca_cpm_test1	The name of the related asset.

Parameter	Type	Example	Description
InternetIp	String	1.2.3.5	The public IP address of the related asset.
IntranetIp	String	1.2.3.1	The private IP address of the related asset.
Uuid	String	bffb12c3-590a-4db2-b538-***	The ID of the related asset.
EventDesc	String	This file may have been uploaded by an attacker that has intruded into your website. Check the validity of this file.	The description of the exception.
EventTypeDesc	String	Webshell - Webshell	The type of the exception.
Level	String	serious	The severity level of the exception. Valid values: • serious • suspicious • remind
EventStatus	String	1	The status of the exception. Valid values: • 1: unhandled • 2: ignored • 4: confirmed • 8: marked as false positive • 16: handling • 32: handled • 64: expired
SaleVersion	String	1	The version in which exception detection can be enabled. Valid values: • 0: Basic Edition • 1: Enterprise Edition
DataSource	String	aegis_suspicious_***	The data source on which the exception is detected.
OperateMsg	String	success	The operation remarks of the exception.

Parameter	Type	Example	Description
SasId	String	1sdeswdd****	The ID of the service in Threat Detection Service.
EventName	String	WEBSHELL	The name of the exception.
CanBeDealOnline	Boolean	true	Indicates whether the online processing of the exception is supported. Valid values: • true: Online processing is supported. • false: Online processing is not supported.
Details	Array		The details of the exception.
Name	String	The update time.	The name in the exception details.
Type	String	html	The format in the exception details. Valid values: • text • html
InfoType	String	download_url	The type of the icon.
Value	String	2018-12-12 12:00:00	The content in the exception details.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSuspEventDetail
&From=sas
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeSuspEventDetailResponse>
  <RequestId>43F670F3-AB40-4E91-BC7D-C57468834F67</RequestId>
  <EventDesc>This file may have been uploaded by an attacker that has intruded into your website. Check the validity of this file. </EventDesc>
  <EventTypeDesc>Webshell - Webshell</EventTypeDesc>
  <EventStatus>1</EventStatus>
  <EventName>WEBSHELL</EventName>
  <SaleVersion>1</SaleVersion>
  <IntranetIn>1 2 3 4</IntranetIn>
```

```
<InstanceIp>1.2.3.4</InstanceIp>
<DataSource>aegis_suspicious_***</DataSource>
<InstanceName>ca_***</InstanceName>
<CanBeDealOnLine>true</CanBeDealOnLine>
<OperateMsg></OperateMsg>
<Uuid>bfffb12c3-590a-4db2-b538-***</Uuid>
<Details>
  <Type>text</Type>
  <Value>/data/ftpUser/pub/***</Value>
  <InfoType>trojan_path</InfoType>
  <Name>Trojan path</Name>
</Details>
<Details>
  <Type>text</Type>
  <Value>--</Value>
  <Name>Affected domain</Name>
</Details>
<Details>
  <Type>text</Type>
  <Value>2018-10-30 05:00:56</Value>
  <InfoType>frist_found_time</InfoType>
  <Name>First detected time</Name>
</Details>
<Details>
  <Type>text</Type>
  <Value>2018-10-30 11:43:45</Value>
  <InfoType>update_time</InfoType>
  <Name>Update time</Name>
</Details>
<Details>
  <Type>text</Type>
  <Value>Webshell</Value>
  <InfoType>trojan_type</InfoType>
  <Name>Trojan type</Name>
</Details>
<Details>
  <Type>html</Type>
  <Value>&lt;a href="http:// bucket"&gt; Download&lt;/a&gt;</Value>
  <InfoType>download_url</InfoType>
  <Name>Source file download</Name>
</Details>
<InternetIp>1.2.3.5</InternetIp>
<Level>serious</Level>
<Id>129636</Id>
<LastTime>2018-10-30 11:43:46</LastTime>
<SasId>39938056</SasId>
</DescribeSuspEventDetailResponse>
```

JSON format

```
{
  "RequestId": "43F670F3-AB40-4E91-BC7D-C57468834F67",
  "EventDesc": "This file may have been uploaded by an attacker that has intruded into yo
ur website. Check the validity of this file.",
```

```
"EventTypeDesc": "Webshell - Webshell",
"EventStatus": 1,
"EventName": "WEBSHELL",
"SaleVersion": "1",
"IntranetIp": "1.2.3.4",
"DataSource": "aegis_suspicious_***",
"InstanceName": "ca_***",
"CanBeDealOnLine": true,
"OperateMsg": "",
"Uuid": "bffb12c3-590a-4db2-b538-***",
"Details": [
  {
    "Type": "text",
    "Value": "/data/ftpUser/pub/***",
    "InfoType": "trojan_path",
    "Name": "Trojan path",
  },
  {
    "Type": "text",
    "Value": "--",
    "Name": "Affected domain",
  },
  {
    "Type": "text",
    "Value": "2018-10-30 05:00:56",
    "InfoType": "frist_found_time",
    "Name": "First detected time",
  },
  {
    "Type": "text",
    "Value": "2018-10-30 11:43:45",
    "InfoType": "update_time",
    "Name": "Update time",
  },
  {
    "Type": "text",
    "Value": "Webshell",
    "InfoType": "trojan_type",
    "Name": "Trojan type",
  },
  {
    "Type": "html",
    "Value": "<a href=\" http:// ${*}\"> Download </a>",
    "InfoType": "download_url",
    "Name": "Source file download",
  }
],
"InternetIp": "1.2.3.5",
"Level": "serious",
"Id": 129636,
"LastTime": "2018-10-30 11:43:46",
"SasId": "39938056"
}
```


Error codes

For a list of error codes, see [Error codes](#).

7.4. Configuration assessment

7.4.1. DescribeRiskItemType

Queries types of check items for cloud service configurations. Each check item is categorized into a type. Types of check items include identity authentication and permissions, network access control, log auditing, data security, monitoring and alerting, and basic security protection.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeRiskItemType	The operation that you want to perform. Set the value to DescribeRiskItemType.
Lang	String	No	zh	The natural language of the request and response. Valid values: zh: Chinese en: English
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
List	Array		The information about the check item.
Id	Long	1	The ID of the check item.
Title	String	Identity authentication and permissions	The type of the check item. Example: Identity authentication and permissions.
RequestId	String	3B3F3A90-46A5-4023-A2D8-D68B14262F96	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeRiskItemType  
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeRiskItemType>  
  <RequestId>3B3F3A90-46A5-4023-A2D8-D68B14262F96</RequestId>  
  <List>  
    <Title>Identity authentication and permissions</Title>  
    <Id>1</Id>  
  </List>  
  <List>  
    <Title>Network access control</Title>  
    <Id>2</Id>  
  </List>  
  <List>  
    <Title>Log auditing</Title>  
    <Id>3</Id>  
  </List>  
  <List>  
    <Title>Data security</Title>  
    <Id>4</Id>  
  </List>  
  <List>  
    <Title>Basic security protection</Title>  
    <Id>6</Id>  
  </List>  
</DescribeRiskItemType>
```

JSON format

```
{
  "RequestId": "3B3F3A90-46A5-4023-A2D8-D68B14262F96",
  "List": [
    {
      "Id": 1,
      "Title": "Identity authentication and permissions"
    },
    {
      "Id": 2,
      "Title": "Network access control"
    },
    {
      "Id": 3,
      "Title": "Log auditing"
    },
    {
      "Id": 4,
      "Title": "Data security"
    },
    {
      "Id": 6,
      "Title": "Basic security protection"
    }
  ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.4.2. StartBaselineSecurityCheck

Checks cloud service configurations. You can check all items or a specific item, and you can verify whether an item is already checked.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	StartBaselineSecurityCheck	The operation that you want to perform. Set the value to StartBaselineSecurityCheck .
Type	String	Yes	check	The type of the check task. Valid values: • check • verify

Parameter	Type	Required	Example	Description
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
ItemIds.N	RepeatList	No	1	The ID of the check item.  Note To perform the check task on cloud service configurations, you must provide the ID of the check item. You can call the DescribeRiskItemType operation to obtain the ID.

Response parameters

Parameter	Type	Example	Description
RequestId	String	48D2E9A9-A1B0-4295-B727-0995757C47E9	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=StartBaselineSecurityCheck
&Type=check
&<Common request parameters>
```

Sample success responses

XML format

```
<StartBaselineSecurityCheckResponse>
  <RequestId>48D2E9A9-A1B0-4295-B727-0995757C47E9</RequestId>
</StartBaselineSecurityCheckResponse>
```

JSON format

```
{
  "RequestId": "48D2E9A9-A1B0-4295-B727-0995757C47E9"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.4.3. DescribeRiskCheckSummary

Queries the summary of check items for cloud service configurations. The operation returns the following information: the number of risk items, the risk rate, the number of affected assets, the last check time, and the statistics of each type of check items.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeRiskCheckSummary	The operation that you want to perform. Set the value to DescribeRiskCheckSummary.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: zh: Chinese en: English

Response parameters

Parameter	Type	Example	Description
RequestId	String	291B49F9-1685-4005-9D34-606B6F78740F	The ID of the request.
RiskCheckSummary	Struct		The summary of check items for cloud service configurations.
RiskCount	Integer	1	The number of risk items.
PreviousCount	Integer	0	The number of risk items in the last check.
ItemCount	Integer	4	The number of check items.

Parameter	Type	Example	Description
RiskRate	Float	0.25	The proportion of risk items in the total number to check items.
AffectedAssetCount	Integer	0	The number of affected assets.
PreviousTime	Long	1545012926000	The timestamp of the last check.
EnabledRiskCount	Integer	3	The number of check items that passed the check.
DisabledRiskCount	Integer	0	The number of risk items that failed to pass the check.
RiskLevelCount	Array		The number of risk items for each level. • high • medium • low
Key	String	medium	The severity level of the risk item.
Count	Integer	1	The number of risk items.
Groups	Array		The types of check items.
Id	Long	1	The type ID of the check item.
Title	String	Identity authentication and permissions	The type of the check item.
Status	String	finish	Indicates whether the check is finished. • finish: The check is finished. • Running: The check is in process. • waiting: The check is pending. • NoStart: The check is not started.
RemainingTime	Integer	0	The time when the next check will be performed.

Parameter	Type	Example	Description
Sort	Integer	1	The sequence number of the check item type in the All Types drop-down list in the console.
CountByStatus	Array		The statistics of check results.
Status	String	pass	The status of the check item after the check is finished. Valid values: • pass: The check item is normal. • failed: The check item is at risk.
Count	Integer	2	The number of risk items.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeRiskCheckSummary
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeRiskCheckSummary>
  <RequestId>291B49F9-1685-4005-9D34-606B6F78740F</RequestId>
  <RiskCheckSummary>
    <RiskCount>1</RiskCount>
    <RiskRate>0.25</RiskRate>
    <PreviousTime>1545012926000</PreviousTime>
    <ItemCount>4</ItemCount>
    <AffectedAssetCount>0</AffectedAssetCount>
    <RiskLevelCount>
      <Count>1</Count>
      <Key>medium</Key>
    </RiskLevelCount>
    <Groups>
      <Status>finish</Status>
      <CountByStatus>
        <Status>exception</Status>
        <Count>2</Count>
      </CountByStatus>
      <RemainingTime>0</RemainingTime>
      <Sort>1</Sort>
      <Title>Identity authentication and permissions</Title>
      <Id>1</Id>
    </Groups>
  </RiskCheckSummary>
</DescribeRiskCheckSummary>
```

```

        <Status>finish</Status>
        <CountByStatus>
            <Status>exception</Status>
            <Count>5</Count>
        </CountByStatus>
        <RemainingTime>0</RemainingTime>
        <Sort>2</Sort>
        <Title>Network access control</Title>
        <Id>2</Id>
    </Groups>
    <Groups>
        <Status>finish</Status>
        <CountByStatus>
            <Status>pass</Status>
            <Count>1</Count>
        </CountByStatus>
        <RemainingTime>0</RemainingTime>
        <Sort>3</Sort>
        <Title>Log auditing</Title>
        <Id>3</Id>
    </Groups>
    <Groups>
        <Status>finish</Status>
        <CountByStatus>
            <Status>exception</Status>
            <Count>2</Count>
        </CountByStatus>
        <RemainingTime>0</RemainingTime>
        <Sort>4</Sort>
        <Title>Data security</Title>
        <Id>4</Id>
    </Groups>
    <Groups>
        <Status>finish</Status>
        <CountByStatus>
            <Status>exception</Status>
            <Count>2</Count>
        </CountByStatus>
        <RemainingTime>0</RemainingTime>
        <Sort>6</Sort>
        <Title>Basic security protection</Title>
        <Id>6</Id>
    </Groups>
    <PreviousCount>0</PreviousCount>
</RiskCheckSummary>
</DescribeRiskCheckSummary>

```

JSON format

```

{
  "RequestId": "291B49F9-1685-4005-9D34-606B6F78740F",
  "RiskCheckSummary": {
    "RiskCount": 1,

```



```
"RiskRate": 0.25,
"PreviousTime": 1545012926000,
"ItemCount": 4,
"AffectedAssetCount": 0,
"RiskLevelCount": [
  {
    "Count": 1,
    "Key": "medium"
  }
],
"Groups": [
  {
    "Status": "finish",
    "CountByStatus": [
      {
        "Status": "exception",
        "Count": 2
      }
    ],
    "RemainingTime": 0,
    "Sort": 1,
    "Title": "Identity authentication and permissions",
    "Id": 1
  },
  {
    "Status": "finish",
    "CountByStatus": [
      {
        "Status": "exception",
        "Count": 5
      }
    ],
    "RemainingTime": 0,
    "Sort": 2,
    "Title": "Network access control",
    "Id": 2
  },
  {
    "Status": "finish",
    "CountByStatus": [
      {
        "Status": "pass",
        "Count": 1
      }
    ],
    "RemainingTime": 0,
    "Sort": 3,
    "Title": "Log auditing",
    "Id": 3
  },
  {
    "Status": "finish",
    "CountByStatus": [
      {
        "Status": "exception"
```

```
        "Status": "exception",
        "Count": 2
    },
    ],
    "RemainingTime": 0,
    "Sort": 4,
    "Title": "Data security",
    "Id": 4
},
{
    "Status": "finish",
    "CountByStatus": [
        {
            "Status": "exception",
            "Count": 2
        }
    ],
    "RemainingTime": 0,
    "Sort": 6,
    "Title": "Basic security protection",
    "Id": 6
}
],
"PreviousCount": 0
}
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.4.4. DescribeRiskCheckResult

Queries the results of check items by type or name.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeRiskCheckResult	The operation that you want to perform. Set the value to DescribeRiskCheckResult .
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
GroupId	Long	No	21000	The type ID of the check item. Valid values: • 1: identity authentication and permissions • 2: network access control • 3: log audit • 4: data security • 5: monitoring and alerting • 6: basic security protection
CurrentPage	Integer	No	1	The page number of the current page.
RiskLevel	String	No	high	The risk level of the check item. Valid values: • high • medium • low
Status	String	No	pass	The status of the check result. Valid values: • pass • failed • running • waiting • ignored • falsePositive
ItemIds.N	RepeatList	No	sde***	The ID of check item N. For more information about the description of the check item specified by this parameter, see the check item table in the "Response parameters" section of this topic.

Parameter	Type	Required	Example	Description
AssetType	String	No	RDS	The type of the cloud service. For more information about the description of the cloud service specified by this parameter, see the check item table in the "Response parameters" section of this topic.
Name	String	No	Cloud platform - Multi-factor authentication (MFA) configuration of Apsara Stack tenant accounts	The name of the check item. For more information about the description of the check item name, see the check item table in the "Response parameters" section of this topic.
PageSize	Integer	No	10	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
Count	Integer	10	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
List	Array		The information about the check item.
AffectedCount	Integer	0	The number of the affected assets.
CheckTime	Long	1543991525000	The time when the last check was performed. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
ItemId	Long	1	The ID of the check item. For more information about the description of the check item specified by this parameter, see the check item table in the "Response parameters" section of this topic.

Parameter	Type	Example	Description
RemainingTime	Integer	0	The time when the next check will be performed.
RepairStatus	String	disabled	Indicates whether the risk of the check item can be fixed. Valid values: • enabled: The risk can be fixed. • disabled: The risk cannot be fixed.
RiskAssertType	String	ECS	The type of the affected asset.
RiskItemResources	Array		The details of the check item.
ContentResource	Json	<pre>{"type": "link", "value": "Risk: MFA is disabled\n", "url": "https://***.aliyun.c om/#/secure\n" }</pre>	The content in the check item details.
ResourceName	String	bestPractice	The title in the check item details. Valid values: • bestPractice: description • influence: risk • suggestion: solution • helpResource: reference
RiskLevel	String	high	The risk level of the check item. Valid values: • high • medium • low
Sort	Integer	1	The sequence number of the check result. The check items are sorted based on the sequence number.
StartStatus	String	enabled	Indicates whether the check item is supported by the cloud service. Valid values: • enabled: supported • disable: unsupported

Parameter	Type	Example	Description
Status	String	pass	The status of the check result. Valid values: • pass • failed • running • waiting • ignored • falsePositive
TaskId	Long	647189	The ID of the check task.
Title	String	Cloud platform - MFA configuration of Apsara Stack tenant accounts	The name of the check item.
Type	String	Identity authentication and permissions	The type of the check item. Valid values: • Identity authentication and permissions • Network access control • Log audit • Data security • Monitoring and alerting • Basic security protection
PageCount	Integer	20	The total number of pages returned.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	AD271C07-4ACE- 413D-AA9B- F14FD3B7717F	The ID of the request.
TotalCount	Integer	12	The total number of entries returned.

The following table describes the check items supported by the cloud platform, including the ID, name, type, risk level, and service type.

ItemId	Name	GroupId	RiskLevel	AssetType	Description

ItemId	Name	GroupId	RiskLevel	AssetType	Description
1	ActionTrail - Logging configuration	3: log audit	medium	ActionTrail	Checks whether you enable ActionTrail to record operations logs on the cloud and save the logs to Object Storage Service (OSS) buckets.
2	ApsaraDB RDS - Database security policy	4: data security	medium	RDS	Checks whether you enable Secure Sockets Layer (SSL), Transparent Data Encryption (TDE), and SQL audit services for each ApsaraDB RDS instance.
3	Apsara Stack tenant account security - MFA	1: identity authentication and permissions	high	RAM	Checks whether MFA is enabled for Apsara Stack tenant accounts.
					Checks whether actual IP addresses of backend servers are hidden after you use Anti-DDoS Pro or Anti-DDoS Premium. If the actual IP addresses are hidden,

ItemId	Name	GroupId	RiskLevel	AssetType	Description
4	Apsara Stack Security - Back-to-origin configurations of Anti-DDoS Pro or Anti-DDoS Premium	2: network access control	high	DDOS	attackers can directly access the actual IP addresses. <note> To hide the actual IP addresses, you can configure whitelist policies, for example, when the actual IP addresses are the IP addresses of Server Load Balancer (SLB) instances. When the IP addresses are the IP addresses of Elastic Compute Service (ECS) instances, you can configure access control policies for ECS security groups. All these policies allow access from only back-to-origin IP addresses of Anti-DDoS Pro or Anti-DDoS Premium. </note>

ItemId	Name	GroupId	RiskLevel	AssetType	Description
5	ApsaraDB RDS - Whitelist configuration	2: network access control	high	RDS	Checks whether the RDS access control policy is set to 0.0.0.0/0, which allows requests from all IP addresses. We recommend that you limit the access scope to a specific range of IP addresses rather than exposing database services to the Internet.
6	SLB - High-risk port	2: network access control	high	SLB	Checks whether SLB forwards requests from high-risk ports to the Internet.

ItemId	Name	GroupId	RiskLevel	AssetType	Description
7	Apsara Stack Security - Back-to-origin configurations of Web Application Firewall (WAF)	2: network access control	high	WAF	Checks whether the actual IP addresses of backend servers are hidden after you use WAF. If the actual IP addresses are hidden, attackers cannot directly access the actual IP addresses. To hide the actual IP addresses, you can configure whitelist policies, for example, when the actual IP addresses are the IP addresses of SLB instances. When the IP addresses are the IP addresses of ECS instances, you can configure access control policies for ECS security groups. All these policies allow access from only back-to-origin IP addresses of WAF.

ItemId	Name	GroupId	RiskLevel	AssetType	Description
8	Apsara Stack Security - Threat Detection Service agent online status	6: basic security protection	high	ECS	Checks whether the Threat Detection Service agent on the ECS instance is always online and provides protection.
12	OSS - Bucket access permissions	4: data security	high	OSS	Checks whether the access permission on your OSS buckets is public-read or public-read-write. If yes, the check fails.
13	Threat Detection Service - AccessKey leak detection	5: monitoring and alerting	medium	RAM	Checks whether AccessKey leak detection is enabled. If no, the check fails.

ItemId	Name	GroupId	RiskLevel	AssetType	Description
14	ApsaraDB for MongoDB - Whitelist configuration	2: network access control	high	MongoDB	Checks whether the whitelist is enabled for ApsaraDB for MongoDB instances. If the whitelist is enabled and set to 0.0.0.0/0, which allows access from all devices, the check fails.
15	RAM - MFA configuration for RAM users	1: identity authentication and permissions	medium	RAM	Checks whether MFA is enabled for RAM users.
16	OSS - Logging configuration	4: data security	medium	OSS	Checks whether the logging feature is enabled for all OSS buckets. If no, the check fails.

ItemId	Name	GroupId	RiskLevel	AssetType	Description
17	OSS - Cross-region replication configuration	4: data security	low	OSS	Checks whether the cross-region replication is enabled for all OSS buckets. If no, the check fails.
18	ApsaraDB RDS - Backup configuration	4: data security	medium	RDS	Checks whether database backup is enabled for ApsaraDB RDS instances. If no, the check fails.
19	KVStore for Redis - Whitelist configuration	2: network access control	high	Redis	Checks access control configurations of KVStore for Redis.
20	ECS - SSH key pairs	1: identity authentication and permissions	medium	ECS	Checks whether SSH key pair-based logons are enabled for ECS instances.
21	SLB - Health status	5: monitoring and alerting	low	SLB	Checks the health status of SLB instances.

ItemId	Name	GroupId	RiskLevel	AssetType	Description
22	PolarDB - Whitelist configuration	2: network access control	medium	POLARDB	Checks the whitelist configured for PolarDB. If the whitelist is enabled and set to 0.0.0.0/0, which allows access from all devices, the check fails.
23	AnalyticDB for PostgreSQL - Whitelist configuration	2: network access control	medium	PostgreSQL	Checks the whitelist configured for AnalyticDB for PostgreSQL instances. If the whitelist is enabled and set to 0.0.0.0/0, which allows access from all devices, the check fails.
24	ECS - Storage encryption	4: data security	low	ECS	Checks whether storage encryption is enabled. If no, the check fails.
25	SLB - Whitelist configuration	2: network access control	medium	SLB	Checks SLB whitelist configurations . If the whitelist is enabled and set to 0.0.0.0/0, which allows access from all devices, the check fails.

ItemId	Name	GroupId	RiskLevel	AssetType	Description
26	SLB - Certificate expiration	5: monitoring and alerting	medium	SLB	Checks whether the SLB certificate has expired.
27	ECS - Automatic snapshot policy	4: data security	medium	ECS	Checks whether automatic snapshot policies are enabled for ECS instances.
28	SSL certificate - Expiration check	4: data security	medium	SSL	Checks whether the SSL certificate is within its validity period.
30	OSS - Server-side encryption	4: data security	low	OSS	Checks whether server-side encryption is enabled for OSS buckets.
31	OSS - Hotlink protection	2: network access control	low	OSS	Checks whether hotlink protection is configured for OSS buckets.
32	ApsaraDB RDS - Cross-region backup configuration	4: data security	low	RDS	Checks whether cross-region backup is configured for ApsaraDB RDS instances.

ItemId	Name	GroupId	RiskLevel	AssetType	Description
33	ApsaraDB for MongoDB - Backup configuration	4: data security	medium	MongoDB	Checks whether data backup is enabled for ApsaraDB for MongoDB instances.
34	ApsaraDB for MongoDB - Log audit	3: log audit	medium	MongoDB	Checks whether log audit is enabled for ApsaraDB for MongoDB instances.
35	ApsaraDB for MongoDB - SSL certificate	4: data security	medium	MongoDB	Checks whether SSL certificate checks are enabled for ApsaraDB for MongoDB instances.
36	Cloud Monitor - Host monitoring plug-in	5: monitoring and alerting	medium	CloudMonitor	Checks whether the status of the Cloud Monitor agent is normal.
37	ECS - Security group policies	2: network access control	medium	ECS	Checks the ECS security group policies.
38	VPC - DNAT management port mapping	2: network access control	medium	VPC	Checks whether a VPC DNAT rule is configured to map management ports to the Internet.

ItemId	Name	GroupId	RiskLevel	AssetType	Description
39	KVStore for Redis - Backup configuration	4: data security	medium	Redis	Checks whether data backup is enabled for KVStore for Redis.
40	Container Registry - Repository permission configurations	4: data security	high	CR	Checks whether permissions are correctly configured for the repository in Container Registry.
41	Container Registry - Security scan	6: basic security protection	low	CR	Checks whether security scan is enabled for Container Registry.
42	SLB - Access logging configuration	3: log audit	medium	SLB	Checks whether access logging is configured for SLB instances.
43	KVStore for Redis - Log audit	3: log audit	low	Redis	Checks whether log audit is configured for KVStore for Redis.
44	OSS - Authorization policy	1: identity authentication and permissions	medium	OSS	Checks whether correct authorization policies are enabled for OSS.

ItemId	Name	GroupId	RiskLevel	AssetType	Description
46	PolarDB - Backup configuration	4: data security	medium	POLARDB	Checks whether the backup configuration is enabled for PolarDB.
47	PolarDB - SQL explorer	3: log audit	medium	POLARDB	Checks whether SQL Explorer is enabled for PolarDB.
48	Apsara Stack tenant account security - AccessKey pair	1: identity authentication and permissions	medium	RAM	Checks whether the AccessKey pair is enabled for your Apsara Stack tenant account.
50	CDN - Real-time logging	3: log audit	medium	CDN	Checks whether real-time logging push is enabled for CDN.
51	KVStore for Redis - SSL certificate	4: data security	medium	Redis	Checks whether KVStore for Redis uses SSL certificates.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeRiskCheckResult
&GroupId=1
&RiskLevel=high
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeRiskCheckResultResponse>
  <TotalCount>12</TotalCount>
  <RequestId>AD271C07-4ACE-413D-AA9B-F14FD3B7717F</RequestId>
  <PageCount>20</PageCount>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
  <List>
    <Status>pass</Status>
    <CheckTime>1543991525000</CheckTime>
    <TaskId>647189</TaskId>
    <RemainingTime>0</RemainingTime>
    <Title>Cloud platform - MFA configuration of Apsara Stack tenant accounts</Titl
e>
    <ItemId>1</ItemId>
    <RiskAssertType>ECS</RiskAssertType>
    <Type>Identity authentication and permissions</Type>
    <StartStatus>enabled</StartStatus>
    <AffectedCount>0</AffectedCount>
    <Sort>1</Sort>
    <RepairStatus>disabled</RepairStatus>
    <RiskLevel>high</RiskLevel>
    <RiskItemResources>
      <ContentResource>{  "type": "link",  "value": "Risk: MFA is disabled\n"
,    "url": "https://***.aliyun.com/#/secure\n" }</ContentResource>
      <ResourceName>bestPractice</ResourceName>
    </RiskItemResources>
  </List>
  <Count>10</Count>
</DescribeRiskCheckResultResponse>
```

JSON format

```
{
  "TotalCount": "12",
  "RequestId": "AD271C07-4ACE-413D-AA9B-F14FD3B7717F",
  "PageCount": "20",
  "PageSize": "10",
  "CurrentPage": "1",
  "List": {
    "Status": "pass",
    "CheckTime": "1543991525000",
    "TaskId": "647189",
    "RemainingTime": "0",
    "Title": "Cloud platform - MFA configuration of Apsara Stack tenant accounts",
    "ItemId": "1",
    "RiskAssertType": "ECS",
    "Type": "Identity authentication and permissions",
    "StartStatus": "enabled",
    "AffectedCount": "0",
    "Sort": "1",
    "RepairStatus": "disabled",
    "RiskLevel": "high",
    "RiskItemResources": {
      "ContentResource": "{  \"type\": \"link\",  \"value\": \"Risk: MFA is disabled\\n\\n\",  \"url\": \"https://***.aliyun.com/#/secure\\n\\n\" }",
      "ResourceName": "bestPractice"
    }
  },
  "Count": "10"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.4.5. DescribeSecurityCheckScheduleConfig

Queries the custom check cycle and time period.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSecurityCheckScheduleConfig	The operation that you want to perform. Set the value to DescribeSecurityCheckScheduleConfig.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
RequestId	String	48D2E9A9-A1B0-4295-B727-0995757C47E9	The ID of the request.
RiskCheckJobConfig			The settings of scheduled checks.
DaysOfWeek	String	1,2,3	The days when checks are performed every week. You can specify multiple days. Separate multiple days with commas (.). Valid values: • 1: Monday • 2: Tuesday • 3: Wednesday • 4: Thursday • 5: Friday • 6: Saturday • 7: Sunday
EndTime	Integer	12	The time period during which the configuration check ends. Valid values: • 6: 00:00 to 06:00 • 12: 06:00 to 12:00 • 18: 12:00 to 18:00 • 24: 18:00 to 24:00

Parameter	Type	Example	Description
StartTime	Integer	6	The time period during which the configuration check starts. Valid values: 0: 00:00 to 06:00 6: 06:00 to 12:00 12: 12:00 to 18:00 18: 18:00 to 24:00

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSecurityCheckScheduleConfig
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeSecurityCheckScheduleConfig>
  <RiskCheckJobConfig>
    <DaysOfWeek>1,2,3</DaysOfWeek>
    <EndTime>12</EndTime>
    <StartTime>6</StartTime>
  </RiskCheckJobConfig>
  <RequestId>C17F3C01-0AFD-4898-A950-AA0129025B41</RequestId>
</DescribeSecurityCheckScheduleConfig>
```

JSON format

```
{
  "RequestId": "C17F3C01-0AFD-4898-A950-AA0129025B41",
  "RiskCheckJobConfig": {
    "DaysOfWeek": "1,2,3",
    "EndTime": 12,
    "StartTime": 6
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.5. Vulnerability management

7.5.1. DescribeVulList

Queries vulnerabilities by type.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVulList	The operation that you want to perform. Set the value to DescribeVulList .
Type	String	Yes	cve	The type of the vulnerability. Valid values: • cve: Linux software vulnerabilities • sys: Windows vulnerabilities • cms: Web CMS vulnerabilities • app: application vulnerabilities • emg: emergency vulnerabilities
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
Remark	String	No	1.2.3.4	The tag to query, which can be the internal IP address, public IP address, or name of the asset.
Uuids	String	No	1587bedb-fdb4-48c4-9330-*****	The ID of the asset. Separate multiple IDs with commas (,).
AliasName	String	No	RHSA-2019:0230-Important: polkit security update	The alias of the vulnerability.
Necessity	String	No	asap, later, nntf	The priority to fix vulnerabilities. Separate multiple priorities with commas (,). Valid values: • asap: high • later: medium • nntf: low
Dealed	String	No	n	Specifies whether the vulnerability is handled. Valid values: • y: handled • n: unhandled

Parameter	Type	Required	Example	Description
CurrentPage	Integer	No	1	The page number of the current page. Pages start from page 1. Default value: 1.
PageSize	Integer	No	20	The number of entries to return on each page. Default value: 20.

Response parameters

Parameter	Type	Example	Description
RequestId	String	ECDE6715-6286-40E6-A32D-3094051FD74D	The ID of the request.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	2	The total number of entries returned.
VulRecords	Array		The vulnerability information.
AliasName	String	RHSA-2017:0574: gnutls security, bug fix, and enhancement update	The alias of the vulnerability.
ExtendContentJ son	Struct		The extended information.
AbsolutePath	String	/roo/www/web	The package path of the software that has the vulnerability.
AliasName	String	RHSA-2017:0574: gnutls security, bug fix, and enhancement update	The alias of the vulnerability.
Ip	String	1.2.3.1	The public IP address of the asset that is affected by the vulnerability.

Parameter	Type	Example	Description
LastTs	Long	1554189334000	The timestamp when the vulnerability was last detected.
Necessity	Struct		Indicates whether the vulnerability needs to be fixed.
Assets_factor	String	1	The asset score.
Cvss_factor	String	7.8	The Common Vulnerability Scoring System (CVSS) score.
Enviroment_factor	String	1.0	The environmental score.
Gmt_create	String	20190331	The creation time.
Is_calc	String	1	Indicates whether the vulnerability severity score is calculated. Valid values: • 0: The score is not calculated. • 1: The score is calculated.
Status	String	normal	The status of the vulnerability severity score. Valid values: • none: No score is generated. • pending: The score is pending calculation. • miss: The score failed to be calculated. • normal: The calculation is normal.
Time_factor	String	1.0	The temporal score.

Parameter	Type	Example	Description
Total_score	String	7.8	The total vulnerability severity score. We recommend that you apply the following rules: • Critical: The severity score is between 13.5 and 15, which typically represents a high-risk vulnerability. • Important: The severity score is between 7.1 and 13.5, which typically represents a medium-risk vulnerability. • Moderate: The severity score is below 7, which typically represents a low-risk vulnerability.
Os	String	centos	The operating system.
OsRelease	String	7	The version of the operating system.
PrimaryId	Long	111	The ID of the vulnerability.
RpmEntityList	Array		The details about the RPM package.
FullVersion	String	3.10.0-693.2.2.el7	The complete version number.
MatchDetail	String	python-perf version less than 0:3.10.0-693.21.1.el7	The detailed matching information of the vulnerability.
Name	String	python-perf	The name of the RPM package.
Path	String	/usr/lib64/python2.7/site-packages	The path of the software that has the vulnerability.
UpdateCmd	String	*** update python-perf	The command that can be run to fix the vulnerability.
Version	String	3.10.0	The version of the operating system.

Parameter	Type	Example	Description
Status	Integer	1	The status of the vulnerability. Valid values: • 1: unfixed • 2: fix failed • 3: rollback failed • 4: fixing • 5: rolling back • 6: verifying • 7: fixed • 8: fixed and to be restarted • 9: rolled back • 10: ignored • 11: rolled back and to be restarted • 12: not found • 20: expired
Tag	String	oval	The tag of the vulnerability.
cveList	List	["CVE-2016-8610", "CVE-2017-5335"]	The Common Vulnerabilities and Exposures (CVEs) list.
FirstTs	Long	1554189334000	The first time when the vulnerability was detected. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
GroupId	Integer	281801	The ID of the asset group.
InstanceId	String	i-bp18t***	The ID of the asset instance.
InstanceName	String	Test ECS	The name of the asset instance.
InternetIp	String	1.2.3.1	The public IP address of the asset.
IntranetIp	String	1.2.3.4	The private IP address of the asset.
LastTs	Long	1541207563000	The timestamp when the vulnerability was last detected.

Parameter	Type	Example	Description
ModifyTs	Long	1541207563000	The timestamp when the vulnerability was modified.
Name	String	oval:com.redhat.rhsa:def:20170574	The name of the vulnerability.
Necessity	String	asap	The priority to fix vulnerabilities. Valid values: • asap: high • later: medium • nntf: low  Note We recommend that you fix the high-level vulnerabilities as soon as possible.
Online	Boolean	true	Indicates whether the asset instance is online. Valid values: • true: online • false: offline
OsVersion	String	linux	The version of the operating system.
PrimaryId	Long	101162078	The ID of the vulnerability.
Related	String	CVE-2017-7518,CVE-2017-12188	The list of CVEs related to the vulnerability. Separate multiple CVEs with commas (,).
RepairTs	Long	1541207563000	The timestamp when the vulnerability was fixed.
ResultCode	String	0	The result code returned after the vulnerability is fixed.
ResultMessage	String	timeout	The message returned after the vulnerability is fixed.

Parameter	Type	Example	Description
Status	Integer	1	The status of the vulnerability. Valid values: • 1: unfixed • 2: fix failed • 3: rollback failed • 4: fixing • 5: rolling back • 6: verifying • 7: fixed • 8: fixed and to be restarted • 9: rolled back • 10: ignored • 11: rolled back and to be restarted • 12: not found • 20: expired
Tag	String	oval	The tag of the vulnerability.
Type	String	cve	The type of the vulnerability. Valid values: • cve: Linux vulnerabilities • sys: Windows vulnerabilities • cms: Web CMS vulnerabilities • emg: emergency vulnerabilities • app: application vulnerabilities
Uuid	String	04c56617-23fc-43a5-ab9b-*****	The ID of the asset.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVulList
&Type=cve
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeVulListResponse>
  <TotalCount>2</TotalCount>
  <RequestId>ECDE6715-6286-40E6-A32D-3094051FD74D</RequestId>
  <PageSize>20</PageSize>
```

```

    <VulRecords>
      <Status>1</Status>
      <InstanceId>i-bp18t***</InstanceId>
      <OsVersion>linux</OsVersion>
      <LastTs>1541207563000</LastTs>
      <Necessity>asap</Necessity>
      <ResultMessage>timeout</ResultMessage>
      <IntranetIp>1.2.3.4</IntranetIp>
      <Name>oval:com.redhat.rhsa:def:20170574</Name>
      <GroupId>281801</GroupId>
      <RepairTs>1541207563000</RepairTs>
      <InstanceName>Test ECS</InstanceName>
      <Type>cve</Type>
      <FirstTs>1554189334000</FirstTs>
      <Uuid>04c56617-23fc-43a5-ab9b-*****</Uuid>
      <Related>CVE-2017-7518,CVE-2017-12188</Related>
      <ModifyTs>1541207563000</ModifyTs>
      <InternetIp>1.2.3.1</InternetIp>
      <AliasName>RHSA-2017:0574: gnutls security, bug fix, and enhancement update</Al
iasName>
      <Tag>oval</Tag>
      <Online>true</Online>
      <PrimaryId>101162078</PrimaryId>
      <ResultCode>0</ResultCode>
    </VulRecords>
  <VulRecords>
    <ExtendContentJson>
      <Status>1</Status>
      <Os>centos</Os>
      <AliasName>RHSA-2017:0574: gnutls security, bug fix, and enhancement upda
te</AliasName>
      <Ip>1.2.3.1</Ip>
      <LastTs>1554189334000</LastTs>
      <cveList>["CVE-2016-8610", "CVE-2017-5335" ]</cveList>
      <Necessity>
        <Status>normal</Status>
        <Total_score>7.8</Total_score>
        <Gmt_create>20190331</Gmt_create>
        <Cvss_factor>7.8</Cvss_factor>
        <Time_factor>1.0</Time_factor>
        <Is_calc>1</Is_calc>
        <Enviroment_factor>1.0</Enviroment_factor>
        <Assets_factor>1</Assets_factor>
      </Necessity>
      <RpmEntityList>
        <Path>/usr/lib64/python2.7/site-packages</Path>
        <UpdateCmd>*** update python-perf</UpdateCmd>
        <Version>3.10.0</Version>
        <FullVersion>3.10.0-693.2.2.el7</FullVersion>
        <MatchDetail>python-perf version less than 0:3.10.0-693.21.1.el7</M
atchDetail>
        <Name>python-perf</Name>
      </RpmEntityList>
      <Tag>oval</Tag>
    </ExtendContentJson>
  </VulRecords>

```

```
<OsRelease>7</OsRelease>
<AbsolutePath>/roo/www/web</AbsolutePath>
<PrimaryId>111</PrimaryId>
</ExtendContentJson>
</VulRecords>
<CurrentPage>1</CurrentPage>
</DescribeVulListResponse>
```

JSON format

```
{
  "TotalCount": "2",
  "RequestId": "ECDE6715-6286-40E6-A32D-3094051FD74D",
  "PageSize": "20",
  "VulRecords": [{
    "Status": "1",
    "InstanceId": "i-bp18t***",
    "OsVersion": "linux",
    "LastTs": "1541207563000",
    "Necessity": "asap",
    "ResultMessage": "timeout",
    "IntranetIp": "1.2.3.4",
    "Name": "oval:com.redhat.rhsa:def:20170574",
    "GroupId": "281801",
    "RepairTs": "1541207563000",
    "InstanceName": "Test ECS",
    "Type": "cve",
    "FirstTs": "1554189334000",
    "Uuid": "04c56617-23fc-43a5-ab9b-*****",
    "Related": "CVE-2017-7518,CVE-2017-12188",
    "ModifyTs": "1541207563000",
    "InternetIp": "1.2.3.1",
    "AliasName": "RHSA-2017:0574: gnutls security, bug fix, and enhancement update"
  }, {
    "Tag": "oval",
    "Online": "true",
    "PrimaryId": "101162078",
    "ResultCode": "0"
  }, {
    "ExtendContentJson": {
      "Status": "1",
      "Os": "centos",
      "AliasName": "RHSA-2017:0574: gnutls security, bug fix, and enhancement upd
ate",
      "Ip": "1.2.3.1",
      "LastTs": "1554189334000",
      "cveList": "[\"CVE-2016-8610\", \"CVE-2017-5335\" ]",
      "Necessity": {
        "Status": "normal",
        "Total_score": "7.8",
        "Gmt_create": "20190331",
        "Cvss_factor": "7.8",
        "Time_factor": "1.0",
        "Is_calc": "1",
```

```
        "Enviroment_factor": "1.0",
        "Assets_factor": "1"
    },
    "RpmEntityList": [{
        "Path": "/usr/lib64/python2.7/site-packages",
        "UpdateCmd": "*** update python-perf",
        "Version": "3.10.0",
        "FullVersion": "3.10.0-693.2.2.el7",
        "MatchDetail": "python-perf version less than 0:3.10.0-693.21.1.el7",
        "Name": "python-perf"
    }],
    "Tag": "oval",
    "OsRelease": "7",
    "AbsolutePath": "/roo/www/web",
    "PrimaryId": "111"
}
}],
"CurrentPage": "1"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.5.2. DescribeVulWhitelist

Queries the whitelist of vulnerabilities by page.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVulWhitelist	The operation that you want to perform. Set the value to DescribeVulWhitelist.
CurrentPage	Integer	No	1	The number of the page to return. Pages start from page 1. Default value: 1.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: 20.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the current page.

Parameter	Type	Example	Description
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	74F97EF7-B543-43FD-A4E9-18456731F9C5	The ID of the request.
TotalCount	Integer	1	The total number of returned entries.
VulWhitelists	Array		The information about the vulnerability whitelist.
AliasName	String	RHSA-2017:3263: curl security update	The alias of the vulnerability.
Name	String	oval:com.redhat.rhsa:def:20173263	The name of the vulnerability.
Reason	String	Not urgent	The reason for adding the vulnerability to the whitelist.
Type	String	cve	The type of the vulnerability.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeVulWhitelist
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeVulWhitelist>
  <TotalCount>1</TotalCount>
  <VulWhitelists>
    <Name>oval:com.redhat.rhsa:def:20173263</Name>
    <AliasName>RHSA-2017:3263: curl security update</AliasName>
    <Type>cve</Type>
    <Reason>Not urgent</Reason>
  </VulWhitelists>
  <PageSize>3</PageSize>
  <RequestId>74F97EF7-B543-43FD-A4E9-18456731F9C5</RequestId>
  <CurrentPage>1</CurrentPage>
</DescribeVulWhitelist>
```

JSON format

```
{
  "TotalCount":1,
  "PageSize":3,
  "VulWhitelists":[
    {
      "Name":"oval:com.redhat.rhsa:def:20173263",
      "AliasName":"RHSA-2017:3263: curl security update",
      "Type":"cve",
      "Reason":"Not urgent"
    }
  ],
  "RequestId":"74F97EF7-B543-43FD-A4E9-18456731F9C5",
  "CurrentPage":1
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.5.3. DescribeConcernNecessity

Queries the priority to fix the vulnerability.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeConcernNecessity	The operation that you want to perform. Set the value to DescribeConcernNecessity.
Lang	String	No	zh	The natural language of the request and response. Valid values: zh: Chinese en: English

Response parameters

Parameter	Type	Example	Description
ConcernNecessity	List	["asap", "later", "nntf"]	The priority to fix the vulnerability. Valid values: asap: high later: medium nntf: low

Parameter	Type	Example	Description
RequestId	String	9139DAF6-5CE0-49A0-926E-07243A290F70	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeConcernNecessity
&Lang=zh
&<Common request parameters>
```

Sample success responses

XML **format**

```
<DescribeConcernNecessity>
  <ConcernNecessity>asap</ConcernNecessity>
  <ConcernNecessity>later</ConcernNecessity>
  <ConcernNecessity>nntf</ConcernNecessity>
  <RequestId>9139DAF6-5CE0-49A0-926E-07243A290F70</RequestId>
</DescribeConcernNecessity>
```

JSON **format**

```
{
  "ConcernNecessity": [
    "asap",
    "later",
    "nntf"
  ],
  "RequestId": "9139DAF6-5CE0-49A0-926E-07243A290F70"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.5.4. DescribeGroupedVul

Queries information about vulnerabilities by group.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeGroupedVul	The operation that you want to perform. Set the value to DescribeGroupedVul.
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
Type	String	No	cve	The type of the vulnerability. Valid values: • cve: Linux vulnerabilities • sys: Windows vulnerabilities • cms: Web CMS vulnerabilities • app: application vulnerabilities • emg: emergency vulnerabilities
Uuids	String	No	d42f938c-d962-48a0-90f9-05e4ea*****	The IDs of the asset instances. Separate multiple IDs with commas (,).
AliasName	String	No	RHSA-2019:0230-Important: polkit security update	The alias of the vulnerability.
Necessity	String	No	asap, later, nntf	The priority to fix the vulnerability. Separate multiple priorities with commas (,). Valid values: • asap: high • later: medium • nntf: low
Dealed	String	No	n	Specifies whether the vulnerability is handled. • y: handled • n: unhandled
CurrentPage	Integer	No	1	The page number of the current page. Pages start from page 1. Default value: 1.

Parameter	Type	Required	Example	Description
PageSize	Integer	No	20	The number of entries to return on each page. Default value: 20.
GroupId	String	No	weds****	The ID of the asset group.

Response parameters

Parameter	Type	Example	Description
RequestId	String	0DFCADBA-7065-42DA-AF17-6868B9C2A8CF	The ID of the request.
PageSize	Integer	20	The number of entries returned per page.
CurrentPage	Integer	1	The page number of the current page.
TotalCount	Integer	2	The total number of entries returned.
GroupedVulItems	Array		Details about vulnerabilities by group.
Name	String	***glibc security and bug fixes	The name of the vulnerability.
AliasName	String	RHSA-2019:0230-Important: polkit security update	The alias of the vulnerability.
Type	String	cve	The type of the vulnerability. Valid values: • cve: Linux vulnerabilities • sys: Windows vulnerabilities • cms: Web CMS vulnerabilities • app: application vulnerabilities • emg: emergency vulnerabilities
GmtLast	Long	1554185744000	The time when the vulnerability was last detected. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Example	Description
AsapCount	Integer	0	The number of high-priority vulnerabilities.
LaterCount	Integer	0	The number of medium-priority vulnerabilities.
NntfCount	Integer	59	The number of low-priority vulnerabilities.
HandledCount	Integer	0	The total number of handled vulnerabilities.
Tags	String	Force restart	The tag of the vulnerability.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeGroupedVul
&Lang=zh
&Type=cve
&AliasName=RHSA-2019:0230-Important: polkit security update
&Necessity=asap, later, nntf
&Dealed=n
&CurrentPage=1
&PageSize=20
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeGroupedVul>
  <GroupedVulItems>
    <Tags></Tags>
    <LaterCount>0</LaterCount>
    <AliasName>RHSA-2019:0230-Important: polkit security update</AliasName>
    <AsapCount>0</AsapCount>
    <Type>cve</Type>
    <NntfCount>59</NntfCount>
    <GmtLast>1554185744000</GmtLast>
    <HandledCount>0</HandledCount>
  </GroupedVulItems>
  <GroupedVulItems>
    <Tags></Tags>
    <LaterCount>0</LaterCount>
    <AliasName>RHSA-2019:0368-Important: systemd security update</AliasName>
    <AsapCount>0</AsapCount>
    <Type>cve</Type>
    <NntfCount>59</NntfCount>
    <GmtLast>1554185744000</GmtLast>
    <HandledCount>0</HandledCount>
  </GroupedVulItems>
  <TotalCount>432</TotalCount>
  <PageSize>2</PageSize>
  <RequestId>0DFCADBA-7065-42DA-AF17-6868B9C2A8CF</RequestId>
  <CurrentPage>1</CurrentPage>
</DescribeGroupedVul>
```

JSON **format**

```
{
  "GroupedVulItems": [
    {
      "Tags": "",
      "LaterCount": 0,
      "AliasName": "RHSA-2019:0230-Important: polkit security update",
      "AsapCount": 0,
      "Type": "cve",
      "NntfCount": 59,
      "GmtLast": 1554185744000,
      "HandledCount": 0
    },
    {
      "Tags": "",
      "LaterCount": 0,
      "AliasName": "RHSA-2019:0368-Important: systemd security update",
      "AsapCount": 0,
      "Type": "cve",
      "NntfCount": 59,
      "GmtLast": 1554185744000,
      "HandledCount": 0
    }
  ],
  "TotalCount": 432,
  "PageSize": 2,
  "RequestId": "0DFCADBA-7065-42DA-AF17-6868B9C2A8CF",
  "CurrentPage": 1
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.5.5. DescribeAutoDelConfig

Queries the configurations for automatic vulnerability deletion.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeAutoDelConfig	The operation that you want to perform. Set the value to DescribeAutoDelConfig .

Response parameters

Parameter	Type	Example	Description
RequestId	String	43186B14-5A39-44E0-860E-8B24D1EF82CC	The ID of the request.
Days	Integer	7	The number of days that a detected vulnerability is retained.

Examples

Sample requests

```
/?Action=DescribeAutoDelConfig  
&<Common request parameters>
```

Sample success responses

XML **format**

```
<DescribeAutoDelConfig>  
  <RequestId>43186B14-5A39-44E0-860E-8B24D1EF82CC</RequestId>  
  <Days>7</Days>  
</DescribeAutoDelConfig>
```

JSON **format**

```
{  
  "RequestId": "43186B14-5A39-44E0-860E-8B24D1EF82CC",  
  "Days": 7  
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.6. Baseline check

7.6.1. DescribeCheckWarningSummary

Queries the statistical information about baseline check results. The information includes the number of servers on which a baseline check is performed, the number of baseline check items, and the last check pass rate.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCheckWarningSummary	The operation that you want to perform. Set the value to DescribeCheckWarningSummary.
CurrentPage	Integer	No	1	The page number of the current page.
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
PageSize	Integer	No	10	The number of entries to return on each page.
RiskName	String	No	Redis security baseline check	The name of the risk item.
RiskStatus	Integer	No	1	The status of the baseline check. Valid values: • 1: failed • 3: passed
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Status	String	No	1	The status of the check item. Valid values: • 1: failed • 2: verifying • 3: passed • 5: expired • 6: ignored
StrategyId	Long	No	1	The ID of the baseline check policy.
TypeName	String	No	database	The level-1 type of check items.
Uuids	String	No	f03259d8-1e81-4fae-bcbb-275fb5*****	The ID of the server.

Response parameters

Parameter	Type	Example	Description
Count	Integer	10	The number of check items returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	00BD7CE2-284A-4534-BD09-FB69836DD750	The ID of the request.
TotalCount	Integer	100	The total number of baseline check items.
WarningSummaries	Array		The statistics of check items.
CheckCount	Integer	10	The number of check items.
HighWarningCount	Integer	1	The number of high-risk items.
LastFoundTime	String	2019-01-01 12:23:00	The time when the last baseline check was performed.
Level	String	high	The severity level of the risk item. Valid values: • High • Medium • Low
LowWarningCount	Integer	3	The number of low-risk check items.
MediumWarningCount	Integer	2	The number of medium-risk check items.
RiskId	Long	1	The ID of the risk item.
RiskName	String	Redis password	The name of the risk item.

Parameter	Type	Example	Description
SubTypeAlias	String	Redis	The level-2 type of the risk item.
TypeAlias	String	Database	The type of the check item. Valid values: database, system, weak password, and middleware.
WarningMachineCount	Integer	11	The number of assets on which risk items are detected.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCheckWarningSummary
&Lang=zh
&TypeName=database
&Status=1
&RiskStatus=1
&RiskName=Redis security baseline check
&StrategyId=1
&Uuids=f03259d8-1e81-4fae-bcbb-275fb55efb34
&CurrentPage=1
&PageSize=20
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeCheckWarningSummary>
  <TotalCount>25</TotalCount>
  <PageSize>20</PageSize>
  <RequestId>DFA6CDC5-E826-4D18-A499-BEF9DA31F1AD</RequestId>
  <CurrentPage>1</CurrentPage>
  <Count>20</Count>
  <WarningSummaries>
    <RiskId>43</RiskId>
    <LastFoundTime>2019-04-10 00:33:00</LastFoundTime>
    <MediumWarningCount>0</MediumWarningCount>
    <WarningMachineCount>3</WarningMachineCount>
    <CheckCount>16</CheckCount>
    <HighWarningCount>8</HighWarningCount>
    <Level>high</Level>
    <TypeAlias>System</TypeAlias>
    <SubTypeAlias>
      CentOS Linux 7 security baseline check
    </SubTypeAlias>
    <LowWarningCount>0</LowWarningCount>
    <RiskName>
```

```
CentOS Linux 7 security baseline check
                                </RiskName>
</WarningSummary>
<WarningSummary>
  <RiskId>47</RiskId>
  <LastFoundTime>2019-04-10 00:58:11</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>2</WarningMachineCount>
  <CheckCount>15</CheckCount>
  <HighWarningCount>7</HighWarningCount>
  <Level>medium</Level>
  <TypeAlias>System</TypeAlias>
  <SubTypeAlias>CentOS Linux 7 security standard compliance - MLPS level-3</SubTypeAlias>
s>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>CentOS Linux 7 security standard compliance - MLPS level-3</RiskName>
</WarningSummary>
<WarningSummary>
  <RiskId>48</RiskId>
  <LastFoundTime>2019-04-10 00:58:11</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>2</WarningMachineCount>
  <CheckCount>12</CheckCount>
  <HighWarningCount>6</HighWarningCount>
  <Level>medium</Level>
  <TypeAlias>System</TypeAlias>
  <SubTypeAlias>CentOS Linux 7 security standard compliance - MLPS level-2</SubTypeAlias>
s>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>CentOS Linux 7 security standard compliance - MLPS level-2</RiskName>
</WarningSummary>
<WarningSummary>
  <RiskId>3</RiskId>
  <LastFoundTime>2019-04-10 08:31:32</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>1</WarningMachineCount>
  <CheckCount>1</CheckCount>
  <HighWarningCount>1</HighWarningCount>
  <Level>high</Level>
  <TypeAlias>Database</TypeAlias>
  <SubTypeAlias>Redis security baseline check</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>Redis security baseline check</RiskName>
</WarningSummary>
<WarningSummary>
  <RiskId>19</RiskId>
  <LastFoundTime>2019-04-10 08:31:32</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>1</WarningMachineCount>
  <CheckCount>1</CheckCount>
  <HighWarningCount>1</HighWarningCount>
  <Level>high</Level>
  <TypeAlias>Weak password</TypeAlias>
  <SubTypeAlias>Linux weak password</SubTypeAlias>
```

```

    <LowWarningCount>0</LowWarningCount>
    <RiskName>Linux weak password</RiskName>
  </WarningSummary>
  <WarningSummary>
    <RiskId>12</RiskId>
    <LastFoundTime>2019-04-10 08:31:32</LastFoundTime>
    <MediumWarningCount>0</MediumWarningCount>
    <WarningMachineCount>1</WarningMachineCount>
    <CheckCount>1</CheckCount>
    <HighWarningCount>1</HighWarningCount>
    <Level>high</Level>
    <TypeAlias>Weak password</TypeAlias>
    <SubTypeAlias>Anonymous FTP logon</SubTypeAlias>
    <LowWarningCount>0</LowWarningCount>
    <RiskName>Anonymous FTP logon</RiskName>
  </WarningSummary>
  <WarningSummary>
    <RiskId>13</RiskId>
    <LastFoundTime>2019-04-10 06:58:58</LastFoundTime>
    <MediumWarningCount>0</MediumWarningCount>
    <WarningMachineCount>1</WarningMachineCount>
    <CheckCount>1</CheckCount>
    <HighWarningCount>1</HighWarningCount>
    <Level>high</Level>
    <TypeAlias>Weak password</TypeAlias>
    <SubTypeAlias>Windows weak password</SubTypeAlias>
    <LowWarningCount>0</LowWarningCount>
    <RiskName>Windows weak password</RiskName>
  </WarningSummary>
  <WarningSummary>
    <RiskId>23</RiskId>
    <LastFoundTime>2019-04-10 14:00:17</LastFoundTime>
    <MediumWarningCount>0</MediumWarningCount>
    <WarningMachineCount>0</WarningMachineCount>
    <CheckCount>8</CheckCount>
    <HighWarningCount>0</HighWarningCount>
    <Level>medium</Level>
    <TypeAlias>Middleware</TypeAlias>
    <SubTypeAlias>Apache Tomcat security baseline check</SubTypeAlias>
    <LowWarningCount>0</LowWarningCount>
    <RiskName>Apache Tomcat security baseline check</RiskName>
  </WarningSummary>
  <WarningSummary>
    <RiskId>2</RiskId>
    <LastFoundTime>2019-04-10 08:31:32</LastFoundTime>
    <MediumWarningCount>0</MediumWarningCount>
    <WarningMachineCount>0</WarningMachineCount>
    <CheckCount>1</CheckCount>
    <HighWarningCount>0</HighWarningCount>
    <Level>high</Level>
    <TypeAlias>Weak password</TypeAlias>
    <SubTypeAlias>PostgreSQL weak password</SubTypeAlias>
    <LowWarningCount>0</LowWarningCount>
    <RiskName>PostgreSQL weak password</RiskName>
  </WarningSummary>

```

```
</warningsummaries>
<WarningSummaries>
  <RiskId>11</RiskId>
  <LastFoundTime>2019-04-10 08:31:32</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>0</WarningMachineCount>
  <CheckCount>1</CheckCount>
  <HighWarningCount>0</HighWarningCount>
  <Level>high</Level>
  <TypeAlias>Weak password</TypeAlias>
  <SubTypeAlias>MySQL weak password</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>MySQL weak password</RiskName>
</WarningSummaries>
<WarningSummaries>
  <RiskId>20</RiskId>
  <LastFoundTime>2019-04-10 08:31:32</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>0</WarningMachineCount>
  <CheckCount>1</CheckCount>
  <HighWarningCount>0</HighWarningCount>
  <Level>high</Level>
  <TypeAlias>Weak password</TypeAlias>
  <SubTypeAlias>FTP weak password</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>FTP weak password</RiskName>
</WarningSummaries>
<WarningSummaries>
  <RiskId>17</RiskId>
  <LastFoundTime>2019-04-10 06:58:58</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>0</WarningMachineCount>
  <CheckCount>1</CheckCount>
  <HighWarningCount>0</HighWarningCount>
  <Level>high</Level>
  <TypeAlias>Weak password</TypeAlias>
  <SubTypeAlias>Microsoft SQL Server weak password</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>Microsoft SQL Server weak password</RiskName>
</WarningSummaries>
<WarningSummaries>
  <RiskId>24</RiskId>
  <LastFoundTime>2019-04-10 06:52:05</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>0</WarningMachineCount>
  <CheckCount>2</CheckCount>
  <HighWarningCount>0</HighWarningCount>
  <Level>medium</Level>
  <TypeAlias>Database</TypeAlias>
  <SubTypeAlias>Memcached security baseline check</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>Memcached security baseline check</RiskName>
</WarningSummaries>
<WarningSummaries>
  <RiskId>42</RiskId>
```

```

<LastFoundTime>2019-02-19 14:59:17</LastFoundTime>
<MediumWarningCount>0</MediumWarningCount>
<WarningMachineCount>0</WarningMachineCount>
<CheckCount>16</CheckCount>
<HighWarningCount>0</HighWarningCount>
<Level>high</Level>
<TypeAlias>System</TypeAlias>
<SubTypeAlias>CentOS Linux 6 security baseline check</SubTypeAlias>
<LowWarningCount>0</LowWarningCount>
<RiskName>CentOS Linux 6 security baseline check</RiskName>
</WarningSummary>
<WarningSummary>
  <RiskId>49</RiskId>
  <LastFoundTime>2019-02-19 14:59:17</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>0</WarningMachineCount>
  <CheckCount>12</CheckCount>
  <HighWarningCount>0</HighWarningCount>
  <Level>medium</Level>
  <TypeAlias>System</TypeAlias>
  <SubTypeAlias>CentOS Linux 6 security standard compliance - MLPS level-2</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>CentOS Linux 6 security standard compliance - MLPS level-2</RiskName>
</WarningSummary>
<WarningSummary>
  <RiskId>50</RiskId>
  <LastFoundTime>2019-02-19 14:59:17</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>0</WarningMachineCount>
  <CheckCount>15</CheckCount>
  <HighWarningCount>0</HighWarningCount>
  <Level>medium</Level>
  <TypeAlias>System</TypeAlias>
  <SubTypeAlias>CentOS Linux 6 security standard compliance - MLPS level-3</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>CentOS Linux 6 security standard compliance - MLPS level-3</RiskName>
</WarningSummary>
<WarningSummary>
  <RiskId>55</RiskId>
  <LastFoundTime>2019-02-19 12:57:23</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>0</WarningMachineCount>
  <CheckCount>14</CheckCount>
  <HighWarningCount>0</HighWarningCount>
  <Level>medium</Level>
  <TypeAlias>System</TypeAlias>
  <SubTypeAlias>Linux Ubuntu security standard compliance - MLPS level-2</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>Linux Ubuntu security standard compliance - MLPS level-2</RiskName>
</WarningSummary>
<WarningSummary>
  <RiskId>56</RiskId>

```



```
<LastFoundTime>2019-02-19 12:57:23</LastFoundTime>
<MediumWarningCount>0</MediumWarningCount>
<WarningMachineCount>0</WarningMachineCount>
<CheckCount>15</CheckCount>
<HighWarningCount>0</HighWarningCount>
<Level>medium</Level>
<TypeAlias>System</TypeAlias>
<SubTypeAlias>Linux Ubuntu security standard compliance - MLPS level-3</SubTypeAlias>
<LowWarningCount>0</LowWarningCount>
<RiskName>Linux Ubuntu security standard compliance - MLPS level-3</RiskName>
</WarningSummaries>
<WarningSummaries>
  <RiskId>54</RiskId>
  <LastFoundTime>2019-02-19 12:57:23</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>0</WarningMachineCount>
  <CheckCount>16</CheckCount>
  <HighWarningCount>0</HighWarningCount>
  <Level>high</Level>
  <TypeAlias>System</TypeAlias>
  <SubTypeAlias>Linux Ubuntu security baseline check</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>Linux Ubuntu security baseline check</RiskName>
</WarningSummaries>
<WarningSummaries>
  <RiskId>51</RiskId>
  <LastFoundTime>2019-02-19 12:44:58</LastFoundTime>
  <MediumWarningCount>0</MediumWarningCount>
  <WarningMachineCount>0</WarningMachineCount>
  <CheckCount>12</CheckCount>
  <HighWarningCount>0</HighWarningCount>
  <Level>high</Level>
  <TypeAlias>System</TypeAlias>
  <SubTypeAlias>Windows 2012 R2 security baseline check</SubTypeAlias>
  <LowWarningCount>0</LowWarningCount>
  <RiskName>Windows 2012 R2 security baseline check</RiskName>
</WarningSummaries>
</DescribeCheckWarningSummary>
```

JSON **format**

```
{
  "Count":20,
  "TotalCount":25,
  "WarningSummaries":[
    {
      "SubTypeAlias":"CentOS Linux 7 security baseline check\n
\n",
      "HighWarningCount":8,
      "WarningMachineCount":3,
      "RiskName":"CentOS Linux 7 security baseline check\n
\n",
      "LowWarningCount":0,
      "CheckCount":16
    }
  ]
}
```

```

    "CheckCount":16,
    "RiskId":43,
    "Level":"high",
    "MediumWarningCount":0,
    "TypeAlias":"System",
    "LastFoundTime":"2019-04-10 00:33:00"
  },
  {
    "SubTypeAlias":"CentOS Linux 7 security standard compliance - MLPS level-3",
    "HighWarningCount":7,
    "WarningMachineCount":2,
    "RiskName":"CentOS Linux 7 security standard compliance - MLPS level-3",
    "LowWarningCount":0,
    "CheckCount":15,
    "RiskId":47,
    "Level":"medium",
    "MediumWarningCount":0,
    "TypeAlias":"System",
    "LastFoundTime":"2019-04-10 00:58:11"
  },
  {
    "SubTypeAlias":"CentOS Linux 7 security standard compliance - MLPS level-2",
    "HighWarningCount":6,
    "WarningMachineCount":2,
    "RiskName":"CentOS Linux 7 security standard compliance - MLPS level-2",
    "LowWarningCount":0,
    "CheckCount":12,
    "RiskId":48,
    "Level":"medium",
    "MediumWarningCount":0,
    "TypeAlias":"System",
    "LastFoundTime":"2019-04-10 00:58:11"
  },
  {
    "SubTypeAlias":"Redis security baseline check",
    "HighWarningCount":1,
    "WarningMachineCount":1,
    "RiskName":"Redis security baseline check",
    "LowWarningCount":0,
    "CheckCount":1,
    "RiskId":3,
    "Level":"high",
    "MediumWarningCount":0,
    "TypeAlias":"Database",
    "LastFoundTime":"2019-04-10 08:31:32"
  },
  {
    "SubTypeAlias":"Linux weak password",
    "HighWarningCount":1,
    "WarningMachineCount":1,
    "RiskName":"Linux weak password",
    "LowWarningCount":0,
    "CheckCount":1,
    "RiskId":19,
    "Level":"high".
  }

```

```
    "Level": "high",
    "MediumWarningCount": 0,
    "TypeAlias": "Weak password",
    "LastFoundTime": "2019-04-10 08:31:32"
  },
  {
    "SubTypeAlias": "Anonymous FTP logon",
    "HighWarningCount": 1,
    "WarningMachineCount": 1,
    "RiskName": "Anonymous FTP logon",
    "LowWarningCount": 0,
    "CheckCount": 1,
    "RiskId": 12,
    "Level": "high",
    "MediumWarningCount": 0,
    "TypeAlias": "Weak password",
    "LastFoundTime": "2019-04-10 08:31:32"
  },
  {
    "SubTypeAlias": "Windows weak password",
    "HighWarningCount": 1,
    "WarningMachineCount": 1,
    "RiskName": "Windows weak password",
    "LowWarningCount": 0,
    "CheckCount": 1,
    "RiskId": 13,
    "Level": "high",
    "MediumWarningCount": 0,
    "TypeAlias": "Weak password",
    "LastFoundTime": "2019-04-10 06:58:58"
  },
  {
    "SubTypeAlias": "Apache Tomcat security baseline check",
    "HighWarningCount": 0,
    "WarningMachineCount": 0,
    "RiskName": "Apache Tomcat security baseline check",
    "LowWarningCount": 0,
    "CheckCount": 8,
    "RiskId": 23,
    "Level": "medium",
    "MediumWarningCount": 0,
    "TypeAlias": "Middleware",
    "LastFoundTime": "2019-04-10 14:00:17"
  },
  {
    "SubTypeAlias": "PostgreSQL weak password",
    "HighWarningCount": 0,
    "WarningMachineCount": 0,
    "RiskName": "PostgreSQL weak password",
    "LowWarningCount": 0,
    "CheckCount": 1,
    "RiskId": 2,
    "Level": "high",
    "MediumWarningCount": 0,
    "TypeAlias": "Weak password",
```

```
"LastFoundTime":"2019-04-10 08:31:32"
},
{
  "SubTypeAlias":"MySQL weak password",
  "HighWarningCount":0,
  "WarningMachineCount":0,
  "RiskName":"MySQL weak password",
  "LowWarningCount":0,
  "CheckCount":1,
  "RiskId":11,
  "Level":"high",
  "MediumWarningCount":0,
  "TypeAlias":"Weak password",
  "LastFoundTime":"2019-04-10 08:31:32"
},
{
  "SubTypeAlias":"FTP weak password",
  "HighWarningCount":0,
  "WarningMachineCount":0,
  "RiskName":"FTP weak password",
  "LowWarningCount":0,
  "CheckCount":1,
  "RiskId":20,
  "Level":"high",
  "MediumWarningCount":0,
  "TypeAlias":"Weak password",
  "LastFoundTime":"2019-04-10 08:31:32"
},
{
  "SubTypeAlias":"Microsoft SQL Server weak password",
  "HighWarningCount":0,
  "WarningMachineCount":0,
  "RiskName":"Microsoft SQL Server weak password",
  "LowWarningCount":0,
  "CheckCount":1,
  "RiskId":17,
  "Level":"high",
  "MediumWarningCount":0,
  "TypeAlias":"Weak password",
  "LastFoundTime":"2019-04-10 06:58:58"
},
{
  "SubTypeAlias":"Memcached security baseline check",
  "HighWarningCount":0,
  "WarningMachineCount":0,
  "RiskName":"Memcached security baseline check",
  "LowWarningCount":0,
  "CheckCount":2,
  "RiskId":24,
  "Level":"medium",
  "MediumWarningCount":0,
  "TypeAlias":"Database",
  "LastFoundTime":"2019-04-10 06:52:05"
},
```

```
{
  "SubTypeAlias": "CentOS Linux 6 security baseline check",
  "HighWarningCount": 0,
  "WarningMachineCount": 0,
  "RiskName": "CentOS Linux 6 security baseline check",
  "LowWarningCount": 0,
  "CheckCount": 16,
  "RiskId": 42,
  "Level": "high",
  "MediumWarningCount": 0,
  "TypeAlias": "System",
  "LastFoundTime": "2019-02-19 14:59:17"
},
{
  "SubTypeAlias": "CentOS Linux 6 security standard compliance - MLPS level-2",
  "HighWarningCount": 0,
  "WarningMachineCount": 0,
  "RiskName": "CentOS Linux 6 security standard compliance - MLPS level-2",
  "LowWarningCount": 0,
  "CheckCount": 12,
  "RiskId": 49,
  "Level": "medium",
  "MediumWarningCount": 0,
  "TypeAlias": "System",
  "LastFoundTime": "2019-02-19 14:59:17"
},
{
  "SubTypeAlias": "CentOS Linux 6 security standard compliance - MLPS level-3",
  "HighWarningCount": 0,
  "WarningMachineCount": 0,
  "RiskName": "CentOS Linux 6 security standard compliance - MLPS level-3",
  "LowWarningCount": 0,
  "CheckCount": 15,
  "RiskId": 50,
  "Level": "medium",
  "MediumWarningCount": 0,
  "TypeAlias": "System",
  "LastFoundTime": "2019-02-19 14:59:17"
},
{
  "SubTypeAlias": "Linux Ubuntu security standard compliance - MLPS level-2",
  "HighWarningCount": 0,
  "WarningMachineCount": 0,
  "RiskName": "Linux Ubuntu security standard compliance - MLPS level-2",
  "LowWarningCount": 0,
  "CheckCount": 14,
  "RiskId": 55,
  "Level": "medium",
  "MediumWarningCount": 0,
  "TypeAlias": "System",
  "LastFoundTime": "2019-02-19 12:57:23"
},
{
  "SubTypeAlias": "Linux Ubuntu security standard compliance - MLPS level-3",
```

```
"HighWarningCount":0,
"WarningMachineCount":0,
"RiskName":"Linux Ubuntu security standard compliance - MLPS level-3",
"LowWarningCount":0,
"CheckCount":15,
"RiskId":56,
"Level":"medium",
"MediumWarningCount":0,
"TypeAlias":"System",
"LastFoundTime":"2019-02-19 12:57:23"
},
{
  "SubTypeAlias":"Linux Ubuntu security baseline check",
  "HighWarningCount":0,
  "WarningMachineCount":0,
  "RiskName":"Linux Ubuntu security baseline check",
  "LowWarningCount":0,
  "CheckCount":16,
  "RiskId":54,
  "Level":"high",
  "MediumWarningCount":0,
  "TypeAlias":"System",
  "LastFoundTime":"2019-02-19 12:57:23"
},
{
  "SubTypeAlias":"Windows 2012 R2 security baseline check",
  "HighWarningCount":0,
  "WarningMachineCount":0,
  "RiskName":"Windows 2012 R2 security baseline check",
  "LowWarningCount":0,
  "CheckCount":12,
  "RiskId":51,
  "Level":"high",
  "MediumWarningCount":0,
  "TypeAlias":"System",
  "LastFoundTime":"2019-02-19 12:44:58"
}
],
"PageSize":20,
"RequestId":"DFA6CDC5-E826-4D18-A499-BEF9DA31F1AD",
"CurrentPage":1
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.6.2. DescribeStrategy

Queries the configurations of baseline check policies.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeStrategy	The operation that you want to perform. Set the value to DescribeStrategy.
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
SourceIp	String	No	1.2.3.4	The source IP address of the request.
StrategyIds	String	No	test1,test2,test3	The IDs of the baseline check policies. Separate multiple IDs with commas (,).

Response parameters

Parameter	Type	Example	Description
RequestId	String	16B9826C-B99F-4F8A-8048-EA81D6D3DE8B	The ID of the request.
Strategies	Array		The information about the baseline check policy.
ConfigTargets	Array		The information about the group associated with the baseline check policy.
Flag	String	add	The related ID.
Target	String	3259405	The ID of the related group.
TargetType	String	groupId	The type of the related group.
CycleDays	Integer	1	The cycle of the baseline check. • 1: every second day • 3: every fourth day • 7: every eighth day • 30: every 31st day

Parameter	Type	Example	Description
CycleStartTime	Integer	6	The time when the baseline check starts. Valid values: 0, 6, 12, and 18.
EcsCount	Integer	5	The number of servers on which baseline checks were performed based on the specified baseline check policy.
ExecStatus	Integer	1	The execution status of the baseline check. Valid values: • 1: The baseline check is not running. • 2: The baseline check is running.
Id	Integer	212635	The ID of the policy.
Name	String	test	The name of the policy.
PassRate	Integer	80	The pass rate of the latest baseline check.
ProcessRate	Integer	80	The progress of the baseline check.
RiskCount	Integer	5	The number of selected check items.
Type	Integer	1	The type of the baseline check policy. Valid values: • 1: default policy • 2: custom policy

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeStrategy
? Lang=zh
&SourceIp=127.0.0.1
&StrategyIds=1,2,3
&<Common request parameters>
```

Sample success responses

XML format


```
<DescribeStratety>
  <RequestId>ACAFE09B-3346-433B-BDA8-369AB3D9B4F9</RequestId>
  <Strategies>
    <CycleStartTime>6</CycleStartTime>
    <EcsCount>0</EcsCount>
    <Type>2</Type>
    <ExecStatus>1</ExecStatus>
    <ProcessRate>0</ProcessRate>
    <CycleDays>3</CycleDays>
    <Id>15161</Id>
    <ConfigTargets>
      <Target>4361221</Target>
      <TargetType>groupId</TargetType>
      <Flag>add</Flag>
    </ConfigTargets>
    <RiskCount>1</RiskCount>
    <Name>test</Name>
  </Strategies>
  <Strategies>
    <CycleStartTime>0</CycleStartTime>
    <EcsCount>17</EcsCount>
    <PassRate>81</PassRate>
    <Type>1</Type>
    <ExecStatus>1</ExecStatus>
    <ProcessRate>0</ProcessRate>
    <CycleDays>1</CycleDays>
    <Id>20</Id>
    <ConfigTargets>
      <Target>281801</Target>
      <TargetType>groupId</TargetType>
      <Flag>del</Flag>
    </ConfigTargets>
    <ConfigTargets>
      <Target>4790960</Target>
      <TargetType>groupId</TargetType>
      <Flag>del</Flag>
    </ConfigTargets>
    <RiskCount>13</RiskCount>
    <Name>Default policy</Name>
  </Strategies>
</DescribeStratety>
```

JSON format

```
{
  "RequestId": "ACAFE09B-3346-433B-BDA8-369AB3D9B4F9",
  "Strategies": [
    {
      "Name": "test",
      "RiskCount": 1,
      "CycleDays": 3,
      "Type": 2,
      "CycleStartTime": 6,
      "ConfigTargets": [
        {
          "Flag": "add",
          "Target": "4361221",
          "TargetType": "groupId"
        }
      ],
      "ProcessRate": 0,
      "Id": 15161,
      "ExecStatus": 1,
      "EcsCount": 0
    },
    {
      "Name": "Default policy",
      "RiskCount": 13,
      "PassRate": 81,
      "CycleDays": 1,
      "Type": 1,
      "CycleStartTime": 0,
      "ConfigTargets": [
        {
          "Flag": "del",
          "Target": "281801",
          "TargetType": "groupId"
        },
        {
          "Flag": "del",
          "Target": "4790960",
          "TargetType": "groupId"
        }
      ],
      "ProcessRate": 0,
      "Id": 20,
      "ExecStatus": 1,
      "EcsCount": 17
    }
  ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.6.3. DescribeStrategyExecDetail

Queries the details of the latest baseline check by using a baseline check policy. The details include the time when the check is performed, the number of risk items, and the baseline risk details.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeStrategyExecDetail	The operation that you want to perform. Set the value to DescribeStrategyExecDetail.
StrategyId	Integer	Yes	1	The ID of the baseline check policy.  Note To query the results of a baseline check that uses only one policy, you must specify the ID of the policy. You can call the DescribeStrategy operation to obtain the ID.
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
EndTime	String	2019-01-08 20:11:20	The time when the baseline check ends.
FailCount	Integer	94	The number of risk items that failed to pass the baseline check.
FailedEcsList	Array		The list of servers on which risk items were detected.
IP	String	1.2.3.4	The IP address of the instance on which the baseline check was performed.
InstanceName	String	Test-20180703	The name of the instance.
IntranetIp	String	1.2.3.5	The internal IP address.

Parameter	Type	Example	Description
Reason	String	Detect timeout	The cause of the baseline check failure.
InProcessCount	Integer	0	The number of baseline check tasks that are running.
Percent	String	100%	The progress of the baseline check.
RequestId	String	09322632-4668-4AD9-BD0D-32757DEFBBA6	The ID of the request.
Source	String	Manual	The type of the baseline check. • Schedule • Manual
StartTime	String	2019-01-08 19:41:12	The time when the baseline check starts.
SuccessCount	Integer	81	The number of check items that passed the baseline check.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeStrategyExecDetail
&StrategyId=1
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribeStrategyExecDetail>
  <RequestId>6489FA6A-D241-4380-9D8C-A8804484CA40</RequestId>
  <EndTime>2019-04-10 00:58:30</EndTime>
  <Percent>100%</Percent>
  <FailCount>1</FailCount>
  <StartTime>2019-04-10 00:19:01</StartTime>
  <SuccessCount>1</SuccessCount>
  <Source>Schedule</Source>
  <FailedEcsList>
    <InstanceName>health-check002</InstanceName>
    <IP>1.2.3.4</IP>
    <IntranetIp>1.2.3.5</IntranetIp>
    <Reason>Agent offline</Reason>
  </FailedEcsList>
  <InProcessCount>0</InProcessCount>
</DescribeStrategyExecDetail>
```

JSON format

```
{
  "Source": "Schedule",
  "InProcessCount": 0,
  "SuccessCount": 1,
  "RequestId": "6489FA6A-D241-4380-9D8C-A8804484CA40",
  "Percent": "100%",
  "FailedEcsList": [
    {
      "IntranetIp": "1.2.3.5",
      "IP": "1.2.3.4",
      "InstanceName": "health-check002",
      "Reason": "Agent offline"
    }
  ],
  "EndTime": "2019-04-10 00:58:30",
  "StartTime": "2019-04-10 00:19:01",
  "FailCount": 1
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.6.4. DescribeCheckWarnings

Queries specified risk items and check items of a specified server.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCheckWarnings	The operation that you want to perform. Set the value to DescribeCheckWarnings.
RiskId	Long	Yes	1	The ID of the risk item.  Note To query specified risk items and check items of a specified server, you must specify the IDs of the risk items. You can call the DescribeCheckWarningSummary operation to obtain the IDs.
Uuid	String	Yes	d42f938c-d962-48a0-90f9-05*****	The ID of the server on which a baseline check is performed. The ID of the risk item.  Note To query specified risk items and check items of a specified server, you must specify the ID of the server on which the baseline check is run. You can call the DescribeWarningMachines operation to obtain the IDs.
CurrentPage	Integer	No	1	The number of the current page. Pages start from page 1. The default value is 1, which indicates that the first page is displayed.
Lang	String	No	zh	The natural language of the request and response. Valid values: zh: Chinese en: English
PageSize	Integer	No	20	The number of entries to return on each page. The default value is 20, which indicates that 20 entries are returned on each page.

Parameter	Type	Required	Example	Description
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
CheckWarnings	Array		The information about the check item.
CheckId	Long	1	The ID of the check item.
CheckWarningId	Long	10	The ID of the alert.
Item	String	Password expiration alert	The name of the check item.
Level	String	high	The severity level of the risk item. Valid values: • high • medium • low
Status	Integer	1	The status of the check item. Valid values: • 1: failed • 2: verifying • 3: passed • 5: expired • 6: ignored
Type	String	Identity authentication	The type of the check item.
Uuid	String	d42f938c-d962-48a0-90f9-*****	The ID of the server on which the baseline check was performed.
Count	Integer	10	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	20	The number of entries returned per page.

Parameter	Type	Example	Description
RequestId	String	0DFCADBA-7065-42DA-AF17-6868B9C2A8CF	The ID of the request.
TotalCount	Integer	100	The total number of entries.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCheckWarnings
&RiskId=1
&Uuid=d42f938c-d962-48a0-90f9-05e4eaf92e34
&Lang=zh
&SourceIp=127.0.0.1
&CurrentPage=1
&PageSize=20
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeCheckWarnings>
  <TotalCount>16</TotalCount>
  <CheckWarnings>
    <Status>6</Status>
    <Item>Check accounts without passwords in the system
      </Item>
    <Type>Identity authentication</Type>
    <Uuid>974af549-3248-44dd-9180-***</Uuid>
    <CheckId>1</CheckId>
    <CheckWarningId>1393768</CheckWarningId>
    <Level>high</Level>
  </CheckWarnings>
  <CheckWarnings>
    <Status>6</Status>
    <Item>Check password complexity</Item>
    <Type>Identity authentication</Type>
    <Uuid>974af549-3248-44dd-9180-***</Uuid>
    <CheckId>52</CheckId>
    <CheckWarningId>1393774</CheckWarningId>
    <Level>high</Level>
  </CheckWarnings>
  <CheckWarnings>
    <Status>6</Status>
    <Item>Make sure that root is the only account whose UID is 0</Item>
    <Type>Identity authentication</Type>
```



```
<Uuid>974af549-3248-44dd-9180-***</Uuid>
<CheckId>15</CheckId>
<CheckWarningId>1393773</CheckWarningId>
<Level>high</Level>
</CheckWarnings>
<CheckWarnings>
  <Status>6</Status>
  <Item>Enable address space layout randomization</Item>
  <Type>Intrusion prevention</Type>
  <Uuid>974af549-3248-44dd-9180-***</Uuid>
  <CheckId>14</CheckId>
  <CheckWarningId>1393772</CheckWarningId>
  <Level>high</Level>
</CheckWarnings>
<CheckWarnings>
  <Status>6</Status>
  <Item>Specify user permissions on file configurations</Item>
  <Type>File permissions</Type>
  <Uuid>974af549-3248-44dd-9180-***</Uuid>
  <CheckId>13</CheckId>
  <CheckWarningId>1393767</CheckWarningId>
  <Level>high</Level>
</CheckWarnings>
<CheckWarnings>
  <Status>6</Status>
  <Item>Specify permissions on the access control configuration file</Item>
  <Type>File permissions</Type>
  <Uuid>974af549-3248-44dd-9180-***</Uuid>
  <CheckId>12</CheckId>
  <CheckWarningId>1393771</CheckWarningId>
  <Level>high</Level>
</CheckWarnings>
<CheckWarnings>
  <Status>6</Status>
  <Item>Make sure that SSH LogLevel is set to INFO</Item>
  <Type>Service configuration</Type>
  <Uuid>974af549-3248-44dd-9180-***</Uuid>
  <CheckId>11</CheckId>
  <CheckWarningId>1393766</CheckWarningId>
  <Level>high</Level>
</CheckWarnings>
<CheckWarnings>
  <Status>6</Status>
  <Item>Make sure that the rsyslog service is enabled</Item>
  <Type>Security auditing</Type>
  <Uuid>974af549-3248-44dd-9180-***</Uuid>
  <CheckId>10</CheckId>
  <CheckWarningId>1393770</CheckWarningId>
  <Level>high</Level>
</CheckWarnings>
<CheckWarnings>
  <Status>6</Status>
  <Item>Specify the timeout period for SSH idle connections</Item>
  <Type>Service configuration</Type>
```

```

        <Uuid>974af549-3248-44dd-9180-***</Uuid>
        <CheckId>8</CheckId>
        <CheckWarningId>1393765</CheckWarningId>
        <Level>high</Level>
    </CheckWarnings>
    <CheckWarnings>
        <Status>6</Status>
        <Item>Make sure that SSH V2 is used</Item>
        <Type>Service configuration</Type>
        <Uuid>974af549-3248-44dd-9180-***</Uuid>
        <CheckId>7</CheckId>
        <CheckWarningId>1393764</CheckWarningId>
        <Level>high</Level>
    </CheckWarnings>
    <CheckWarnings>
        <Status>6</Status>
        <Item>Make sure that SSH MaxAuthTries is set to a value from 3 to 6</Item>
        <Type>Service configuration</Type>
        <Uuid>974af549-3248-44dd-9180-***</Uuid>
        <CheckId>6</CheckId>
        <CheckWarningId>1393763</CheckWarningId>
        <Level>high</Level>
    </CheckWarnings>
    <CheckWarnings>
        <Status>6</Status>
        <Item>Make sure that alerts are triggered at least seven days before passwords expire</Item>
        <Type>Identity authentication</Type>
        <Uuid>974af549-3248-44dd-9180-***</Uuid>
        <CheckId>5</CheckId>
        <CheckWarningId>1393769</CheckWarningId>
        <Level>high</Level>
    </CheckWarnings>
    <CheckWarnings>
        <Status>6</Status>
        <Item>Set the shortest interval between password changes</Item>
        <Type>Identity authentication</Type>
        <Uuid>974af549-3248-44dd-9180-***</Uuid>
        <CheckId>4</CheckId>
        <CheckWarningId>1393761</CheckWarningId>
        <Level>high</Level>
    </CheckWarnings>
    <CheckWarnings>
        <Status>6</Status>
        <Item>Set the password validity period</Item>
        <Type>Identity authentication</Type>
        <Uuid>974af549-3248-44dd-9180-***</Uuid>
        <CheckId>3</CheckId>
        <CheckWarningId>1393760</CheckWarningId>
        <Level>high</Level>
    </CheckWarnings>
    <CheckWarnings>
        <Status>6</Status>
        <Item>Disable SSH logon for accounts without specified passwords

```

```
        </Item>
        <Type>Service configuration</Type>
        <Uuid>974af549-3248-44dd-9180-***</Uuid>
        <CheckId>2</CheckId>
        <CheckWarningId>1393762</CheckWarningId>
        <Level>high</Level>
    </CheckWarnings>
    <CheckWarnings>
        <Status>6</Status>
        <Item>Check whether password reuse is limited</Item>
        <Type>Identity authentication</Type>
        <Uuid>974af549-3248-44dd-9180-***</Uuid>
        <CheckId>58</CheckId>
        <CheckWarningId>1393775</CheckWarningId>
        <Level>high</Level>
    </CheckWarnings>
    <PageSize>20</PageSize>
    <RequestId>C1E6C4FE-DE00-4B75-A01E-FCAB55A36449</RequestId>
    <CurrentPage>1</CurrentPage>
    <Count>16</Count>
</DescribeCheckWarnings>
```

JSON format

```
{
  "Count":16,
  "TotalCount":16,
  "PageSize":20,
  "RequestId":"C1E6C4FE-DE00-4B75-A01E-FCAB55A36449",
  "CurrentPage":1,
  "CheckWarnings":[
    {
      "Uuid":"974af549-3248-44dd-9180-***",
      "Status":6,
      "CheckWarningId":1393768,
      "Item":"Check accounts without passwords in the system\r\n\r\n",
      "Type":"Identity authentication",
      "Level":"high",
      "CheckId":1
    },
    {
      "Uuid":"974af549-3248-44dd-9180-***",
      "Status":6,
      "CheckWarningId":1393774,
      "Item":"Check password complexity",
      "Type":"Identity authentication",
      "Level":"high",
      "CheckId":52
    },
    {
      "Uuid":"974af549-3248-44dd-9180-***",
      "Status":6,
```

```
"CheckWarningId":1393773,
"Item":"Make sure that root is the only account whose UID is 0",
"Type":"Identity authentication",
"Level":"high",
"CheckId":15
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393772,
  "Item":"Enable address space layout randomization",
  "Type":"Intrusion prevention",
  "Level":"high",
  "CheckId":14
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393767,
  "Item":"Specify user permissions on file configurations",
  "Type":"File permissions",
  "Level":"high",
  "CheckId":13
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393771,
  "Item":"Specify the permissions on the access control configuration file",
  "Type":"File permissions",
  "Level":"high",
  "CheckId":12
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393766,
  "Item":"Make sure that SSH LogLevel is set to INFO",
  "Type":"Service configuration",
  "Level":"high",
  "CheckId":11
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393770,
  "Item":"Make sure that the rsyslog service is enabled",
  "Type":"Security auditing",
  "Level":"high",
  "CheckId":10
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
```

```
"CheckWarningId":1393765,
"Item":"Specify the timeout period for SSH idle connections",
"Type":"Service configuration",
"Level":"high",
"CheckId":8
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393764,
  "Item":"Make sure that SSH V2 is used",
  "Type":"Service configuration",
  "Level":"high",
  "CheckId":7
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393763,
  "Item":"Make sure that SSH MaxAuthTries is set to a value from 3 to 6",
  "Type":"Service configuration",
  "Level":"high",
  "CheckId":6
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393769,
  "Item":"Make sure that alerts are triggered at least seven days before passwords expire",
  "Type":"Identity authentication",
  "Level":"high",
  "CheckId":5
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393761,
  "Item":"Set the shortest interval between password changes",
  "Type":"Identity authentication",
  "Level":"high",
  "CheckId":4
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393760,
  "Item":"Set the password validity period",
  "Type":"Identity authentication",
  "Level":"high",
  "CheckId":3
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393762,
  "Item":"Set the password complexity requirements",
  "Type":"Identity authentication",
  "Level":"high",
  "CheckId":2
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393760,
  "Item":"Set the password validity period",
  "Type":"Identity authentication",
  "Level":"high",
  "CheckId":3
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393761,
  "Item":"Set the shortest interval between password changes",
  "Type":"Identity authentication",
  "Level":"high",
  "CheckId":4
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393762,
  "Item":"Set the password complexity requirements",
  "Type":"Identity authentication",
  "Level":"high",
  "CheckId":2
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393763,
  "Item":"Make sure that SSH MaxAuthTries is set to a value from 3 to 6",
  "Type":"Service configuration",
  "Level":"high",
  "CheckId":6
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393764,
  "Item":"Make sure that SSH V2 is used",
  "Type":"Service configuration",
  "Level":"high",
  "CheckId":7
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393765,
  "Item":"Specify the timeout period for SSH idle connections",
  "Type":"Service configuration",
  "Level":"high",
  "CheckId":8
}
```

```
"Status":6,
"CheckWarningId":1393762,
"Item":"Disable SSH logon for accounts without specified passwords
\r\n                                \r\n                                \r\n",
"Type":"Service configuration",
"Level":"high",
"CheckId":2
},
{
  "Uuid":"974af549-3248-44dd-9180-***",
  "Status":6,
  "CheckWarningId":1393775,
  "Item":"Check whether password reuse is limited",
  "Type":"Identity authentication",
  "Level":"high",
  "CheckId":58
}
]
```

Error codes

For a list of error codes, see [Error codes](#).

7.6.5. DescribeCheckWarningDetail

Queries the details of a specific check item.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCheckWarningDetail	The operation that you want to perform. Set the value to DescribeCheckWarningDetail.
CheckWarningId	Long	Yes	1	The ID of the alert triggered by the check item.  Note To query the details of a specific check item, you must specify the ID of the alert triggered by the check item. You can call the DescribeCheckWarnings operation to obtain the alert ID.

Parameter	Type	Required	Example	Description
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
SourceIp	String	No	1.2.3.4	The source IP address of the request.

Response parameters

Parameter	Type	Example	Description
Advice	String	Fix now	The suggestion for the management of the risk item.
CheckId	Long	1	The ID of the check item.
Description	String	Password expiring	The additional details about the risk item.
Item	String	Password expiration alert	The name of the check item.
Level	String	high	The severity level of the risk item. • high: The item is a high-risk one and highlighted in red. • medium: The item is a medium-risk one and highlighted in orange. • low: The item is a low-risk one and highlighted in gray.
Prompt	String	Password expiration alert	The prompt for the risk item.
RequestId	String	09969D2C-4FAD-429E-BFBF-9A60DEF8BF6F	The ID of the request.
Type	String	Identity authentication	The type of the check item.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeCheckWarningDetail
&CheckWarningId=1
&SourceIp=127.0.0.1
&Lang=zh
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeCheckWarningDetail>
  <Item>Specify user permissions on file configurations</Item>
  <Type>File permissions</Type>
  <Description>Specify user permissions on file configurations</Description>
  <RequestId>9F2361B3-B7C3-4189-8DB5-C6D1F67BC225</RequestId>
  <CheckId>13</CheckId>
  <Prompt></Prompt>
  <Level>high</Level>
  <Advice>Run the following five commands
chown root:root /etc/passwd /etc/shadow /etc/group /etc/gshadow
chmod 0644 /etc/group
chmod 0644 /etc/passwd
chmod 0400 /etc/shadow
chmod 0400 /etc/gshadow </Advice>
</DescribeCheckWarningDetail>
```

JSON format

```
{
  "Prompt": "",
  "Description": "Specify user permissions on file configurations",
  "Item": "Specify user permissions on file configurations",
  "Type": "File permissions",
  "RequestId": "9F2361B3-B7C3-4189-8DB5-C6D1F67BC225",
  "Advice": "Run the following five commands\r\nchown root:root /etc/passwd /etc/shadow /etc/group /etc/gshadow\r\nchmod 0644 /etc/group \r\nchmod 0644 /etc/passwd \r\nchmod 0400 /etc/shadow \r\nchmod 0400 /etc/gshadow ",
  "Level": "high",
  "CheckId": 13
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.6.6. DescribeWarningMachines

Queries information about servers on which a baseline check is performed. The information includes the statistics and status of risk items and IDs of the servers.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeWarningMachines	The operation that you want to perform. Set the value to DescribeWarningMachines .
RiskId	Long	Yes	1	The ID of the risk item.  Note To query information about servers on which a baseline check is performed, you must specify the ID of the risk item that is related to the baseline check. You can call the DescribeCheckWarningSummary operation to obtain the ID.
SourceIp	String	No	1.2.3.4	The source IP address of the request.
Lang	String	No	zh	The natural language of the request and response. Valid values: • zh: Chinese • en: English
MachineName	String	No	test_ecs172	The name of the server on which a baseline check is performed.
Uuids	String	No	xxx-aaa-bbb-ccc	The ID of the server on which a baseline check is performed. Separate multiple IDs with commas (,).
StrategyId	Long	No	1	The ID of the baseline check policy.
PageSize	Integer	No	10	The number of entries to return on each page.
CurrentPage	Integer	No	1	The number of the current page.

Response parameters

Parameter	Type	Example	Description
Count	Integer	10	The number of entries returned on the current page.
CurrentPage	Integer	1	The number of the current page.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	00BDE2-284A-4534-BD09-FB69836DD750	The ID of the request.
TotalCount	Integer	100	The total number of returned entries.
WarningMachines	Array		The information about the servers that generate alerts.
HighWarningCount	Integer	10	The number of high-risk check items.
InstanceId	String	i-m5ee8b9nr3h30mhb****	The instance ID of the server.
InstanceName	String	aaaawebtest	The name of the instance.
InternetIp	String	1.2.3.4	The public IP address of the server.
IntranetIp	String	1.2.3.5	The private IP address of the server.
LowWarningCount	Integer	3	The number of low-risk check items.
MediumWarningCount	Integer	2	The number of medium-risk check items.
PassCount	Integer	10	The number of items that have passed the baseline check.
RegionId	String	cn-qingdao	The region ID of the server.

Parameter	Type	Example	Description
Status	Integer	1	The verification status of the risk items that are fixed. Valid values: 1: completed 2: verifying
Uuid	String	xxx-aaa-bbb-ccc	The ID of the server on which a baseline check is performed.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeWarningMachines
&RiskId=1
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribeWarningMachinesResponse>
  <TotalCount>100</TotalCount>
  <RequestId>00BDE2-284A-4534-BD09-FB69836DD750</RequestId>
  <PageSize>10</PageSize>
  <CurrentPage>1</CurrentPage>
  <WarningMachines>
    <InstanceName>aaawebtest</InstanceName>
    <Status>1</Status>
    <MediumWarningCount>2</MediumWarningCount>
    <Uuid>xxx-aaa-bbb-ccc</Uuid>
    <InternetIp>1.2.3.4</InternetIp>
    <InstanceId>i-m5ee8b9nr3h30mhb****</InstanceId>
    <HighWarningCount>10</HighWarningCount>
    <RegionId>cn-qingdao</RegionId>
    <PassCount>10</PassCount>
    <IntranetIp>1.2.3.5</IntranetIp>
    <LowWarningCount>3</LowWarningCount>
  </WarningMachines>
  <Count>10</Count>
</DescribeWarningMachinesResponse>
```

JSON format

```
{
  "TotalCount": "100",
  "RequestId": "00BDE2-284A-4534-BD09-FB69836DD750",
  "PageSize": "10",
  "CurrentPage": "1",
  "WarningMachines": [{
    "InstanceName": "aaawebtest",
    "Status": "1",
    "MediumWarningCount": "2",
    "Uuid": "xxx-aaa-bbb-ccc",
    "InternetIp": "1.2.3.4",
    "InstanceId": "i-m5ee8b9nr3h30mhb****",
    "HighWarningCount": "10",
    "RegionId": "cn-qingdao",
    "PassCount": "10",
    "IntranetIp": "1.2.3.5",
    "LowWarningCount": "3"
  }],
  "Count": "10"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.7. Asset fingerprints

7.7.1. DescribePropertyCount

Queries the statistics of asset fingerprints, including the numbers of processes, ports, software, users, and scheduled tasks.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePropertyCount	The operation that you want to perform. Set the value to DescribePropertyCount.

Parameter	Type	Required	Example	Description
Type	String	No	port	The type of the asset fingerprint. Valid values: • user • software • process • port • cron: scheduled tasks  Note If you do not specify a type, all types of asset fingerprints are queried.
UuidList	String	No	[c4678332-ef3**,c46***]	The IDs of the assets, which are unique.

Response parameters

Parameter	Type	Example	Description
Cron	Integer	261	The number of scheduled tasks.
Port	Integer	163	The number of listening ports.
Process	Integer	367	The number of running processes.
RequestId	String	7E0618A9-D5EF-4220-9471-C42B5E92719F	The ID of the request.
Software	Integer	5073	The number of software assets.
User	Integer	114	The number of users.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePropertyCount
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribePropertyCount>
  <User>340</User>
  <Software>2598</Software>
  <Port>265</Port>
  <Process>395</Process>
  <RequestId>3D93ABAB-0AC2-4A27-A03B-35C0E4AA0443</RequestId>
  <Cron>261</Cron>
</DescribePropertyCount>
```

JSON format

```
{
  "User":340,
  "Software":2598,
  "Port":265,
  "RequestId":"3D93ABAB-0AC2-4A27-A03B-35C0E4AA0443",
  "Process":395,
  "Cron":261
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.7.2. DescribePropertyPortDetail

Queries the details of a port.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePropertyPortDetail	The operation that you want to perform. Set the value to DescribePropertyPortDetail .
Remark	String	No	1.2.3.4	The name or IP address of the server.
Port	String	No	22	The port of the server.
ProcName	String	No	sshd	The name of the process.
Uuid	String	No	50d213b4-3a35-427a-b8a5-***	The ID of the asset, which is unique.
CurrentPage	Integer	No	1	The page number of the current page.

Parameter	Type	Required	Example	Description
PageSize	Integer	No	6	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
RequestId	String	FAA793EF-5B14-4CDD-B3E0-B14D4342C422	The ID of the request.
Propertys	Array		Details of the port.
BindIp	String	1.2.3.4	The IP addresses bound to the port.
Port	String	22	The port number.
InstanceName	String	test-***	The name of the asset related to the port.
Proto	String	tcp	The network protocol.
Ip	String	1.2.3.1	The public IP address of the asset.
Create	String	2019-05-13T10:39Z	The time when the data is last collected.
CreateTimestamp	Long	1557715141000	The timestamp of last data collection.
ProcName	String	sshd	The name of the process that is using the port.
Uuid	String	50d213b4-3a35-427a-b8a5-04b0c7e1f4d2"	The ID of the asset related to the port.
InstanceId	String	50d213b4-3a35-427a-b8a5-04b0c7e1f4d2"	The ID of the asset related to the port.
IntranetIp	String	1.2.3.2	The private IP address of the asset.

Parameter	Type	Example	Description
InternetIp	String	1.2.3.1	The public IP address of the asset.
PageInfo	Struct		The page information.
Count	Integer	5	The number of entries returned on the current page.
PageSize	Integer	5	The number of entries returned per page.
TotalCount	Integer	762	The total number of returned entries.
CurrentPage	Integer	1	The page number of the current page.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePropertyPortDetail
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribePropertyPortDetailResponse>
  <Property>
    <InstanceName>centos-xx</InstanceName>
    <Uuid>00274759-73ef-485a-ae40-c2b5972f50cd</Uuid>
    <Proto>tcp</Proto>
    <InternetIp>101.xx.xx.104</InternetIp>
    <InstanceId>i-2ze645t5u9jo4txxx</InstanceId>
    <Create>2020-01-09T13:53Z</Create>
    <Port>22</Port>
    <Ip>101.xx.xx.104</Ip>
    <ProcName>sshd</ProcName>
    <CreateTimestamp>1578549227000</CreateTimestamp>
    <IntranetIp>192.xx.xx.96</IntranetIp>
    <BindIp>0.0.0.0</BindIp>
  </Property>
  <Property>
    <InstanceName>paas-xxx-test1122</InstanceName>
    <Uuid>007ecd45-e90f-4290-9eac-758407aa1509</Uuid>
    <Proto>tcp</Proto>
    <InternetIp>118.xx.xx.7</InternetIp>
    <InstanceId>i-m5e56ycm6xx7if43xx</InstanceId>
    <Create>2020-02-18T15:52Z</Create>
```



```
<Port>10251</Port>
<Ip>118.xx.xx.7</Ip>
<ProcName>kube-scheduler</ProcName>
<CreateTimestamp>1582012349000</CreateTimestamp>
<IntranetIp>192.xx.xx.192</IntranetIp>
<BindIp>:::</BindIp>
</Property>
<Property>
  <InstanceName>paas-xx-2</InstanceName>
  <Uuid>007ecd45-e9xx-4290-9eac-758407aa15xx</Uuid>
  <Proto>tcp</Proto>
  <InternetIp>118.xx.xx.7</InternetIp>
  <InstanceId>i-m5e56ycm6s0xxf43maxx</InstanceId>
  <Create>2020-02-18T15:52Z</Create>
  <Port>10252</Port>
  <Ip>118.xx.xx.7</Ip>
  <ProcName>kube-controller-manager</ProcName>
  <CreateTimestamp>1582012349000</CreateTimestamp>
  <IntranetIp>192.xx.xx.192</IntranetIp>
  <BindIp>:::</BindIp>
</Property>
<Property>
  <InstanceName>paas-xx-2</InstanceName>
  <Uuid>007ecd45-e90f-42xx-9eac-758407aa15xx</Uuid>
  <Proto>tcp</Proto>
  <InternetIp>118.xx.xx.7</InternetIp>
  <InstanceId>i-m5e56ycmxx07if43maxx</InstanceId>
  <Create>2020-02-18T15:52Z</Create>
  <Port>2379</Port>
  <Ip>118.xx.xx.7</Ip>
  <ProcName>etcd</ProcName>
  <CreateTimestamp>1582012349000</CreateTimestamp>
  <IntranetIp>192.xx.xx.192</IntranetIp>
  <BindIp>:::</BindIp>
</Property>
<Property>
  <InstanceName>paas-xx-2</InstanceName>
  <Uuid>007ecd45-e90f-4290-9exx-758407aa15xx</Uuid>
  <Proto>tcp</Proto>
  <InternetIp>118.xx.xx.7</InternetIp>
  <InstanceId>i-m5e56ycm6s07if43maxx</InstanceId>
  <Create>2020-02-18T15:52Z</Create>
  <Port>6443</Port>
  <Ip>118.xx.xx.7</Ip>
  <ProcName>kube-apiserver</ProcName>
  <CreateTimestamp>1582012349000</CreateTimestamp>
  <IntranetIp>192.xx.xx.192</IntranetIp>
  <BindIp>:::</BindIp>
</Property>
<PageInfo>
  <Count>5</Count>
  <PageSize>5</PageSize>
  <TotalCount>762</TotalCount>
  <CurrentPage>1</CurrentPage>
</PageInfo>
```

```
</PageInfo>
<requestId>FAA793EF-5B14-4CDD-B3E0-B14D4342C422</requestId>
</DescribePropertyPortDetailResponse>
```

JSON **format**

```
{
  "Propertys": [
    {
      "InstanceName": "centos-xx",
      "Uuid": "00274759-73ef-485a-ae40-c2b5972f50cd",
      "Proto": "tcp",
      "InternetIp": "101.xx.xx.104",
      "InstanceId": "i-2ze645t5u9jo4txxx",
      "Create": "2020-01-09T13:53Z",
      "Port": "22",
      "Ip": "101.xx.xx.104",
      "ProcName": "sshd",
      "CreateTimestamp": 1578549227000,
      "IntranetIp": "192.xx.xx.96",
      "BindIp": "0.0.0.0"
    },
    {
      "InstanceName": "paas-xxx-test1122",
      "Uuid": "007ecd45-e90f-4290-9eac-758407aa1509",
      "Proto": "tcp",
      "InternetIp": "118.xx.xx.7",
      "InstanceId": "i-m5e56ycm6xx7if43xx",
      "Create": "2020-02-18T15:52Z",
      "Port": "10251",
      "Ip": "118.xx.xx.7",
      "ProcName": "kube-scheduler",
      "CreateTimestamp": 1582012349000,
      "IntranetIp": "192.xx.xx.192",
      "BindIp": ":::"
    },
    {
      "InstanceName": "paas-xx-2",
      "Uuid": "007ecd45-e9xx-4290-9eac-758407aa15xx",
      "Proto": "tcp",
      "InternetIp": "118.xx.xx.7",
      "InstanceId": "i-m5e56ycm6s0xxf43maxx",
      "Create": "2020-02-18T15:52Z",
      "Port": "10252",
      "Ip": "118.xx.xx.7",
      "ProcName": "kube-controller-manager",
      "CreateTimestamp": 1582012349000,
      "IntranetIp": "192.xx.xx.192",
      "BindIp": ":::"
    },
    {
      "InstanceName": "paas-xx-2",
      "Uuid": "007ecd45-e90f-42xx-9eac-758407aa15xx",
      "Proto": "tcp",
```

```
    "InternetIp": "118.xx.xx.7",
    "InstanceId": "i-m5e56ycmxx07if43maxx",
    "Create": "2020-02-18T15:52Z",
    "Port": "2379",
    "Ip": "118.xx.xx.7",
    "ProcName": "etcd",
    "CreateTimestamp": 1582012349000,
    "IntranetIp": "192.xx.xx.192",
    "BindIp": ":",
  },
  {
    "InstanceName": "paas-xx-2",
    "Uuid": "007ecd45-e90f-4290-9exx-758407aa15xx",
    "Proto": "tcp",
    "InternetIp": "118.xx.xx.7",
    "InstanceId": "i-m5e56ycm6s07if43maxx",
    "Create": "2020-02-18T15:52Z",
    "Port": "6443",
    "Ip": "118.xx.xx.7",
    "ProcName": "kube-apiserver",
    "CreateTimestamp": 1582012349000,
    "IntranetIp": "192.xx.xx.192",
    "BindIp": ":",
  }
],
"PageInfo": {
  "Count": 5,
  "PageSize": 5,
  "TotalCount": 762,
  "CurrentPage": 1
},
"requestId": "FAA793EF-5B14-4CDD-B3E0-B14D4342C422"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.7.3. DescribePropertyProcDetail

Queries the details of a process.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePropertyProcDetail	The operation that you want to perform. Set the value to DescribePropertyProcDetail.

Parameter	Type	Required	Example	Description
Cmdline	String	No	. /8888	The parameter that is used to start the process.
CurrentPage	Integer	No	1	The page number of the current page.
Name	String	No	8888	The name of the process.
PageSize	Integer	No	5	The number of entries to return on each page.
Remark	String	No	1.2.3.4	The name or IP address of the server.
User	String	No	root	The user who runs the process.
Uuid	String	No	c4678332-ef35-4ad4-***	The ID of the asset related to the process.

Response parameters

Parameter	Type	Example	Description
PageInfo			The page information.
Count	Integer	1	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	5	The number of entries returned per page.
TotalCount	Integer	1	The total number of returned entries.
Propertys	Array		The returned process information.
Cmdline	String	. /8888	The parameter that was used to start the process.

Parameter	Type	Example	Description
Create	String	2019-05-15T11:08Z	The last time when the data was collected.
CreateTimestamp	Long	1565686951000	The timestamp of last data collection.
EuidName	String	root	The permission to run the process.
Instanceid	String	c4678332-ef35-4ad4-8358-***	The ID of the asset.
InstanceName	String	test-***	The name of the asset.
InternetIp	String	1.2.3.1	The public IP address of the asset.
IntranetIp	String	1.2.3.2	The private IP address of the asset.
Md5	String	N/A	The MD5 value of the file.
Name	String	8888	The name of the process.
Path	String	/root/Oracle/Middle ware/***/8888	The path of the process.
Pid	String	12826	The ID of the process.
Pname	String	start***.s	The parent name of the process.
StartTime	String	2019-08-07 10:09:05	The time when the process started.
User	String	root	The user who runs the process.
Uuid	String	c4678332-ef35-4ad4-8358-6***	The ID of the asset related to the process.
RequestId	String	64388374-A309-4191-8606-3346CCA364B0	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePropertyProcDetail
&<Common request parameters>
```

Sample success responses

XML **format**

```
<DescribePropertyProcDetail>
  <RequestId>64388374-A309-4191-8606-3346CCA364B0</RequestId>
  <PageInfo>
    <Count>2</Count>
    <TotalCount>8184</TotalCount>
    <PageSize>2</PageSize>
    <CurrentPage>1</CurrentPage>
  </PageInfo>
  <Property>
    <User>N/A</User>
    <Uuid>90d4cc6a-806f-***</Uuid>
    <Md5>N/A</Md5>
    <CreateTimestamp>1557889713000</CreateTimestamp>
    <InstanceId>i-bp1***</InstanceId>
    <InternetIp></InternetIp>
    <Path>N/A</Path>
    <Name>N/A</Name>
    <IntranetIp>1.2.3.4</IntranetIp>
    <Create>2019-05-15T11:08Z</Create>
    <Pname>N/A</Pname>
    <EuidName>N/A</EuidName>
    <StartTime>N/A</StartTime>
    <Pid>0</Pid>
    <InstanceName>test_***</InstanceName>
    <Cmdline>N/A</Cmdline>
  </Property>
  <Property>
    <User>N/A</User>
    <Uuid>90d4cc6a-806f-4***</Uuid>
    <Md5>N/A</Md5>
    <CreateTimestamp>1557889713000</CreateTimestamp>
    <InstanceId>i-b***</InstanceId>
    <InternetIp></InternetIp>
    <Path>N/A</Path>
    <Name>N/A</Name>
    <IntranetIp>1.2.3.5</IntranetIp>
    <Create>2019-05-15T11:08Z</Create>
    <Pname>N/A</Pname>
    <EuidName>N/A</EuidName>
    <StartTime>N/A</StartTime>
    <Pid>4</Pid>
    <InstanceName>tsy_***</InstanceName>
    <Cmdline>N/A</Cmdline>
  </Property>
</DescribePropertyProcDetail>
```

JSON **format**

```
{
  "RequestId": "64388374-A309-4191-8606-3346CCA364B0",
  "PageInfo": {
    "Count": 2,
    "TotalCount": 8184,
    "PageSize": 2,
    "CurrentPage": 1
  },
  "Propertyys": [
    {
      "User": "N/A",
      "Uuid": "90d4cc6a-806f-***",
      "Md5": "N/A",
      "CreateTimestamp": 1557889713000,
      "InstanceId": "i-bp1***",
      "InternetIp": "",
      "Path": "N/A",
      "Name": "N/A",
      "IntranetIp": "1.2.3.4",
      "Create": "2019-05-15T11:08Z",
      "Pname": "N/A",
      "StartTime": "N/A",
      "EuidName": "N/A",
      "Pid": "0",
      "Cmdline": "N/A",
      "InstanceName": "test_***"
    },
    {
      "User": "N/A",
      "Uuid": "90d4cc6a-806f-4***",
      "Md5": "N/A",
      "CreateTimestamp": 1557889713000,
      "InstanceId": "i-b***",
      "InternetIp": "",
      "Path": "N/A",
      "Name": "N/A",
      "IntranetIp": "1.2.3.5",
      "Create": "2019-05-15T11:08Z",
      "Pname": "N/A",
      "StartTime": "N/A",
      "EuidName": "N/A",
      "Pid": "4",
      "Cmdline": "N/A",
      "InstanceName": "tsy_***"
    }
  ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.7.4. DescribePropertyPortItem

Queries information about ports.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePropertyPortItem	The operation that you want to perform. Set the value to DescribePropertyPortItem .
ForceFlush	Boolean	No	true	Specifies whether to force refresh the data that you want to query.
Port	String	No	22	The port number.
CurrentPage	Integer	No	1	The page number of the current page.
PageSize	Integer	No	5	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
RequestId	String	7E0618A9-D5EF-4220-9471-C42B5E92719F	The ID of the request.
PropertyItems	Array		Details of the port.
Port	String	22	The number of the listener port.
Proto	String	tcp	The network protocol of the port.
Count	Integer	495	The number of servers that use the port.
PageInfo	Struct		The page information.

Parameter	Type	Example	Description
Count	Integer	5	The number of entries returned on the current page.
PageSize	Integer	5	The number of entries returned per page.
TotalCount	Integer	163	The total number of entries.
CurrentPage	Integer	1	The page number of the current page.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePropertyPortItem  
&<Common request parameters>
```

Sample success responses

`XML` format

```
<DescribePropertyPortItemResponse>
  <RequestId>7E0618A9-D5EF-4220-9471-C42B5E92719F</RequestId>
  <PropertyItems>
    <Port>22</Port>
    <Proto>tcp</Proto>
    <Count>495</Count>
  </PropertyItems>
  <PropertyItems>
    <Port>111</Port>
    <Proto>tcp</Proto>
    <Count>43</Count>
  </PropertyItems>
  <PropertyItems>
    <Port>6000</Port>
    <Proto>tcp</Proto>
    <Count>2</Count>
  </PropertyItems>
  <PropertyItems>
    <Port>53</Port>
    <Proto>tcp</Proto>
    <Count>1</Count>
  </PropertyItems>
  <PropertyItems>
    <Port>80</Port>
    <Proto>tcp</Proto>
    <Count>38</Count>
  </PropertyItems>
  <PageInfo>
    <Count>5</Count>
    <PageSize>5</PageSize>
    <TotalCount>163</TotalCount>
    <CurrentPage>1</CurrentPage>
  </PageInfo>
</DescribePropertyPortItemResponse>
```

JSON **format**

```
{
  "requestId": "7E0618A9-D5EF-4220-9471-C42B5E92719F",
  "PropertyItems": [
    {
      "Port": "22",
      "Proto": "tcp",
      "Count": 495
    },
    {
      "Port": "111",
      "Proto": "tcp",
      "Count": 43
    },
    {
      "Port": "6000",
      "Proto": "tcp",
      "Count": 2
    },
    {
      "Port": "53",
      "Proto": "tcp",
      "Count": 1
    },
    {
      "Port": "80",
      "Proto": "tcp",
      "Count": 38
    }
  ],
  "PageInfo": {
    "Count": 5,
    "PageSize": 5,
    "TotalCount": 163,
    "CurrentPage": 1
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.7.5. DescribePropertyProcItem

Queries information about all processes.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePropertyProcItem	The operation that you want to perform. Set the value to DescribePropertyProcItem.
CurrentPage	Integer	No	1	The page number of the current page.
ForceFlush	Boolean	No	true	Specifies whether to force refresh the data that you want to query.
Name	String	No	test	The name of the process.
PageSize	Integer	No	10	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
PageInfo			The page information.
Count	Integer	5	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	5	The number of entries returned per page.
TotalCount	Integer	372	The total number of entries.
PropertyItems	Array		The process information.
Count	Integer	8888	The number of servers on which the process runs.
Name	String	.ss	The name of the process.
RequestId	String	BD8AD4C6-A169-4FA3-BA1F-ED40ED52973B	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePropertyProcItem
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribePropertyProcItem>
  <PropertyItems>
    <Name>(sd-**)</Name>
    <Count>7</Count>
  </PropertyItems>
  <PropertyItems>
    <Name>6Cm***</Name>
    <Count>1</Count>
  </PropertyItems>
  <RequestId>BD8AD4C6-A169-4FA3-BA1F-ED40ED52973B</RequestId>
  <PageInfo>
    <Count>2</Count>
    <TotalCount>395</TotalCount>
    <PageSize>2</PageSize>
    <CurrentPage>1</CurrentPage>
  </PageInfo>
</DescribePropertyProcItem>
```

JSON format

```
{
  "RequestId": "BD8AD4C6-A169-4FA3-BA1F-ED40ED52973B",
  "PropertyItems": [
    {
      "Name": "(sd-**)",
      "Count": 7
    },
    {
      "Name": "6Cm***",
      "Count": 1
    }
  ],
  "PageInfo": {
    "Count": 2,
    "TotalCount": 395,
    "PageSize": 2,
    "CurrentPage": 1
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.7.6. DescribePropertySoftwareDetail

Queries the details of a software asset.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePropertySoftwareDetail	The operation that you want to perform. Set the value to DescribePropertySoftwareDetail.
CurrentPage	Integer	No	1	The page number of the current page.
Name	String	No	tes***	The name of the software.
PageSize	Integer	No	5	The number of entries to return on each page.
Path	String	No	/etc/test	The directory where the software is installed.
Remark	String	No	1.2.3.4	The name or IP address of the server.
SoftwareVersion	String	No	11	The version of the software.
Uuid	String	No	50d213b4-3a35-427a-b8a5-***	The ID of the software asset.

Response parameters

Parameter	Type	Example	Description
PageInfo			The page information.
Count	Integer	2	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	2	The number of entries returned per page.

Parameter	Type	Example	Description
TotalCount	Integer	23	The total number of returned entries.
Propertys	Array		The details of the software.
Create	Long	2019-06-24	The last time when the data was collected.
CreateTimestamp	Long	1565539587000	The last time when the data was collected. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
InstallTime	String	2017-09-07 10:54:49	The time when the software was installed.
Instanceld	String	i-uf***	The ID of the asset.
InstanceName	String	test	The name of the asset.
InternetIp	String	1.2.3.1	The public IP address of the asset.
IntranetIp	String	1.2.3.2	The private IP address of the asset.
Ip	String	1.2.3.1	The public IP address of the asset.
Name	String	aaa_base	The name of the software.
Path	String	/etc/test	The directory where the software is installed.
Uuid	String	4ef1115b-e423- 4b4b-b930-***	The UUID of the asset.
Version	String	11	The version of the software.
RequestId	String	9C5AE850-7140- 4DE6-B892- 055EB0D9F28A	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePropertySoftwareDetail
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribePropertySoftwareDetail>
  <RequestId>9C5AE850-7140-4DE6-B892-055EB0D9F28A</RequestId>
  <PageInfo>
    <Count>2</Count>
    <TotalCount>35795</TotalCount>
    <PageSize>2</PageSize>
    <CurrentPage>1</CurrentPage>
  </PageInfo>
  <Property>
    <Uuid>04c56617-23fc-***</Uuid>
    <Name>abrt</Name>
    <Ip>1.2.3.1</Ip>
    <CreateTimestamp>1561330240000</CreateTimestamp>
    <IntranetIp>1.2.3.3</IntranetIp>
    <InstanceId>i-bp***</InstanceId>
    <Create>2019-06-24T06:50Z</Create>
    <InternetIp>1.2.3.1</InternetIp>
    <InstallTime>2014-08-14 21:18:50</InstallTime>
    <Version>2.0.8</Version>
    <InstanceName>Test***</InstanceName>
    <Path>/etc/abrt</Path>
  </Property>
  <Property>
    <Uuid>c038fd42-3151-4***</Uuid>
    <Name>abrt</Name>
    <Ip>1.2.3.5</Ip>
    <CreateTimestamp>1562283761000</CreateTimestamp>
    <IntranetIp>1.2.3.6</IntranetIp>
    <InstanceId>i-b***</InstanceId>
    <Create>2019-07-05T07:42Z</Create>
    <InternetIp>1.2.3.5</InternetIp>
    <InstallTime>2014-11-21 18:23:32</InstallTime>
    <Version>2.1.11</Version>
    <InstanceName>Test host***</InstanceName>
    <Path>/etc/abrt</Path>
  </Property>
</DescribePropertySoftwareDetail>
```

JSON format


```
{
  "RequestId": "9C5AE850-7140-4DE6-B892-055EB0D9F28A",
  "PageInfo": {
    "Count": 2,
    "TotalCount": 35795,
    "PageSize": 2,
    "CurrentPage": 1
  },
  "Propertys": [
    {
      "Name": "abrt",
      "Uuid": "04c56617-23fc-***",
      "Ip": "1.2.3.1",
      "CreateTimestamp": 1561330240000,
      "Create": "2019-06-24T06:50Z",
      "InstanceId": "i-bp***",
      "IntranetIp": "1.2.3.3",
      "InternetIp": "1.2.3.1",
      "InstallTime": "2014-08-14 21:18:50",
      "Version": "2.0.8",
      "InstanceName": "Test****",
      "Path": "/etc/abrt"
    },
    {
      "Name": "abrt",
      "Uuid": "c038fd42-3151-4***",
      "Ip": "1.2.3.5",
      "CreateTimestamp": 1562283761000,
      "Create": "2019-07-05T07:42Z",
      "InstanceId": "i-b***",
      "IntranetIp": "1.2.3.6",
      "InternetIp": "1.2.3.5",
      "InstallTime": "2014-11-21 18:23:32",
      "Version": "2.1.11",
      "InstanceName": "Test host****",
      "Path": "/etc/abrt"
    }
  ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.7.7. DescribePropertySoftwareItem

Queries information about all software assets.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePropertySoftwareItem	The operation that you want to perform. Set the value to DescribePropertySoftwareItem .
ForceFlush	Boolean	No	true	Specifies whether to force refresh the data that you want to query.
Name	String	No	test	The name of the software.
CurrentPage	Integer	No	1	The page number of the current page.
PageSize	Integer	No	10	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
RequestId	String	3A85CFCF-05C8-451A-9E41-C0D5E96BA407	The ID of the request.
PropertyItems	Array		The returned software assets.
Name	String	aaa_base	The name of the returned software asset.
Count	Integer	23	The number of servers on which the software is installed.
PageInfo	Struct		The page information.
Count	Integer	2	The number of entries returned on the current page.
PageSize	Integer	2	The number of entries returned per page.
TotalCount	Integer	5037	The total number of returned entries.

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the current page.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePropertySoftwareItem
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribePropertySoftwareItemResponse>
  <PageInfo>
    <Count>2</Count>
    <PageSize>2</PageSize>
    <TotalCount>5037</TotalCount>
    <CurrentPage>1</CurrentPage>
  </PageInfo>
  <PropertyItems>
    <Name>ally-profile-manager-indicator</Name>
    <Count>1</Count>
  </PropertyItems>
  <PropertyItems>
    <Name>aaa_base</Name>
    <Count>23</Count>
  </PropertyItems>
  <requestId>3A85CFCF-05C8-451A-9E41-C0D5E96BA407</requestId>
</DescribePropertySoftwareItemResponse>
```

JSON format

```
{
  "PageInfo": {
    "Count": 2,
    "PageSize": 2,
    "TotalCount": 5037,
    "CurrentPage": 1
  },
  "PropertyItems": [
    {
      "Name": "ally-profile-manager-indicator",
      "Count": 1
    },
    {
      "Name": "aaa_base",
      "Count": 23
    }
  ],
  "requestId": "3A85CFCF-05C8-451A-9E41-C0D5E96BA407"
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.7.8. DescribePropertyUserDetail

Queries the details of an account in the account list.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePropertyUserDetail	The operation that you want to perform. Set the value to DescribePropertyUserDetail .
Remark	String	No	0.0.0.0	The name or IP address of the server.
User	String	No	test	The name of the account that you want to query.
IsRoot	String	No	0	Specifies whether the account has root permissions. Valid values: 0: The account does not have root permissions. 1: The account has root permissions.

Parameter	Type	Required	Example	Description
Uuid	String	No	50d213b4-3a35-427a-b8a5-04b0c7e1f4d2	The UUID of the asset.
CurrentPage	Integer	No	1	The number of the page to return.
PageSize	Integer	No	2	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
RequestId	String	FAA793EF-5B14-4CDD-B3E0-B14D4342C422	The ID of the request.
Propertys	Array		The returned account details.
LastLoginTime	String	xxxx	The time of the last logon.
IsRoot	String	0	Indicates whether the account has root permissions. • 0: The account does not have root permissions. • 1: The account has root permissions.
InstanceName	String	null	The name of the asset.
AccountsExpirationDate	String	never	The expiration date of the account.
PasswordExpirationDate	String	never	The expiration date of the account password.
Ip	String	null	The IP address of the asset.
Create	String	1565644643000	The timestamp when the last asset fingerprint was collected.

Parameter	Type	Example	Description
CreateTimestamp	Long	1565644643000	The timestamp generated for the asset fingerprint.
User	String	adm	The name of the account.
Uuid	String	02c4a5dc-c2d2-483a-9015-f972b44d2cd9	The UUID of the asset.
LastLoginIp	String	N/A	The source IP address of the last logon.
InstanceId	String	02c4a5dc-c2d2-483a-9015-f972b44d2cd9	The ID of the asset.
IntranetIp	String	0.0.0.0	The private IP address of the asset.
InternetIp	String	0.0.0.0	The public IP address of the asset.
Status	String	0	The logon status of the account. Valid values: • 0: The account cannot log on. • 1: The account can log on.
GroupNames	List	adm	The name of the user group.
PageInfo	Struct		The page information.
Count	Integer	2	The number of entries returned on the current page.
PageSize	Integer	2	The number of entries returned per page.
TotalCount	Integer	384	The total number of returned entries.
CurrentPage	Integer	1	The page number of the returned page.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePropertyUserDetail
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribePropertyUserDetailResponse>
  <requestId>FAA793EF-5B14-4CDD-B3E0-B14D4342C422</requestId>
  <PageInfo>
    <Count>2</Count>
    <PageSize>2</PageSize>
    <TotalCount>384</TotalCount>
    <CurrentPage>1</CurrentPage>
  </PageInfo>
  <Property>
    <LastLoginTime>N/A</LastLoginTime>
    <GroupName>adm</GroupName>
    <IsRoot>0</IsRoot>
    <InstanceName></InstanceName>
    <AccountsExpirationDate>never</AccountsExpirationDate>
    <PasswordExpirationDate>never</PasswordExpirationDate>
    <Ip></Ip>
    <Create>1565644643000</Create>
    <Status>0</Status>
    <User>adm</User>
    <Uid>00ea0155-548e-4f32-bb53-3a000110b30d</Uid>
    <LastLoginIp>N/A</LastLoginIp>
  </Property>
  <Property>
    <LastLoginTime>N/A</LastLoginTime>
    <GroupName>adm</GroupName>
    <IsRoot>0</IsRoot>
    <InstanceName></InstanceName>
    <AccountsExpirationDate>never</AccountsExpirationDate>
    <PasswordExpirationDate>never</PasswordExpirationDate>
    <Ip></Ip>
    <Create>1565652008000</Create>
    <Status>0</Status>
    <User>adm</User>
    <Uid>02c4a5dc-c2d2-483a-9015-f972b44d2cd9</Uid>
    <LastLoginIp>N/A</LastLoginIp>
  </Property>
</DescribePropertyUserDetailResponse>
```

JSON format

```
{
  "requestId": "FAA793EF-5B14-4CDD-B3E0-B14D4342C422",
  "PageInfo": {
    "Count": 2,
    "PageSize": 2,
    "TotalCount": 384,
    "CurrentPage": 1
  },
  "Propertyys": [
    {
      "LastLoginTime": "N/A",
      "GroupName": [
        "adm"
      ],
      "IsRoot": "0",
      "InstanceName": null,
      "AccountsExpirationDate": "never",
      "PasswordExpirationDate": "never",
      "Ip": null,
      "Create": 1565644643000,
      "Status": 0,
      "User": "adm",
      "Uuid": "00ea0155-548e-4f32-bb53-3a000110b30d",
      "LastLoginIp": "N/A"
    },
    {
      "LastLoginTime": "N/A",
      "GroupName": [
        "adm"
      ],
      "IsRoot": "0",
      "InstanceName": null,
      "AccountsExpirationDate": "never",
      "PasswordExpirationDate": "never",
      "Ip": null,
      "Create": 1565652008000,
      "Status": 0,
      "User": "adm",
      "Uuid": "02c4a5dc-c2d2-483a-9015-f972b44d2cd9",
      "LastLoginIp": "N/A"
    }
  ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.7.9. DescribePropertyUserItem

Queries the account information about an asset.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePropertyUserItem	The operation that you want to perform. Set the value to DescribePropertyUserItem.
CurrentPage	Integer	No	1	The page number of the current page.
ForceFlush	Boolean	No	true	Specifies whether to force refresh the data that you want to query.
PageSize	Integer	No	2	The number of entries to return on each page.
User	String	No	adm	The account information about the asset fingerprint.

Response parameters

Parameter	Type	Example	Description
PageInfo			The page information.
Count	Integer	2	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the current page.
PageSize	Integer	2	The number of entries returned per page.
TotalCount	Integer	114	The total number of returned entries.
PropertyItems	Array		The account information.
Count	Integer	384	The number of servers that belong to the current account.
User	String	adm	The name of the account.

Parameter	Type	Example	Description
RequestId	String	76068BE2-F9C4-4EDD-967B-F503B8CCDD3D	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePropertyUserItem
&<Common request parameters>
```

Sample success responses

XML format

```
<DescribePropertyUserItem>
  <PropertyItems>
    <User>a123456</User>
    <Count>1</Count>
  </PropertyItems>
  <PropertyItems>
    <User>aaaa</User>
    <Count>1</Count>
  </PropertyItems>
  <PropertyItems>
    <User>aaaal</User>
    <Count>1</Count>
  </PropertyItems>
  <RequestId>76068BE2-F9C4-4EDD-967B-F503B8CCDD3D</RequestId>
  <PageInfo>
    <Count>3</Count>
    <TotalCount>340</TotalCount>
    <PageSize>3</PageSize>
    <CurrentPage>1</CurrentPage>
  </PageInfo>
</DescribePropertyUserItem>
```

JSON format

```
{
  "RequestId": "76068BE2-F9C4-4EDD-967B-F503B8CCDD3D",
  "PropertyItems": [
    {
      "User": "a123456",
      "Count": 1
    },
    {
      "User": "aaaa",
      "Count": 1
    },
    {
      "User": "aaaa1",
      "Count": 1
    }
  ],
  "PageInfo": {
    "Count": 3,
    "TotalCount": 340,
    "PageSize": 3,
    "CurrentPage": 1
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

7.8. Asset exposure

7.8.1. DescribeExposedInstanceList

Queries the assets that are exposed.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeExposedInstanceList	The operation that you want to perform. Set the value to DescribeExposedInstanceList .
PageSize	Integer	No	20	The number of entries to return on each page.
CurrentPage	Integer	No	1	The number of the page to return.
GroupId	Long	No	9469268	The ID of the server group.

Parameter	Type	Required	Example	Description
VulStatus	Boolean	No	true	Specifies whether the server has vulnerabilities. Valid values: • true: yes • false: no
HealthStatus	Boolean	No	true	Specifies whether baseline risks exist in the server.
ExposureComponent	String	No	openssl	The server component that is exposed on the Internet.
ExposurePort	String	No	22	The port that is exposed on the Internet.
ExposureIp	String	No	116.12.XX.XX	The public IP address of the server.
InstanceId	String	No	i-bp1g6wxdwps7s9dz****	The ID of the server.
InstanceName	String	No	abc_centos7.2_005	The name of the server.

Response parameters

Parameter	Type	Example	Description
ExposedInstances	Array of ExposedInstance		An array that consists of the details of the exposed asset.
AsapVulCount	Integer	0	The number of high-risk vulnerabilities that are exposed on the Internet and can be exploited by attackers.
ExploitHealthCount	Integer	0	The number of baseline risks that can be exploited.
ExposureComponent	String	openssl,openssh	The server component that is exposed on the Internet.

Parameter	Type	Example	Description
ExposureIp	String	116.12.XX.XX	The public IP address that is exposed on the Internet.
ExposurePort	String	22	The port that is exposed on the Internet.
ExposureType	String	INTERNET_IP	The resource from which the asset is exposed. Valid values: • INTERNET_IP: the IP address of the Elastic Compute Service (ECS) instance • SLB: the public IP address of the Server Load Balancer (SLB) instance • EIP: the elastic IP address (EIP) • DNAT: the NAT gateway that connects to the Internet by using the DNAT feature
ExposureTypeId	String	i-ew11313a****	The ID of the instance from which the asset is exposed. The value of this parameter varies based on the value of the ExposureType parameter. • If the value of the ExposureType parameter is INTERNET_IP, the value of this parameter is an empty string. • If the value of the ExposureType parameter is SLB, the value of this parameter is the ID of the Internet-facing SLB instance. • If the value of the ExposureType parameter is EIP, the value of this parameter is the ID of the EIP. • If the value of the ExposureType parameter is DNAT, the value of this parameter is the ID of the NAT gateway.
GroupId	Long	9469268	The ID of the server group.
GroupName	String	Ungrouped	The name of the server group.
InstanceId	String	i-bp1g6wxdwps7s9dz****	The ID of the server.
InstanceName	String	abc_centos7.2_005	The name of the server.

Parameter	Type	Example	Description
InternetIp	String	116.12.XX.XX	The public IP address of the server.
IntranetIp	String	192.168.XX.XX	The private IP address of the server.
LaterVulCount	Integer	0	The number of medium-risk vulnerabilities that are exposed on the Internet and can be exploited by attackers.
NntfVulCount	Integer	0	The number of low-risk vulnerabilities that are exposed on the Internet and can be exploited by attackers.
RegionId	String	cn-hangzhou	The ID of the region where the server resides.
TotalVulCount	Integer	0	The total number of vulnerabilities that are exposed on the Internet and can be exploited by attackers.
Uuid	String	dd803d9e-a337-4add-9c5b-7d503e08****	The UUID of the server.
PageInfo	Struct		The pagination information.
Count	Integer	2	The number of entries returned on the current page.
CurrentPage	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
TotalCount	Integer	2	The total number of entries returned.
RequestId	String	598A4A61-ABA7-456B-8725-7378258276D9	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeExposedInstanceList
&<Common request parameters>
```

Sample success responses

XML format

```
<PageInfo>
  <TotalCount>2</TotalCount>
  <PageSize>20</PageSize>
  <CurrentPage>1</CurrentPage>
  <Count>2</Count>
</PageInfo>
<RequestId>598A4A61-ABA7-456B-8725-7378258276D9</RequestId>
<ExposedInstances>
  <GroupName>Ungrouped</GroupName>
  <TotalVulCount>0</TotalVulCount>
  <ExposureType>INTERNET_IP</ExposureType>
  <InstanceId>i-bp1g6wxdwps7s9dz****</InstanceId>
  <ExposureComponent>openssl,openssh</ExposureComponent>
  <ExposurePort>22</ExposurePort>
  <NntfVulCount>0</NntfVulCount>
  <AsapVulCount>0</AsapVulCount>
  <ExploitHealthCount>0</ExploitHealthCount>
  <IntranetIp>192.168.XX.XX </IntranetIp>
  <GroupId>9469268</GroupId>
  <InstanceName>abc_centos7.2_005 </InstanceName>
  <Uuid>dd803d9e-a337-4add-9c5b-7d503e08****</Uuid>
  <ExposureIp>116.12.XX.XX </ExposureIp>
  <ExposureTypeId>i-ew11313a****</ExposureTypeId>
  <InternetIp>116.12.XX.XX</InternetIp>
  <LaterVulCount>0</LaterVulCount>
  <RegionId>cn-hangzhou</RegionId>
</ExposedInstances>
```

JSON format

```
{ "PageInfo": { "TotalCount": "2", "PageSize": "20", "CurrentPage": "1", "Count": "2" }, "RequestId": "598A4A61-ABA7-456B-8725-7378258276D9", "ExposedInstances": [ { "GroupName": "Ungrouped", "TotalVulCount": "0", "ExposureType": "INTERNET_IP", "InstanceId": "i-bp1g6wxdwps7s9dz****", "ExposureComponent": "openssl,openssh", "ExposurePort": "22", "NntfVulCount": "0", "AsapVulCount": "0", "ExploitHealthCount": "0", "IntranetIp": "192.168.XX.XX\t", "GroupId": "9469268", "InstanceName": "abc_centos7.2_005\t", "Uuid": "dd803d9e-a337-4add-9c5b-7d503e08****", "ExposureIp": "116.12.XX.XX\t", "ExposureTypeId": "i-ew11313a****", "InternetIp": "116.12.XX.XX", "LaterVulCount": "0", "RegionId": "cn-hangzhou" } ] }
```

8. Network Traffic Monitoring System

8.1. IP address blocking

8.1.1. AddToBlackList

Adds the source IP address of an attack to the blacklist.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AddToBlackList	The operation that you want to perform. Set the value to AddToBlackList .
SrcIp	String	Yes	183.100.XX.XX	The source IP address of an attack.
DstIp	String	No	120.223.XX.XX	The destination IP address of an attack.
DstPort	String	Yes	8080	The start of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.
DstPortEnd	String	No	8081	The end of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.
LiveTime	String	Yes	5	The validity period of the blacklist. Unit: minutes. Valid values: 1 to 10080. If you leave this parameter unspecified, the default value 5 is used.

Parameter	Type	Required	Example	Description
Filter	String	No	inbound	The direction of the attack traffic that can be blocked by the blacklist. This parameter is available only for the blacklist. Valid values: • inbound: blocks traffic destined for data centers in which Apsara Stack is deployed. This is the default value. • outbound: blocks traffic sent from data centers in which Apsara Stack is deployed.
AliUid	String	No	123456****	The Apsara Stack tenant account.
IpType	String	No	4	The type of the IP addresses. Valid values: • 4: IPv4 addresses. This is the default value. • 6: IPv6 addresses.
Note	String	No	Add the IP address to the blacklist.	The additional description.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see [Common parameters](#).

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
code	String	200	The status code returned for the request.
success	String	true	Indicates whether the request is successful. Valid values: • true: The request is successful. • false: The request failed.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=AddToBlackList
&SrcIp=183.100.XX.XX
&DstIp=120.223.XX.XX
&DstPort=8080
&LiveTime=5
&<Common request parameters>
```

Sample success responses

XML format

```
<code>200</code>
<success>true</requestId>
```

JSON format

```
{
  "code": 200,
  "success": "true"
}
```

Error codes

For a list of error codes, see [Error codes](#).

8.1.2. AddToWhiteList

Adds the source IP address of an attack to the whitelist.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AddToWhiteList	The operation that you want to perform. Set the value to AddToWhiteList .
SrcIp	String	No	183.100.XX.XX	The source IP address of an attack.
DstIp	String	Yes	120.223.XX.XX	The destination IP address of an attack.
DstPort	String	No	8080	The start of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.

Parameter	Type	Required	Example	Description
DstPortEnd	String	No	8081	The end of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.
LiveTime	String	No	5	The validity period of the whitelist. Unit: minutes. Valid values: 1 to 10080. If you leave this parameter unspecified, the default value 5 is used.
AliUid	String	Yes	123456****	The Apsara Stack tenant account.
IpType	String	Yes	4	The type of the IP addresses. Valid values: • 4: IPv4 addresses. This is the default value. • 6: IPv6 addresses.
Note	String	Yes	Add the IP address to the whitelist.	The additional description.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see [Common parameters](#).

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
code	String	200	The status code returned for the request.
success	String	true	Indicates whether the request is successful. Valid values: • true: The request is successful. • false: The request failed.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=AddToWhiteList
&SrcIp=183.100.XX.XX
&DstIp=120.223.XX.XX
&AliUid=123456****
&IpType=4
&Note=Add the IP address to the whitelist.
&<Common request parameters>
```

Sample success responses

XML format

```
<code>200</code>
<success>true</requestId>
```

JSON format

```
{
  "code": 200,
  "success": "true"
}
```

Error codes

For a list of error codes, see [Error codes](#).

8.1.3. DelFromBlackList

Removes the source IP address of an attack from the blacklist.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DelFromBlackList	The operation that you want to perform. Set the value to DelFromBlackList .
SrcIp	String	Yes	183.100.XX.XX	The source IP address of an attack.
DstIp	String	No	120.223.XX.XX	The destination IP address of an attack.
DstPort	String	No	8080	The start of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.

Parameter	Type	Required	Example	Description
DstPortEnd	String	No	8081	The end of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.
LiveTime	String	No	5	The validity period of the blacklist. Unit: minutes. Valid values: 1 to 10080. If you leave this parameter unspecified, the default value 5 is used.
Filter	String	No	outbound	The direction of the attack traffic that can be blocked by the blacklist. This parameter is available only for the blacklist. Valid values: • inbound: blocks traffic destined for data centers in which Apsara Stack is deployed. This is the default value. • outbound: blocks traffic sent from data centers in which Apsara Stack is deployed.
AliUid	String	Yes	123456****	The Apsara Stack tenant account.
IpType	String	No	4	The type of the IP addresses. Valid values: • 4: IPv4 addresses. This is the default value. • 6: IPv6 addresses.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see [Common parameters](#).

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
code	String	200	The status code returned for the request.

Parameter	Type	Example	Description
success	String	true	Indicates whether the request is successful. Valid values: • true: The request is successful. • false: The request failed.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DelFromBlackList
&SrcIp=183.100.XX.XX
&DstIp=120.223.XX.XX
&AliUid=123456****
&<Common request parameters>
```

Sample success responses

XML format

```
<code>200</code>
<success>true</requestId>
```

JSON format

```
{
  "code": 200,
  "success": "true"
}
```

Error codes

For a list of error codes, see [Error codes](#).

8.1.4. DelFromWhiteList

Removes the source IP address of an attack from the whitelist.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DelFromWhiteList	The operation that you want to perform. Set the value to DelFromWhiteList .
SrcIp	String	No	183.100.XX.XX	The source IP address of an attack.

Parameter	Type	Required	Example	Description
DstIp	String	Yes	120.223.XX.XX	The destination IP address of an attack.
DstPort	String	No	8080	The start of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.
DstPortEnd	String	No	8081	The end of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.
LiveTime	String	No	5	The validity period of the whitelist. Unit: minutes. Valid values: 1 to 10080. If you leave this parameter unspecified, the default value 5 is used.
AliUid	String	Yes	123456****	The Apsara Stack tenant account.
IpType	String	No	4	The type of the IP addresses. Valid values: • 4: IPv4 addresses. This is the default value. • 6: IPv6 addresses.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see [Common parameters](#).

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
code	String	200	The status code returned for the request.
success	String	true	Indicates whether the request is successful. Valid values: • true: The request is successful. • false: The request failed.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DelFromWhiteList
&SrcIp=183.100.XX.XX
&DstIp=120.223.XX.XX
&AliUid=123456****
&<Common request parameters>
```

Sample success responses

XML format

```
<code>200</code>
<success>true</requestId>
```

JSON format

```
{
  "code": 200,
  "success": "true"
}
```

Error codes

For a list of error codes, see [Error codes](#).

8.1.5. DescribeBlackList

Queries the details of the blacklist.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeBlackList	The operation that you want to perform. Set the value to DescribeBlackList .
SrcIp	String	No	183.100.XX.XX	The source IP address of an attack.
DstIp	String	No	120.223.XX.XX	The destination IP address of an attack.
DstPort	String	No	8080	The start of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.

Parameter	Type	Required	Example	Description
StartTime	Number	No	1630996231000	The beginning of the time range when the blacklist is valid. Unit: milliseconds.
EndTime	Number	No	1630996411000	The end of the time range when the blacklist expires. Unit: milliseconds.
AliUid	String	Yes	123456****	The Apsara Stack tenant account.
IpType	String	No	4	The type of the IP addresses. Valid values: • 4: IPv4 addresses. This is the default value. • 6: IPv6 addresses.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see [Common parameters](#).

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
code	String	200	The status code returned for the request.
success	String	true	Indicates whether the request is successful. Valid values: • true: The request is successful. • false: The request failed.
data	Object		The returned data.
└ DataList	Array		The details of the entry returned.
└ └ SrcIp	String	183.100.XX.XX	The source IP address of an attack.
└ └ DstIp	String	120.223.XX.XX	The destination IP address of an attack.
└ └ DstPort	Number	8080	The start of the destination port range of an attack.
└ └ DstPortEnd	Number	8081	The end of the destination port range of an attack.
└ └ LiveTime	String	5	The validity period of the blacklist. Default value: 5. Unit: minutes.

Parameter	Type	Example	Description
<code>HitTimes</code>	String	10000	The number of attacks.
<code>Filter</code>	String	inbound	The direction of the attack traffic that can be blocked by the blacklist. Valid values: • inbound: blocks traffic destined for data centers in which Apsara Stack is deployed. This is the default value. • outbound: blocks traffic sent from data centers in which Apsara Stack is deployed.
<code>Note</code>	String	Query the details of the blacklist.	The additional description.
<code>StartTime</code>	String	1630996231000	The beginning of the time range when the blacklist is valid. Unit: milliseconds.
<code>EndTime</code>	String	1630996411000	The end of the time range when the blacklist expires. Unit: milliseconds.
<code>IpType</code>	String	4	The type of the IP addresses. Valid values: • 4: IPv4 addresses. This is the default value. • 6: IPv6 addresses.
<code>Count</code>	Number	5	The number of entries returned.
<code>Module</code>	String	dispatch_rule	The name of the process for this request. Default value: dispatch_rule .

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeBlackList
&AliUid=123456****
&<Common request parameters>
```

Sample success responses

XML format

```
<code>200</code>
<success>true</success>
<data>
  <DataList>
    <SrcIp>183.100.XX.XX</SrcIp>
    <DstIp>120.223.XX.XX</DstIp>
    <DstPort>8080</DstPort>
    <DstPortEnd>8081</DstPortEnd>
    <LiveTime>5</LiveTime>
    <HitTimes>10000</HitTimes>
    <Filter></Filter>
    <Note></Note>
    <StartTime>1630996231000</StartTime>
    <EndTime>1630996411000</EndTime>
    <IpType>4</IpType>
  </DataList>
  <Count>1</Count>
  <Module>dispatch_rule</Module>
</data>
```

JSON format

```
{
  "code": "200",
  "success": "true",
  "data": {
    "DataList": [
      {
        "SrcIp": "183.100.XX.XX",
        "DstIp": "120.223.XX.XX",
        "DstPort": 8080,
        "DstPortEnd": 8081,
        "LiveTime": "5",
        "HitTimes": "10000",
        "Filter": "",
        "Note": "",
        "StartTime": "1630996231000",
        "EndTime": "1630996411000",
        "IpType": "4"
      }
    ],
    "Count": 1,
    "Module": "dispatch_rule"
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

8.1.6. DescribeWhiteList

Queries the details of the whitelist.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeWhiteList	The operation that you want to perform. Set the value to DescribeWhiteList .
SrcIp	String	No	183.100.XX.XX	The source IP address of an attack.
DstIp	String	No	120.223.XX.XX	The destination IP address of an attack.
DstPort	String	No	8080	The start of the destination port range of an attack. Valid values: 0 to 65535. If you set this parameter to 0, all ports are specified.
StartTime	Number	No	1630996231000	The beginning of the time range when the whitelist is valid. Unit: milliseconds.
EndTime	Number	No	1630996411000	The end of the time range when the whitelist is valid. Unit: milliseconds.
AliUid	String	Yes	123456****	The Apsara Stack tenant account.
IpType	String	No	4	The type of the IP addresses. Valid values: • 4: IPv4 addresses. This is the default value. • 6: IPv6 addresses.

All Alibaba Cloud API operations must include common request parameters. For more information about common request parameters, see [Common parameters](#).

For more information about sample requests, see the "Examples" section of this topic.

Response parameters

Parameter	Type	Example	Description
code	String	200	The status code returned for the request.

Parameter	Type	Example	Description
success	String	true	Indicates whether the request is successful. Valid values: true: The request is successful. false: The request failed.
data	Object		The returned data.
└ DataList	Array		The details of the entry returned.
└ └ SrcIp	String	183.100.XX.XX	The source IP address of an attack.
└ └ DstIp	String	120.223.XX.XX	The destination IP address of an attack.
└ └ DstPort	Number	8080	The start of the destination port range of an attack.
└ └ DstPortEnd	Number	8081	The end of the destination port range of an attack.
└ └ LiveTime	String	5	The validity of the whitelist. Default value: 5. Unit: minutes.
└ └ HitTimes	String	10000	The number of attacks.
└ └ Filter	String	inbound	The direction of the traffic that is allowed by the whitelist. Valid values: inbound: allows traffic destined for data centers in which Apsara Stack is deployed. This is the default value. outbound: allows traffic sent from data centers in which Apsara Stack is deployed.
└ └ Note	String	Query the details of the whitelist.	The additional description.
└ └ StartTime	String	1630996231000	The beginning of the time range when the whitelist is valid. Unit: milliseconds.
└ └ EndTime	String	1630996411000	The end of the time range when the whitelist is valid. Unit: milliseconds.
└ └ IpType	String	4	The type of the IP addresses. Valid values: 4: IPv4 addresses 6: IPv6 addresses
└ Count	Number	5	The number of entries returned.

Parameter	Type	Example	Description
L-Module	String	dispatch_rule	The name of the process for this request. Default value: dispatch_rule .

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeWhiteList
&AliUid=123456****
&<Common request parameters>
```

Sample success responses

XML format

```
<code>200</code>
<success>true</success>
<data>
  <DataList>
    <SrcIp>183.100.XX.XX</SrcIp>
    <DstIp>120.223.XX.XX</DstIp>
    <DstPort>8080</DstPort>
    <DstPortEnd>8081</DstPortEnd>
    <LiveTime>5</LiveTime>
    <HitTimes>10000</HitTimes>
    <Filter></Filter>
    <Note></Note>
    <StartTime>1630996231000</StartTime>
    <EndTime>1630996411000</EndTime>
    <IpType>4</IpType>
  </DataList>
  <Count>1</Count>
  <Module>dispatch_rule</Module>
</data>
```

JSON format

```
{
  "code": "200",
  "success": "true",
  "data": {
    "DataList": [
      {
        "SrcIp": "183.100.XX.XX",
        "DstIp": "120.223.XX.XX",
        "DstPort": 8080,
        "DstPortEnd": 8081,
        "LiveTime": "5",
        "HitTimes": "10000",
        "Filter": "",
        "Note": "",
        "StartTime": "1630996231000",
        "EndTime": "1630996411000",
        "IpType": "4"
      }
    ],
    "Count": 1,
    "Module": "dispatch_rule"
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

8.2. Application-layer rules

8.2.1. DescribeL7Rule

Queries the details of the application-layer rules that are used to block traffic.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeL7Rule	The operation that you want to perform. Set the value to DescribeL7Rule .
Lang	String	No	zh	The language of the content within the request and response. zh: Chinese en: English

Parameter	Type	Required	Example	Description
RuleStatus	String	No	online	The status of the rules. • %: all states • init: initializing • online: in effect • offline: expired
AliUid	Long	No	1234567890	The Apsara Stack tenant account.
CurrentPage	Integer	No	1	The number of the page to return.
PageSize	Integer	No	10	The number of entries to return on each page.
ActionType	String	No	drop	The action of the rules. • pass: allows traffic. • alert: only records traffic in logs. • drop: blocks traffic.
Direction	String	No	in	The direction of traffic. • in: inbound traffic • out: outbound traffic
Query	String	No	%	The query string. • %: a wildcard character in SQL statements. You can use a percent sign (%) to match all characters in rules that are used to monitor HTTP requests.

Parameter	Type	Required	Example	Description
QueryTimeType	Integer	No	1	The time condition of the rules to query. • 1: queries rules that are created before the specified time condition • 2: queries rules that are created at the specified time condition • 3: queries rules that are created after the specified time condition • 4: queries rules that are created within the specified time condition • 5: queries rules that expire before the specified time condition • 6: queries rules that expire at the specified time condition • 7: queries rules that expire after the specified time condition • 8: queries rules that expire within the specified time condition
QueryStartTime	Long	No	1934325423	The beginning of the time range to query. Unit: seconds.
QueryEndTime	Long	No	1934325428	The end of the time range to query. Unit: seconds.
WhiteRuleID	Long	No	13285	The ID of the whitelist or the rule that allows traffic.
BlackRuleID	Long	No	13285	The ID of the blacklist or the rule that blocks traffic.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
DataList	Array of Data		The list of the returned data.

Parameter	Type	Example	Description
ActionType	String	drop	The action of the rules. pass : indicates that the rules are used to allow traffic. alert : indicates that the rules are used to only record traffic in logs. drop : indicates that the rules are used to block traffic.
AliUid	Long	1234567890	The Apsara Stack tenant account.
CreateTime	String	2018-05-14 14:50:54	The time when the rule was created. The time follows the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format.
Direction	String	in	The direction of traffic. • in: inbound traffic • out: outbound traffic
EndTime	Long	1642747110	The end of the time range that is queried. The value is a UNIX timestamp. Unit: seconds.
ExpiredTime	String	2018-05-14 14:50:54	The expected expiration time of the rule. This parameter takes effect only for rules in the online state.
HitTimes	Integer	10	The number of times the rule is matched.
MatchesDesc	String	["The URL contains a.com", "The host address contains 1.1.1.1"]	The matching item in the rule that is used to monitor HTTP requests.
MatchesDescEn	String	["The URL contains a.com", "The host address contains 1.1.1.1"]	The matching item in the rule that is used to monitor HTTP requests. This parameter is intended for users outside the Chinese mainland.
ModifiedTime	String	2018-05-14 14:50:54	The time when the rule is updated. The time follows the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format.
Modifier	String	administrator	The user who modified the rule for the last time.

Parameter	Type	Example	Description
OfflineTime	String	2018-05-14 14:50:54	The time when the rule expires. The time follows the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format.
OnlineTime	String	2018-05-14 14:50:54	The time when the rule takes effect. This parameter takes effect only for the rule in the online state. The time follows the ISO 8601 standard in the yyyy-MM-ddTHH:mm:ssZ format.
RuleDescription	String	test	The description of the rule.
RuleId	Integer	13285	The ID of the rule.
RuleName	String	bot_scanner_block	The name of the rule.
RuleUuid	String	cfa13285-5330-402e-980c-5075c12c6aa8	The UUID of the rule.
StartTime	Long	1642747110	The beginning of the time range that is queried. The value is a UNIX timestamp. Unit: milliseconds.
SwitchStatus	String	online	The status of the rule. • init: indicates that the rule is being initialized. • online: indicates that the rule is in effect. • offline: indicates that the rule expired.
matches	Array of Matchs		An array that consists of match conditions.
Content	String	8.8.8.8	The value of the HTTP header.
HeaderName	String	x-forward-for	The name of the HTTP header. This value is case-insensitive. Valid values: method , x-forward-for , host , url , cookie , and custom values.

Parameter	Type	Example	Description
MatchType	String	strict	The matching logic. • strict: exact match. • fuzzy: fuzzy match. • notexist: The HTTP header does not exist.
NoCase	Integer	1	Indicates whether the rule is case-sensitive. • 1: case-insensitive • 0: case-sensitive
TcpOptionKind	Integer	28	The decimal value of the TCP Options field.
XPosition	Integer	-1	The position from which the originating IP address is obtained in the HTTP header, such as X-Forwarded-For. The value of this parameter starts from 1. If 2 is returned, 9.9.9.9 is the originating IP address that is obtained from x-forward-for:8.8.8.8,9.9.9.9.7.7.7.7. If -1 or an integer that is smaller than 0 is returned, the originating IP address may be in any position of the HTTP header.
HttpStatusCode	Integer	200	The status code of the request. • 200: The request is successful.
Module	String	dispatch_rule	The module name of the request.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Valid values: • true: The request is successful. • false: The request failed.
TotalCount	Integer	10	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeL7Rule
&<Common request parameters>
```

Sample success responses

XML format

```
<DataList>
  <RuleDescription>test</RuleDescription>
  <MatchesDescEn>[  "The URL contains a.com",  "The host address contains 1.1.1.1" ]</MatchesDescEn>
  <OfflineTime>2018-05-14 14:50:54</OfflineTime>
  <ActionType>drop</ActionType>
  <EndTime>1642747110</EndTime>
  <CreateTime>2018-05-14 14:50:54</CreateTime>
  <RuleId>13285</RuleId>
  <StartTime>1642747110</StartTime>
  <OnlineTime>2018-05-14 14:50:54</OnlineTime>
  <RuleUuid>cfa13285-5330-402e-980c-5075c12c6aa8</RuleUuid>
  <Direction>in</Direction>
  <ModifiedTime>2018-05-14 14:50:54</ModifiedTime>
  <HitTimes>10</HitTimes>
  <ExpiredTime>2018-05-14 14:50:54</ExpiredTime>
  <MatchesDesc>[  "The URL contains a.com",  "The host address contains 1.1.1.1" ]</MatchesDesc>
  <Modifier>administrator</Modifier>
  <SwitchStatus>online</SwitchStatus>
  <RuleName>bot_scanner_block</RuleName>
  <AliUid>1234567890</AliUid>
  <matches>
    <XPosition>-1</XPosition>
    <MatchType>strict</MatchType>
    <HeaderName>x-forward-for</HeaderName>
    <TcpOptionKind>28</TcpOptionKind>
    <Content>8.8.8.8</Content>
    <NoCase>1</NoCase>
  </matches>
</DataList>
<TotalCount>10</TotalCount>
<PageSize>10</PageSize>
<RequestId>CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX</RequestId>
<CurrentPage>1</CurrentPage>
<HttpStatusCode>200</HttpStatusCode>
<Module>dispatch_rule</Module>
<Success>true</Success>
```

JSON format

```
{
  "DataList": {
    "RuleDescription": "test",
    "MatchesDescEn": "[  \\\"The URL contains a.com\\\",  \\\"The host address contains 1.1.1.1\\\" ]",
    "OfflineTime": "2018-05-14 14:50:54",
    "ActionType": "drop",
    "EndTime": 1642747110,
    "CreateTime": "2018-05-14 14:50:54",
    "RuleId": 13285,
    "StartTime": 1642747110,
    "OnlineTime": "2018-05-14 14:50:54",
    "RuleUuid": "cfa13285-5330-402e-980c-5075c12c6aa8",
    "Direction": "in",
    "ModifiedTime": "2018-05-14 14:50:54",
    "HitTimes": 10,
    "ExpiredTime": "2018-05-14 14:50:54",
    "MatchesDesc": "[  \\\"The URL contains a.com\\\",  \\\"The host address contains 1.1.1.1\\\" ]",
    "Modifier": "administrator",
    "SwitchStatus": "online",
    "RuleName": "bot_scanner_block",
    "AliUid": 1234567890,
    "matches": {
      "XPosition": -1,
      "MatchType": "strict",
      "HeaderName": "x-forward-for",
      "TcpOptionKind": 28,
      "Content": "8.8.8.8",
      "NoCase": 1
    }
  },
  "TotalCount": 10,
  "PageSize": 10,
  "RequestId": "CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX",
  "CurrentPage": 1,
  "HttpStatusCode": 200,
  "Module": "dispatch_rule",
  "Success": true
}
```

8.2.2. SwitchL7RuleStatus

Changes the status of application-layer rules.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	SwitchL7RuleStatus	The operation that you want to perform. Set the value to SwitchL7RuleStatus .
Lang	String	No	zh	The language of the content within the request and response. • zh: Chinese • en: English
AliUid	Long	No	1234567890	The Apsara Stack tenant account.
RuleUuidList	String	No	cfa13285-5330-402e-980c-5075c12c6aa8, cfa13285-5330-402e-980c-5075c12c6aa8	The UUIDs of the rules. Separate multiple UUIDs with commas (,).
SwitchStatus	String	No	online	The status of the rules. • online: in effect • offline: expired

Response parameters

Parameter	Type	Example	Description
HttpStatusCode	Integer	200	The status code of the request. • 200: The request is successful.
Module	String	dispatch_rule	The module name of the request.
RequestId	String	CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Valid values: • true: The request is successful. • false: The request failed.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=SwitchL7RuleStatus
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX</RequestId>
<HttpStatusCode>200</HttpStatusCode>
<Module>dispatch_rule</Module>
<Success>true</Success>
```

JSON format

```
{
  "RequestId": "CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX",
  "HttpStatusCode": 200,
  "Module": "dispatch_rule",
  "Success": true
}
```

8.2.3. AddL7Rule

Creates an HTTP rule.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	AddL7Rule	The operation that you want to perform. Set the value to AddL7Rule .
Lang	String	No	zh	The language of the content within the request and response. zh: Chinese en: English
AliUid	Long	No	13973495843021	The Apsara Stack tenant account.
RuleName	String	No	bot_scanner_block	The name of the rule.
RuleDescription	String	No	test	The description of the rule.

Parameter	Type	Required	Example	Description
Direction	String	No	in	The direction of traffic. • in: inbound traffic • out: outbound traffic
ActionType	String	No	drop	The action of the rule. • pass: allows traffic. • alert: only records traffic in logs. • drop: blocks traffic.
SwitchStatus	String	No	online	The status of the rule. • init: The rule is being initialized. • online: The rule is in effect. • offline: The rule expired.
StartTime	Long	No	1642664320	The time when the rule takes effect. The value is a UNIX timestamp. Unit: milliseconds.
EndTime	Long	No	1642664320	The time when the rule expires. If you set this parameter to 9999999999 , the rule never expires. The value is a UNIX timestamp. Unit: milliseconds.
Matches	String	No	None	The content of the rule.

Response parameters

Parameter	Type	Example	Description
HttpStatusCode	Integer	200	The status code of the request. • 200: The request is successful.
Module	String	dispatch_rule	The module name of the request.
RequestId	String	CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX	The ID of the request.

Parameter	Type	Example	Description
Success	Boolean	true	Indicates whether the request is successful. Valid values: true: The request is successful. false: The request failed.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=AddL7Rule
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX</RequestId>
<HttpStatusCode>200</HttpStatusCode>
<Module>dispatch_rule</Module>
<Success>true</Success>
```

JSON format

```
{
  "RequestId": "CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX",
  "HttpStatusCode": 200,
  "Module": "dispatch_rule",
  "Success": true
}
```

8.2.4. DelL7Rule

Deletes application-layer rules.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DelL7Rule	The operation that you want to perform. Set the value to DelL7Rule .
Lang	String	No	zh	The language of the content within the request and response. zh: Chinese en: English

Parameter	Type	Required	Example	Description
AliUid	Long	No	13973495843021	The Apsara Stack tenant account.
RuleUuidList	String	No	cfa13285-5330-402e-980c-5075c12c6aa8	The UUIDs of the rules. Separate multiple UUIDs with commas (,).

Response parameters

Parameter	Type	Example	Description
HttpStatusCode	Integer	200	The status code of the request. 200: The request is successful.
Module	String	dispatch_rule	The module name of the request.
RequestId	String	CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX	The ID of the request.
Success	Boolean	true	Indicates whether the request is successful. Valid values: true: The request is successful. false: The request failed.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=Dell7Rule
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX</RequestId>
<HttpStatusCode>200</HttpStatusCode>
<Module>dispatch_rule</Module>
<Success>true</Success>
```

JSON format

```
{
  "RequestId": "CFE6DXXX-XXX-XXXX-XXXX-99XX99XX99XX",
  "HttpStatusCode": 200,
  "Module": "dispatch_rule",
  "Success": true
}
```

9. Web Application Firewall

9.1. Website protection

9.1.1. DescribeWebsite

Queries the information about the websites that are protected by WAF.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeWebsite	The operation that you want to perform. Set the value to DescribeWebsite.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	No	1	The ID of the website.
PageSize	Integer	No	20	The number of entries to return on each page. Default value: 10.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.
IsVpcWebsite	Boolean	No	true	Specifies whether the websites to query are in a virtual private cloud (VPC). Default value: false . Valid values: • true • false
WebsiteNameFilter	RepeatList	No	["website-1", "website-2"]	The name of the website to query. You can enter multiple names.
ServerNameFilter	RepeatList	No	["www.taobao.com", "www.aliyun.com"]	The domain name of the website to query. You can enter multiple domain names.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	<pre>{ "items": [{"id": 1, "ip": ["0.0.XX.XX"], "session_method": {"type": "off"}, "policy_rules": [], "health_check_status": "", "backend_config": {"type": "proxy", "load_balance_policy": "Round Robin", "servers": [{"protocol": "http", "attr": "slb", "host": "192.168.XX.XX", "port": 80, "weight": 1}], "x_forwarded_for_action": "append", "header_config": [], "health_check_config": {"is_enabled": false, "check_http_expect_alive": ["http_2xx", "http_3xx"], "check_type": "http", "interval": 30000, "fall": 5, "rise": 2, "timeout": 1000, "port": null, "host": "", "method": "GET", "path": "/"}, "proxy_ssl_protocols": [], "proxy_ssl_ciphers": ""}, "vpc": "vpc- tx9isq1jrry8k3h9q****", "vpc_name": "tongquesingle****", "vip": ["42.36.XX.XX"], "ports": [{"port": 80, "ssl": false, "http2": false}], "is_vpc_website": false, "operation_mode": "Software Reverse Proxy", "interface": "virtual", "server_names": ["www.taobao.com"], "ssl_protocols": [], "ssl_ciphers": "", "name": "www.taobao.com", "create_time": "1594371049", "last_update_time": "1594374794", "is_enabled": false, "detector_ip_source": ["Socket"], "proxy_ip_list": [], "proxy_ip_groups": [], "access_log": {"is_enabled": true, "log_request_header": false, "log_response_header": false, "log_request_body": false, "log_payload": false, "log_dest_ip": true, "is_enable_full_access_log": false, "log_src_port": true, "log_event_id": true, "log_proxy_name": true}, "proxy_bind_config": {"enable": false, "hash_select_ip_method": "remote_addr_and_port", "proxy_bind_ip_list": null}, "remark": "", "ssl_cert": null, "policy_group": 6}], "total": 1} </pre>	The information about the websites.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeWebsite
&RegionId=cn-hangzhou
&Id=1
&PageSize=20
&PageNumber=1
&IsVpcWebsite=true
&WebsiteNameFilter.1=website-1
&ServerNameFilter.1=www.taobao.com
```

Sample success responses

XML format

```
<DescribeWebsiteResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"items": [{"id": 1, "ip": ["0.0.XX.XX"], "session_method": {"type": "off"}, "policy_rules": [], "health_check_status": "", "backend_config": {"type": "proxy", "load_balance_policy": "Round Robin", "servers": [{"protocol": "http", "attr": "slb", "host": "192.168.XX.XX", "port": 80, "weight": 1}], "x_forwarded_for_action": "append", "header_config": [], "health_check_config": {"is_enabled": false, "check_http_expect_alive": ["http_2xx", "http_3xx"], "check_type": "http", "interval": 30000, "fall": 5, "rise": 2, "timeout": 1000, "port": null, "host": "", "method": "GET", "path": "/"}, "proxy_ssl_protocols": [], "proxy_ssl_ciphers": ""}, "vpc": "vpc-tx9isqljrry8k3h9q****", "vpc_name": "tongquesingletunnel", "vip": ["42.36.XX.XX"], "ports": [{"port": 80, "ssl": false, "http2": false}], "is_vpc_website": false, "operation_mode": "Software Reverse Proxy", "interface": "virtual", "server_names": ["www.taobao.com"], "ssl_protocols": [], "ssl_ciphers": "", "name": "www.taobao.com", "create_time": "1594371049", "last_update_time": "1594374794", "is_enabled": false, "detector_ip_source": ["Socket"], "proxy_ip_list": [], "proxy_ip_groups": [], "access_log": {"is_enabled": true, "log_request_header": false, "log_response_header": false, "log_request_body": false, "log_payload": false, "log_dest_ip": true, "is_enable_full_access_log": false, "log_src_port": true, "log_event_id": true, "log_proxy_name": true}, "proxy_bind_config": {"enable": false, "hash_select_ip_method": "remote_addr_and_port", "proxy_bind_ip_list": null}, "remark": "", "ssl_cert": null, "policy_group": 6}], "total": 1}</Result>
</DescribeWebsiteResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "items": [
      {
        "id": 1,
        "ip": ["0.0.XX.XX"],
        "session_method": {
          "type": "off",
          "policy_rules": [],
          "health_check_status": "",
          "backend_config": {
            "type": "proxy",
            "load_balance_policy": "Round Robin",
            "servers": [
              {
                "protocol": "http",
                "attr": "slb",
                "host": "192.168.XX.XX",
                "port": 80,
                "weight": 1
              }
            ],
            "x_forwarded_for_action": "append",
            "header_config": [],
            "health_check_config": {
              "is_enabled": false,
              "check_http_expect_alive": ["http_2xx", "http_3xx"],
              "check_type": "http",
              "interval": 30000,
              "fall": 5,
              "rise": 2,
              "timeout": 1000,
              "port": null,
              "host": "",
              "method": "GET",
              "path": "/"
            },
            "proxy_ssl_protocols": [],
            "proxy_ssl_ciphers": "",
            "vpc": "vpc-tx9isqljrry8k3h9q***",
            "vpc_name": "tongquesingletunnel",
            "vip": ["42.36.XX.XX"],
            "ports": [
              {
                "port": 80,
                "ssl": false,
                "http2": false
              }
            ],
            "is_vpc_website": false,
            "operation_mode": "Software Reverse Proxy",
            "interface": "virtual",
            "server_names": ["www.taobao.com"],
            "ssl_protocols": [],
            "ssl_ciphers": "",
            "name": "www.taobao.com",
            "create_time": "1594371049",
            "last_update_time": "1594374794",
            "is_enabled": false,
            "detector_ip_source": "Socket",
            "proxy_ip_list": [],
            "proxy_ip_groups": [],
            "access_log": {
              "is_enabled": true,
              "log_request_header": false,
              "log_response_header": false,
              "log_request_body": false,
              "log_payload": false,
              "log_dest_ip": true,
              "is_enable_full_access_log": false,
              "log_src_port": true,
              "log_event_id": true,
              "log_proxy_name": true
            },
            "proxy_bind_config": {
              "enable": false,
              "hash_select_ip_method": "remote_addr_and_port",
              "proxy_bind_ip_list": null
            },
            "remark": "",
            "ssl_cert": null,
            "policy_group": 6
          }
        ],
        "total": 1
      }
    ]
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.2. CreateWebsite

Adds a website.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateWebsite	The operation that you want to perform. Set the value to CreateWebsite.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Name	String	Yes	test-website-1	The name of the website.
ServerNameList	RepeatList	Yes	["www.aliyun.com", "www.taobao.com"]	The domain name of the website. You can enter multiple domain names.

Parameter	Type	Required	Example	Description
PortList	RepeatList	Yes	<pre>[{"port":80,"ssl":false,"http2":false}, {"port":443,"ssl":true,"http2":true}]</pre>	The port information about the website. This parameter is a string consisting of JSON arrays. Each element in a JSON array is a JSON struct that includes the following fields: • port: the port number of the website. This field is required. Data type: integer. Valid values: 1 to 65535. • ssl: specifies whether to enable an SSL certificate. This field is required. Data type: Boolean. • http2: specifies whether to enable HTTP/2. This field is required. Data type: Boolean.
SSLCertId	Integer	No	3	The ID of the SSL certificate. If ssl of a port specified in PortList is set to true, this field is required. You can call the DescribeSSLCert operation to query the IDs of SSL certificates.
				The configurations of the website. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • type: the method to respond to requests. This field is required. Data type: string. Valid values: ◦ proxy: forwards requests to the backend server. ◦ redirect: redirects requests. ◦ response: returns specific content. • servers: the information about the backend server. This field is a string consisting of JSON arrays. Each element in a JSON array is a JSON struct that includes the following fields: ◦ path: the destination address for redirection. Data type: string. If type in BackendConfig is set to redirect or response, this field is required.

Parameter	Type	Required	Example	Description
BackendConfig	Json	Yes	<pre>{ "type": "proxy", "servers": [{ "host": "192.168.XX.XX", "port": 80, "protocol": "http", "attr": "ecs", "weight": 1 }], "load_balance_policy": "RoundRobin", "x_forwarded_for_action": "append", "header_config": [] }</pre>	◦ status_code: the status code in the responses. Data type: integer. If type in BackendConfig is set to redirect or response, this field is required. ◦ host: the IP address of the backend server. This field is required. Data type: string. If the backend server is an Elastic Compute Service (ECS) or Server Load Balancer (SLB) instance, you can call the DescribeEcs or DescribeSlb operation to query the IP addresses (values of the host field) of backend servers. ◦ port: the port number of the backend server. This field is required. Data type: integer. Valid values: 1 to 65535. ◦ protocol: the protocol of the backend server. This field is required. Data type: string. Valid values: http and https. ◦ attr: the type of the backend server. This field is required. Data type: string. If you do not need to forward requests destined for the website to a specific backend server, set the value to normal. If you need to forward requests destined for the website to a specific backend server, set the value to ecs or slb. ◦ weight: the weight of the backend server. This field is required. Data type: integer. Valid values: any non-zero positive integer. • load_balance_policy: the scheduling algorithm. This field is required. Data type: string. Valid values: ◦ Round Robin: weighted round-robin ◦ Least Connected: least connection scheduling ◦ IP Hash: source IP hash • x_forwarded_for_action: the action on the X-Forwarded-For field in the HTTP request header. To identify the actual IP addresses of the clients that access your website by using HTTP proxies or load

Parameter	Type	Required	Example	Description
				balancing servers, you can specify this field. This field is required. Data type: string. Valid values: ◦ append: appends the last-hop IP address to the X-Forwarded-For field. ◦ cover: overwrites the original value of the X-Forwarded-For field with the last-hop IP address. ◦ no_action: retains the original value of the X-Forwarded-For field. • header_config: the HTTP header configurations. This field is required. Data type: list. If you do not need to configure the HTTP header, set the field to an empty array. This field is a string consisting of JSON arrays. Each element in a JSON array is a JSON struct that includes the following fields: ◦ name: the name of the HTTP header. This field is required. Data type: string. ◦ context: the type of the HTTP header. This field is required. Data type: string. Valid values: request and response. ◦ action: the action on the HTTP header. This field is required. Data type: string. Valid values: set and hide. ◦ value: the value of the HTTP header. This field is required. Data type: string.
PolicyGroupId	Integer	No	6	The ID of the protection policy. If type in BackendConfig is set to proxy, this field is required. You can call the DescribePolicyGroup operation to query the IDs of protection policies.

Parameter	Type	Required	Example	Description
SessionMethod	Json	Yes	<pre>{"param": "userId", "type": "url_query"}</pre>	The method to identify users. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • param: the ID of the user. • type: the method to identify users. This field is required. Data type: string. Valid values: ◦ off: does not identify users. ◦ custom: identifies users based on their IDs that are extracted from requests. ◦ cookie: identifies users based on the Cookie field. ◦ url_query: identifies users based on the GET parameters. ◦ body_form: identifies users based on the POST parameters. ◦ header: identifies users based on the HTTP header. ◦ internal_session: identifies users based on their systems.
Remark	String	No	Test site-1	The remarks.
Vpc	String	No	vpc-RSABVqbNiS****	The ID of the virtual private cloud (VPC). You can call the DescribeVpc operation to query the IDs of VPCs.
VpcName	String	No	csW	The name of the VPC. You can call the DescribeVpc operation to query the names of VPCs.
IsVpcWebsite	Boolean	No	true	Specifies whether the website is in a VPC. Default value: false. Valid values: • true • false
VipList	RepeatList	Yes	<pre>["192.168.XX.XX", "192.168.XX.XX"]</pre>	The virtual IP address (VIP). You can enter multiple VIPs. You can call the DescribeInternetVip operation to query the VIPs on the Internet and the DescribeVpcVip operation to query the VIPs in VPCs.

Parameter	Type	Required	Example	Description
IpSourceMethod	RepeatList	No	["Socket"]	The method to obtain the actual IP address. You can enter multiple methods. To obtain the actual IP address from a field in the HTTP request header, set the value to <i>XYZ/X-Forwarded-For: -n</i> . To obtain the socket information about the <i>last nth proxy</i> from X-Forwarded-For , append Socket to the end of the parameter value.

Parameter	Type	Required	Example	Description
AccessLogConfig	Json	No	<pre>{ "is_enabled": true, "log_request_header": false, "log_response_header": false, "log_request_body": false, "log_payload": false, "log_dest_ip": true, "is_enable_full_access_log": false, "log_src_port": true, "log_event_id": true, "log_proxy_name": true }</pre>	The configurations for access logs. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • is_enabled: specifies whether to record HTTP access logs. This parameter is required. Data type: Boolean. • log_request_header: specifies whether to record the HTTP request header. This parameter is required. Data type: Boolean. • log_response_header: specifies whether to record the HTTP response header. This parameter is required. Data type: Boolean. • log_request_body: specifies whether to record the HTTP request body. This parameter is required. Data type: Boolean. The maximum size of the HTTP request body that can be logged is 4 KB. • log_payload: specifies whether to record the payload. This parameter is required. Data type: Boolean. • log_dest_ip: specifies whether to record the destination IP address. This parameter is required. Data type: Boolean. • is_enable_full_access_log: specifies whether to record the full access logs. This parameter is required. Data type: Boolean. • log_src_port: specifies whether to record the source port. This parameter is required. Data type: Boolean. • log_event_id: specifies whether to record the ID of the event. This parameter is required. Data type: Boolean. • log_proxy_name: specifies whether to record the name of the proxy. This parameter is required. Data type: Boolean.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
SuccessCode	String	1	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.
		{ "id": 7, "ip": ["0.0.XX.XX"], "session_method": {"type": "off"}, "policy_rules": [], "health_check_statuses": "", "backend_config": {"type": "proxy", "load_balance_policy": "Round Robin", "servers": [{"protocol": "http", "attr": "normal", "host": "10.10.XX.XX", "port": 15334, "weight": 1}], "x_forwarded_for_action": "append",	

Parameter	Type	Example	Description
Result	String	<pre> "header_config": [], "health_check_config": { "g": {"is_enabled": false, "check_http_expect_alive": ["http_2xx", "http_3xx"], "check_type": "http", "interval": 30000, "fall": 5, "rise": 2, "timeout": 1000, "port": null, "host": "", "method": "GET", "path": "/"}, "proxy_ssl_protocols": [], "proxy_ssl_ciphers": "", "vpc": "vpc-tx9v6pc1nwc7pgtjx****", "vpc_name": "yundun****", "vip": ["10.10.XX.XX"], "ports": [{"port": 80, "ssl": false, "http2": false}], "is_vpc_website": false, "operation_mode": "Software Reverse Proxy", "interface": "virtual", "server_names": ["www.aliyun.com"], "ssl_protocols": [], "ssl_ciphers": "", "name": "www.aliyun.com", "create_time": "1598243334", "last_update_time": "1598339330", "is_enabled": true, "detector_ip_source": ["Socket"], "proxy_ip_list": [], "proxy_ip_groups": [], "access_log": {"is_enabled": true, "log_request_header": false, "log_response_header": false, "log_request_body": false, "log_payload": </pre>	The information about the added website.

Parameter	Type	Example	Description
		<pre> false, "enable_full_access_log": false, "ss_log": false, "log_dest_ip": true, "log_src_port": true, "log_event_id": true, "log_proxy_name": true, "remark": "", "ssl_cert": null, "policy_group": 26} </pre>	

Examples

Sample requests

```

https://semawaf.[RegionId].aliyuncs.com/?Action=CreateWebsite
&RegionId=cn-hangzhou
&Name=test-website-1
&ServerNameList.1=www.aliyun.com
&PortList.1={"port":80,"http2":false,"ssl":false}
&SSLCertId=3
&BackendConfig={"type": "proxy", "servers": [{"host": "192.168.XX.XX", "port": 80, "protocol": "http", "attr": "ecs", "weight": 1, "health_check_status": "UNKNOWN"}], "load_balance_policy": "Round Robin", "x_forwarded_for_action": "append", "header_config": []}
&PolicyGroupId=6
&SessionMethod={"param":"userId","type":"url_query"}
&Remark=**site -1
&Vpc=vpc-RSABVqbNiS****
&VpcName=csW
&IsVpcWebsite=true
&VipList.1=192.168.XX.XX
&IpSourceMethod.1=Socket
&AccessLogConfig={"is_enabled": true, "log_request_header": false, "log_response_header": false, "log_request_body": false, "log_payload": false, "log_dest_ip": true, "is_enable_full_access_log": false, "log_src_port": true, "log_event_id": true, "log_proxy_name": true}

```

Sample success responses

XML format

```
<CreateWebsiteResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"id": 7, "ip": ["0.0.XX.XX"], "session_method": {"type": "off"}, "policy_rules": [], "health_check_status": "", "backend_config": {"type": "proxy", "load_balance_policy": "Round Robin", "servers": [{"protocol": "http", "attr": "normal", "host": "10.10.XX.XX", "port": 15334, "weight": 1}], "x_forwarded_for_action": "append", "header_config": [], "health_check_config": {"is_enabled": false, "check_http_expect_alive": ["http_2xx", "http_3xx"], "check_type": "http", "interval": 30000, "fall": 5, "rise": 2, "timeout": 1000, "port": null, "host": "", "method": "GET", "path": "/"}, "proxy_ssl_protocols": [], "proxy_ssl_ciphers": ""}, "vpc": "vpc-tx9v6pc1nwc7pgtjx****", "vpc_name": "yundun****", "vip": ["10.10.XX.XX"], "ports": [{"port": 80, "ssl": false, "http2": false}], "is_vpc_website": false, "operation_mode": "Software Reverse Proxy", "interface": "virtual", "server_names": ["www.aliyun.com"], "ssl_protocols": [], "ssl_ciphers": "", "name": "www.aliyun.com", "create_time": "1598243334", "last_update_time": "1598339330", "is_enabled": true, "detector_ip_source": ["Socket"], "proxy_ip_list": [], "proxy_ip_groups": [], "access_log": {"is_enabled": true, "log_request_header": false, "log_response_header": false, "log_request_body": false, "log_payload": false, "is_enable_full_access_log": false, "log_dest_ip": true, "log_src_port": true, "log_event_id": true, "log_proxy_name": true}, "remark": "", "ssl_cert": null, "policy_group": 26}</Result>
  </TaskStatus>
</CreateWebsiteResponse>
```

JSON **format**

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": "[\"Website-related configuration generation\", \"Policy-related configuration generation\"]",
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": {
      "id": 7,
      "ip": ["0.0.XX.XX"],
      "session_method": {
        "type": "off",
        "policy_rules": [],
        "health_check_status": "",
        "backend_config": {
          "type": "proxy",
          "load_balance_policy": "Round Robin",
          "servers": [
            {
              "protocol": "http",
              "attr": "normal",
              "host": "10.10.XX.XX",
              "port": 15334,
              "weight": 1
            }
          ],
          "x_forwarded_for_action": "append",
          "header_config": [],
          "health_check_config": {
            "is_enabled": false,
            "check_http_expect_alive": ["http_2xx", "http_3xx"],
            "check_type": "http",
            "interval": 30000,
            "fall": 5,
            "rise": 2,
            "timeout": 1000,
            "port": null,
            "host": "",
            "method": "GET",
            "path": "/"
          },
          "proxy_ssl_protocols": [],
          "proxy_ssl_ciphers": "",
          "vpc": "vpc-tx9v6pclnwc7pgtjx****",
          "vpc_name": "yundun****",
          "vip": ["10.10.XX.XX"],
          "ports": [
            {
              "port": 80,
              "ssl": false,
              "http2": false
            }
          ],
          "is_vpc_website": false,
          "operation_mode": "Software Reverse Proxy",
          "interface": "virtual",
          "server_names": ["www.aliyun.com"],
          "ssl_protocols": [],
          "ssl_ciphers": "",
          "name": "www.aliyun.com",
          "create_time": "1598243334",
          "last_update_time": "1598339330",
          "is_enabled": true,
          "detector_ip_source": "Socket",
          "proxy_ip_list": [],
          "proxy_ip_groups": [],
          "access_log": {
            "is_enabled": true,
            "log_request_header": false,
            "log_response_header": false,
            "log_request_body": false,
            "log_payload": false,
            "is_enable_full_access_log": false,
            "log_dest_ip": true,
            "log_src_port": true,
            "log_event_id": true,
            "log_proxy_name": true
          },
          "remark": "",
          "ssl_cert": null,
          "policy_group": 26
        }
      }
    }
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.3. EditWebsite

Modifies the information about a specific website.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	EditWebsite	The operation that you want to perform. Set the value to EditWebsite.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	Yes	1	The ID of the website.
Name	String	Yes	test-website-1	The name of the website.

Parameter	Type	Required	Example	Description
ServerNameList	RepeatList	Yes	["www.aliyun.com", "www.taobao.com"]	The domain name of the website. You can enter multiple domain names.
PortList	RepeatList	Yes	[{"port": 80, "ssl": false, "http2": false}, {"port": 443, "ssl": true, "http2": true}]	The port information about the website. This parameter is a string consisting of JSON arrays. Each element in a JSON array is a JSON struct that includes the following fields: • port: the port number of the website. This field is required. Data type: integer. Valid values: 1 to 65535. • ssl: specifies whether to enable an SSL certificate. This field is required. Data type: Boolean. • http2: specifies whether to enable HTTP/2. This field is required. Data type: Boolean.
SSLCertId	Integer	No	3	The ID of the SSL certificate. If ssl of a port specified in PortList is set to true, this field is required. You can call the DescribeSSLCert operation to query the IDs of SSL certificates.
				The configurations of the website. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • type: the method to respond to requests. This field is required. Data type: string. Valid values: ◦ proxy: forwards requests to the backend server. ◦ redirect: redirects requests. ◦ response: returns specific content. • servers: the information about the backend server. This field is a string consisting of JSON arrays. Each element in a JSON array is a JSON struct that includes the following fields:

Parameter	Type	Required	Example	Description
BackendConfig	Json	Yes	<pre>{ "type": "proxy", "servers": [{ "host": "192.168.XX.XX", "port": 80, "protocol": "http", "attr": "ecs", "weight": 1 }], "load_balance_policy": "RoundRobin", "x_forwarded_for_action": "append", "header_config": [] }</pre>	◦ path: the destination address for redirection. Data type: string. If type in BackendConfig is set to redirect or response, this field is required. ◦ status_code: the status code in the responses. Data type: integer. If type in BackendConfig is set to redirect or response, this field is required. ◦ host: the IP address of the backend server. This field is required. Data type: string. If the backend server is an Elastic Compute Service (ECS) or Server Load Balancer (SLB) instance, you can call the DescribeEcs or DescribeSlb operation to query the IP addresses (values of the host field) of backend servers. ◦ port: the port number of the backend server. This field is required. Data type: integer. Valid values: 1 to 65535. ◦ protocol: the protocol of the backend server. This field is required. Data type: string. Valid values: http and https. ◦ attr: the type of the backend server. This field is required. Data type: string. If you do not need to forward requests destined for the website to a specific backend server, set the value to normal. If you need to forward requests destined for the website to a specific backend server, set the value to ecs or slb. ◦ weight: the weight of the backend server. This field is required. Data type: integer. Valid values: any non-zero positive integer. • load_balance_policy: the scheduling algorithm. This field is required. Data type: string. Valid values: ◦ Round Robin: weighted round-robin ◦ Least Connected: least connection scheduling ◦ IP Hash: source IP hash

Parameter	Type	Required	Example	Description
				• x_forwarded_for_action: the action on the X-Forwarded-For field in the HTTP request header. To identify the actual IP addresses of the clients that access your website by using HTTP proxies or load balancing servers, you can specify this field. This field is required. Data type: string. Valid values: ◦ append: appends the last-hop IP address to the X-Forwarded-For field. ◦ cover: overwrites the original value of the X-Forwarded-For field with the last-hop IP address. ◦ no_action: retains the original value of the X-Forwarded-For field. • header_config: the HTTP header configurations. This field is required. Data type: list. If you do not need to configure the HTTP header, set the field to an empty array. This field is a string consisting of JSON arrays. Each element in a JSON array is a JSON struct that includes the following fields: ◦ name: the name of the HTTP header. This field is required. Data type: string. ◦ context: the type of the HTTP header. This field is required. Data type: string. Valid values: request and response. ◦ action: the action on the HTTP header. This field is required. Data type: string. Valid values: set and hide. ◦ name: the value of the HTTP header. This field is required. Data type: string.
PolicyGroupId	Integer	No	6	The ID of the protection policy. If type in BackendConfig is set to proxy, this field is required. You can call the DescribePolicyGroup operation to query the IDs of protection policies.

Parameter	Type	Required	Example	Description
SessionMethod	Json	Yes	<code>{"param": "userId", "type": "url_query"}</code>	The method to identify users. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • param: the ID of the user. • type: the method to identify users. This field is required. Data type: string. Valid values: ◦ off: does not identify users. ◦ custom: identifies users based on their IDs that are extracted from requests. ◦ cookie: identifies users based on the Cookie field. ◦ url_query: identifies users based on the GET parameters. ◦ body_form: identifies users based on the POST parameters. ◦ header: identifies users based on the HTTP header. ◦ internal_session: identifies users based on their systems.
Remark	String	No	Test site-1	The remarks.
Vpc	String	No	vpc-RSABVqbNiS****	The ID of the virtual private cloud (VPC). You can call the DescribeVpc operation to query the IDs of VPCs.
VpcName	String	No	csw	The name of the VPC. You can call the DescribeVpc operation to query the names of VPCs.
IsVpcWebsite	Boolean	No	true	Specifies whether the website is in a VPC. Default value: false. Valid values: • true • false
VipList	RepeatList	Yes	<code>["192.168.XX.XX", "192.168.XX.XX"]</code>	The virtual IP address (VIP). You can enter multiple VIPs. You can call the DescribeInternetVip operation to query the VIPs on the Internet and the DescribeVpcVip operation to query the VIPs in VPCs.

Parameter	Type	Required	Example	Description
IpSourceMethod	RepeatList	Yes	["Socket"]	The method to obtain the actual IP address. You can enter multiple methods. To obtain the actual IP address from a field in the HTTP request header, set the value to <i>XYZ/X-Forwarded-For: -n</i> . To obtain the socket information about the <i>last nth proxy</i> from X-Forwarded-For , append Socket to the end of the parameter value.

Parameter	Type	Required	Example	Description
AccessLogConfig	Json	Yes	<pre>{ "is_enabled": true, "log_request_header": false, "log_response_header": false, "log_request_body": false, "log_payload": false, "log_dest_ip": true, "is_enable_full_access_log": false, "log_src_port": true, "log_event_id": true, "log_proxy_name": true }</pre>	The configurations for access logs. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • is_enabled: specifies whether to record HTTP access logs. This parameter is required. Data type: Boolean. • log_request_header: specifies whether to record the HTTP request header. This parameter is required. Data type: Boolean. • log_response_header: specifies whether to record the HTTP response header. This parameter is required. Data type: Boolean. • log_request_body: specifies whether to record the HTTP request body. This parameter is required. Data type: Boolean. The maximum size of the HTTP request body that can be logged is 4 KB. • log_payload: specifies whether to record the payload. This parameter is required. Data type: Boolean. • log_dest_ip: specifies whether to record the destination IP address. This parameter is required. Data type: Boolean. • is_enable_full_access_log: specifies whether to record the full access logs. This parameter is required. Data type: Boolean. • log_src_port: specifies whether to record the source port. This parameter is required. Data type: Boolean. • log_event_id: specifies whether to record the ID of the event. This parameter is required. Data type: Boolean. • log_proxy_name: specifies whether to record the name of the proxy. This parameter is required. Data type: Boolean.
SSLProtocols	RepeatList	No	["TLSv1.1", "TLSv1.2"]	The version of the SSL protocol. Valid values: SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2, and TLSv1.3.

Parameter	Type	Required	Example	Description
SSLCiphers	String	No	TLS_RSA_WITH_AES_128_CBC_SHA	The SSL cipher suite. This parameter is empty by default. You can directly use the cipher strings provided by OpenSSL. You can also concatenate and combine the cipher strings to match the value of the SSLProtocols parameter. Example: TLSv1.2:!eNULL:!aNULL:!TLSv1.1:!TLSv1:!SSLv3
ProxyBindingConfig	Json	No	<pre>{ "enable": true, "hash_select_ip_method": "remote_addr_and_port", "proxy_bind_ip_list": [{"id": "c43b02112.cloud.b03.amtest21", "ips": ["10.10.XX.XX"]}]} </pre>	The configurations of back-to-origin IP addresses. The value is a string that consists of a JSON struct. The JSON struct contains the following fields: • enable: specifies whether to enable session persistence. This field is required. Data type: Boolean. • hash_select_ip_method: the method for session persistence. This field is optional. Data type: string. Valid values: ◦ remote_addr: source address-based hashing ◦ remote_addr_and_port: source port-based hashing • proxy_bind_ip_list: the list of IP addresses. This field is optional. Data type: list.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the video moderation task. This ID is returned by the Content Moderation server.
└Time	String	1593593692	The UNIX timestamp of when the task ends. Unit: seconds.

Parameter	Type	Example	Description
<code>LTaskList</code>	String	<code>["Website-related configuration generation", "Policy-related configuration generation"]</code>	The descriptions of the task. This value is returned only for asynchronous tasks.
<code>LStatusMessage</code>	String	The configuration is in effect.	The status message of the task.
<code>LSuccessCode</code>	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.
		<pre>{ "id": 7, "ip": "0.0.XX.XX", "session_method": { "type": "off" }, "policy_rules": [], "health_check_statuses": "", "backend_config": { "type": "proxy", "load_balance_policy": "Round Robin", "servers": [{ "protocol": "http", "attr": "normal", "host": "10.10.XX.XX", "port": 15334, "weight": 1 }], "x_forwarded_for_action": "append", "header_config": [], "health_check_config": { "is_enabled": false, "check_http_expect_alive": ["http_2xx", "http_3xx"], "check_type": "http", "interval": 30000, "fall": 5, "rise": 2, "timeout": 1000, "port": null, "host": "", "method": "GET", "path": "/" }, "proxy_ssl_protocols": [] } }</pre>	

Parameter	Type	Example	Description
Result	String	<pre> { "proxy_ssl_ciphers": "SSLv3", "vpc": "vpc- tx9v6pc1nwc7pgtjx*", "vpc_name": "****", "yundun****": "vip": ["10.10.XX.XX"], "ports": [{"port": 80, "ssl": false, "http2": false}], "is_vpc_website": false, "operation_mode": "Software Reverse Proxy", "interface": "virtual", "server_names": ["www.aliyun.com"], "ssl_protocols": [], "ssl_ciphers": "", "name": "www.aliyun.com", "create_time": "1598243334", "last_update_time": "1598339330", "is_enabled": true, "detector_ip_source": ["Socket"], "proxy_ip_list": [], "proxy_ip_groups": [], "access_log": {"is_enabled": true, "log_request_header": false, "log_response_header": false, "log_request_body": false, "log_payload": false, "is_enable_full_access_log": false, "log_dest_ip": true, "log_src_port": true, "log_event_id": true, "log_proxy_name": true}, "remark": "", "ssl_cert": null, "policy_group": 26} </pre>	The information about the website after modification.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=EditWebsite
&RegionId=cn-hangzhou
&Id=1
&Name=test-website-1
&ServerNameList.1=www.aliyun.com
&PortList.1={"port":80,"http2":false,"ssl":false}
&SSLCertId=3
&BackendConfig={"type": "proxy", "servers": [{"host": "192.168.XX.XX", "port":
80, "protocol": "http", "attr": "ecs", "weight": 1, "health_check_status": "UN
KNOWN"}], "load_balance_policy": "Round Robin", "x_forwarded_for_action": "append"
, "header_config": []}
&PolicyGroupId=6
&SessionMethod={"param":"userId","type":"url_query"}
&Remark=***website-1
&Vpc=vpc-RSABVqbNiS***
&VpcName=csw
&IsVpcWebsite=true
&VipList.1=192.168.XX.XX
&IpSourceMethod.1=Socket
&AccessLogConfig={"is_enabled": true, "log_request_header": false, "log_response_heade
r": false, "log_request_body": false, "log_payload": false, "log_dest_ip": true, "i
s_enable_full_access_log": false, "log_src_port": true, "log_event_id": true, "log_pr
oxy_name": true}
&SSLProtocols.1=TLSv1.1
&SSLCiphers=TLS_RSA_WITH_AES_128_CBC_SHA
&ProxyBindingConfig={"enable": true, "hash_select_ip_method": "remote_addr_and_port",
"proxy_bind_ip_list": [{"id": "c43b02112.cloud.b03***", "ips": ["10.10.XX.XX"]}]}
}
```

Successful response examples

XML [format](#)

```

<EditWebsiteResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"id": 7, "ip": ["0.0.XX.XX"], "session_method": {"type": "off"}, "policy_rules": [], "health_check_status": "", "backend_config": {"type": "proxy", "load_balance_policy": "Round Robin", "servers": [{"protocol": "http", "attr": "normal", "host": "10.10.XX.XX", "port": 15334, "weight": 1}], "x_forwarded_for_action": "append", "header_config": [], "health_check_config": {"is_enabled": false, "check_http_expect_alive": ["http_2xx", "http_3xx"], "check_type": "http", "interval": 30000, "fall": 5, "rise": 2, "timeout": 1000, "port": null, "host": "", "method": "GET", "path": "/"}, "proxy_ssl_protocols": [], "proxy_ssl_ciphers": ""}, "vpc": "vpc-tx9v6pc1nwc7pgtjx****", "vpc_name": "yundun****", "vip": ["10.10.XX.XX"], "ports": [{"port": 80, "ssl": false, "http2": false}], "is_vpc_website": false, "operation_mode": "Software Reverse Proxy", "interface": "virtual", "server_names": ["www.aliyun.com"], "ssl_protocols": [], "ssl_ciphers": "", "name": "www.aliyun.com", "create_time": "1598243334", "last_update_time": "1598339330", "is_enabled": true, "detector_ip_source": ["Socket"], "proxy_ip_list": [], "proxy_ip_groups": [], "access_log": {"is_enabled": true, "log_request_header": false, "log_response_header": false, "log_request_body": false, "log_payload": false, "is_enable_full_access_log": false, "log_dest_ip": true, "log_src_port": true, "log_event_id": true, "log_proxy_name": true}, "remark": "", "ssl_cert": null, "policy_group": 26}</Result>
  </TaskStatus>
</EditWebsiteResponse>

```

JSON **format**

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": {
      "id": 7,
      "ip": ["0.0.XX.XX"],
      "session_method": {
        "type": "off",
        "policy_rules": [],
        "health_check_status": "",
        "backend_config": {
          "type": "proxy",
          "load_balance_policy": "Round Robin",
          "servers": [
            {
              "protocol": "http",
              "attr": "normal",
              "host": "10.10.XX.XX",
              "port": 15334,
              "weight": 1
            }
          ],
          "x_forwarded_for_action": "append",
          "header_config": [],
          "health_check_config": {
            "is_enabled": false,
            "check_http_expect_alive": ["http_2xx", "http_3xx"],
            "check_type": "http",
            "interval": 30000,
            "fall": 5,
            "rise": 2,
            "timeout": 1000,
            "port": null,
            "host": "",
            "method": "GET",
            "path": "/"
          },
          "proxy_ssl_protocols": [],
          "proxy_ssl_ciphers": [],
          "vpc": "vpc-tx9v6pclnwc7pgtjx****",
          "vpc_name": "yundun****",
          "vip": ["10.10.XX.XX"],
          "ports": [
            {
              "port": 80,
              "ssl": false,
              "http2": false
            }
          ],
          "is_vpc_website": false,
          "operation_mode": "Software Reverse Proxy",
          "interface": "virtual",
          "server_names": ["www.aliyun.com"],
          "ssl_protocols": [],
          "ssl_ciphers": "",
          "name": "www.aliyun.com",
          "create_time": "1598243334",
          "last_update_time": "1598339330",
          "is_enabled": true,
          "detector_ip_source": "Socket",
          "proxy_ip_list": [],
          "proxy_ip_groups": [],
          "access_log": {
            "is_enabled": true,
            "log_request_header": false,
            "log_response_header": false,
            "log_request_body": false,
            "log_payload": false,
            "is_enable_full_access_log": false,
            "log_dest_ip": true,
            "log_src_port": true,
            "log_event_id": true,
            "log_proxy_name": true
          },
          "remark": "",
          "ssl_cert": null,
          "policy_group": 26
        }
      }
    }
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.4. ToggleWebsite

Enables or disables WAF protection for a specific website.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ToggleWebsite	The operation that you want to perform. Set the value to ToggleWebsite.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
IdList	RepeatList	Yes	[1, 2]	The ID of the asynchronous task.

Parameter	Type	Required	Example	Description
ToggleAction	String	Yes	disable	Specifies the protection status of the website. Valid values: • enable: enables WAF protection. • disable: disables WAF protection.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		The returned information.
L-TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
L-Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
L-TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
L-StatusMessage	String	The configuration is in effect.	The status message of the task.
L-SuccessCode	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=ToggleWebsite
&RegionId=cn-hangzhou
&IdList.1=1
&ToggleAction=disable
```


Sample success responses

XML format

```
<ToggleWebsiteResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</ToggleWebsiteResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": "[\"Website-related configuration generation\", \"Policy-related configuration generation\"]",
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.5. QueryAsyncTaskStatus

Queries the status of an asynchronous task.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryAsyncTaskStatus	The operation that you want to perform. Set the value to QueryAsyncTaskStatus.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
TaskId	String	Yes	11c745fc-1d66-40ea-90d7-7e9a12b987b2	The ID of the asynchronous task.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
LTaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
LTime	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
LTaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
LStatusMessage	String	The configuration is in effect.	The status message of the task.
LSuccessCode	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=QueryAsyncTaskStatus
&RegionId=cn-hangzhou
&TaskId=11c745fc-1d66-40ea-90d7-7e9a12b987b2
```

Sample success responses

XML format

```
<QueryAsyncTaskStatusResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</QueryAsyncTaskStatusResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": "[\"Website-related configuration generation\", \"Policy-related configuration generation\"]",
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.6. UploadResponsePage

Uploads a response page file.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UploadResponsePage	The operation that you want to perform. Set the value to UploadResponsePage.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
FileName	String	No	forbidden.html	The name of the file.
FileContent	String	Yes	VXVPVm5QZEVuWHJhc2ViUGhNZEZRWHBjSnNRZXJn	The Base64-encoded content of the file.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"path": "572e83ed3331eb575f2dbd39f07e155"}	The returned information. path : the path of the uploaded file.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=UploadResponsePage
&RegionId=cn-hangzhou
&FileName=forbidden.html
&FileContent=VXVPVm5QZEVuWHJhc2ViUGhNZEZRWHBjSnNRZXJn
```

Sample success responses

XML format

```
<UploadResponsePageResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"path": "572e83ed3331eb575f2dbd39f07e155"}</Result>
</UploadResponsePageResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"path": "572e83ed3331eb575f2dbd39f07e155"}
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.7. DescribeInvalidWebsite

Queries the information about the invalid websites that are discovered by the upgrade detection feature.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeInvalidWebsite	The operation that you want to perform. Set the value to DescribeInvalidWebsite.

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	No	1	The ID of the invalid website.
PageSize	Integer	No	20	The number of entries to return on each page. Default value: 10.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	<pre>[{"id": 1, "name": "invalid_website_1", "server_names": ["www.taobao.com "], "backend_config": {"type": "proxy", "load_balance_polic y": "Round Robin", "servers": [{"protocol": "http", "attr": "slb", "host": "192.168.XX.XX", "port": 80, "weight": 1}], "x_forwarded_for_a ction": "append", "header_config": [], "health_check_confi g": {"is_enabled": false, "check_http_expect _alive": ["http_2xx", "http_3xx"], "check_type": "http", "interval": 30000, "fall": 5, "rise": 2, "timeout": 1000, "port": null, "host": "", "method": "GET", "path": "/"}, "proxy_ssl_protocol s": [], "proxy_ssl_ciphers": ""}, "aliyun_info": {"id": 1, "vpc": "vpc- tx9isq1jrry8k3h9q*** ", "vswitch": "vsw- tx9v9qpazlcc86f* ****", "vip": ["10.10.XX.XX"], "is_normal": true, "frontend_port": [80]}]}</pre>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeInvalidWebsite
&RegionId=cn-hangzhou
&Id=1
&PageSize=20
&PageNumber=1
```

Sample success responses

XML format

```
<DescribeInvalidWebsiteResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>[{ "id": 1, "name": "invalid_website_1", "server_names": ["www.taobao.com"], "ba
ckend_config": { "type": "proxy", "load_balance_policy": "Round Robin", "servers": [{ "protoc
ol": "http", "attr": "slb", "host": "192.168.XX.XX", "port": 80, "weight": 1}], "x_forwarde
d_for_action": "append", "header_config": [], "health_check_config": { "is_enabled": false,
"check_http_expect_alive": ["http_2xx", "http_3xx"], "check_type": "http", "interval": 3000
0, "fall": 5, "rise": 2, "timeout": 1000, "port": null, "host": "", "method": "GET", "path"
: "/"}, "proxy_ssl_protocols": [], "proxy_ssl_ciphers": ""}, "aliyun_info": { "id": 1, "vpc"
: "vpc-tx9isqljrry8k3h9q****", "vswitch": "vsw-tx9v9qpazlcc86f****", "vip": ["10.10.XX.XX
"], "is_normal": true, "frontend_port": [80]} }]</Result>
</DescribeInvalidWebsiteResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": "[{"id": 1, "name": "invalid_website_1", "server_names": ["www.taobao.c
om"], "backend_config": {"type": "proxy", "load_balance_policy": "Round Robin",
"servers": [{"protocol": "http", "attr": "slb", "host": "192.168.XX.XX", "po
rt": 80, "weight": 1}], "x_forwarded_for_action": "append", "header_config": [], \
"health_check_config": {"is_enabled": false, "check_http_expect_alive": ["http_2xx",
"http_3xx"], "check_type": "http", "interval": 30000, "fall": 5, "rise": 2, "t
imeout": 1000, "port": null, "host": "", "method": "GET", "path": "/"}, "pr
oxy_ssl_protocols": [], "proxy_ssl_ciphers": ""}, "aliyun_info": {"id": 1, "vpc"
: "vpc-tx9isqljrry8k3h9q****", "vswitch": "vsw-tx9v9qpazlcc86f****", "vip": ["10
.10.XX.XX"], "is_normal": true, "frontend_port": [80]} }]"
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.8. DeleteInvalidWebsite

Deletes a specific invalid website. If you use Apsara Stack Enterprise V3.12.0 or upgrade Apsara Stack Enterprise to a later version, WAF performs validity checks and measures invalid websites.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteInvalidWebsite	The operation that you want to perform. Set the value to DeleteInvalidWebsite.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
IdList	RepeatList	Yes	[1, 2]	The ID of the invalid website. You can enter multiple IDs. You can call the DescribeWebsite operation to query the IDs of websites.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	None	The returned information. This value is empty.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DeleteInvalidWebsite
&RegionId=cn-hangzhou
&IdList.1=1
```

Sample success responses

XML format

```
<DeleteInvalidWebsiteResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result></Result>
</DeleteInvalidWebsiteResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": ""
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.9. DescribeInternetVip

Queries the information about the virtual IP addresses (VIPs) on the Internet.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeInternetVip	The operation that you want to perform. Set the value to DescribeInternetVip.
RegionId	String	Yes	cn-hangzhou	The ID of the region.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	<pre>{ "ip": "42.36.XX.XX", "type": "internet IP", "delete": false, "ip": "10.10.XX.XX", "type": "intranet IP", "delete": false }</pre>	The information about the VIPs on the Internet. The information includes the following fields: ip: the VIP on the Internet. type: the type of the return value. The field value is fixed as internet IP, which indicates a VIP on the Internet. delete: indicates whether the VIP can be deleted. Valid values: true: The VIP can be deleted. false: The VIP cannot be deleted.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeInternetVip
&RegionId=cn-hangzhou
```

Sample success responses

XML format

```
<DescribeInternetVipResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>[{"ip": "42.36.XX.XX", "type": "internet IP", "delete": false}, {"ip": "10.10.XX.XX", "type": "intranet IP", "delete": false}]</Result>
</DescribeInternetVipResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": [{
    "ip": "42.36.XX.XX",
    "type": "internet IP",
    "delete": false
  }, {
    "ip": "10.10.XX.XX",
    "type": "intranet IP",
    "delete": false
  }]
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.10. CreateInternetVip

Creates a virtual IP address (VIP) on the Internet.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateInternetVip	The operation that you want to perform. Set the value to CreateInternetVip.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
IpAddress	String	No	10.10.XX.XX	The VIP that you want to create on the Internet.
IpVersion	String	No	ipv6	The version of the IP protocol. Valid values: • ipv4 • ipv6
NetworkType	String	Yes	internet	The type of the network. Valid values: • intranet • internet If you set the IpVersion parameter to ipv6 , you can set the NetworkType parameter only to intranet .

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	<pre>{"ip": "42.36.XX.XX", "type": "internet IP", "delete": true}</pre>	The information about the created VIP. The information includes the following fields: • ip: the VIP on the Internet. • type: the type of the return value. The field value is fixed as internet IP, which indicates a VIP on the Internet. • delete: indicates whether the VIP can be deleted. Valid values: ◦ true: The VIP can be deleted. ◦ false: The VIP cannot be deleted.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=CreateInternetVip  
&RegionId=cn-hangzhou  
&IpAddress=10.10.XX.XX  
&IpVersion=ipv6  
&NetworkType=internet
```

Sample success responses

XML format

```
<CreateInternetVipResponse>  
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>  
  <Result>{"ip": "42.36.XX.XX", "type": "internet IP", "delete": true}</Result>  
</CreateInternetVipResponse>
```

JSON format

```
{  
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",  
  "Result": {"ip": "42.36.XX.XX", "type": "internet IP", "delete": true}  
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.11. DeleteInternetVip

Deletes a virtual IP address (VIP) on the Internet.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteInternetVip	The operation that you want to perform. Set the value to DeleteInternetVip.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Vip	String	No	10.10.XX.XX	The VIP that you want to delete on the Internet.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	Empty	The returned information. This value is empty.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DeleteInternetVip
&RegionId=cn-hangzhou
&Vip=10.10.XX.XX
```

Sample success responses

XML format

```
<DeleteInternetVipResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result></Result>
</DeleteInternetVipResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": ""
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.12. DescribeVpc

Queries the information about virtual private clouds (VPCs).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVpc	The operation that you want to perform. Set the value to DescribeVpc.
RegionId	String	Yes	cn-hangzhou	The ID of the region.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"vpc_list": [{"vpc_id": "vpc-tx9fk7rftc9wbroix****", "name": "cfw_vpc****", "desc": "", "cidr": "172.16.XX.XX/16"}]}	The information about the VPCs.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeVpc&RegionId=cn-hangzhou
```

Sample success responses

XML format

```
<DescribeVpcResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"vpc_list": [{"vpc_id": "vpc-tx9fk7rftc9wbroix****", "name": "cfw_vpc****", "desc": "", "cidr": "172.16.XX.XX/16"}]}</Result>
</DescribeVpcResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"vpc_list": [{"vpc_id": "vpc-tx9fk7rftc9wbroix****", "name": "cfw_vpc****", "desc": "", "cidr": "172.16.XX.XX/16"}]}
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.13. DescribeVSwitch

Queries the information about the vSwitches in a specific virtual private cloud (VPC).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVSwitch	The operation that you want to perform. Set the value to DescribeVSwitch.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
VpcId	String	Yes	vpc-RSABVqbNiSs***	The ID of the VPC. You can call the DescribeVpc operation to query the IDs of VPCs.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	<pre>{"vswitch_list": [{"instanceId": "vsw-tx9v9qpazldcc86***", "instanceName": "zyp004", "vpcId": "vpc-tx9evaxvf65gt95gb***", "cidrBlock": "192.168.XX.XX/16", "description": ""}]}</pre>	The information about the vSwitches in the VPC.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeVSwitch
&RegionId=cn-hangzhou
&VpcId=vpc-RSABVqbNiSs****
```

Sample success responses

XML format

```
<DescribeVSwitchResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"vswitch_list": [{"instanceId": "vsw-tx9v9qpazlcc86f****", "instanceName": "zyp004", "vpcId": "vpc-tx9evaxvf65gt95gb****", "cidrBlock": "192.168.XX.XX/16", "description": ""}]}</Result>
</DescribeVSwitchResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"vswitch_list": [{"instanceId": "vsw-tx9v9qpazlcc86f****", "instanceName": "zyp004", "vpcId": "vpc-tx9evaxvf65gt95gb****", "cidrBlock": "192.168.XX.XX/16", "description": ""}]}
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.14. DescribeVpcVip

Queries the information about the virtual IP addresses (VIPs) in a specific virtual private cloud (VPC).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeVpcVip	The operation that you want to perform. Set the value to DescribeVpcVip.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
VpcId	String	Yes	vpc-RSABVqbNiS***	The ID of the VPC. You can call the DescribeVpc operation to query the IDs of VPCs.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	<pre>{ "items": [{ "ip": "192.168.XX.XX", "type": "IP" }], "total": 1 }</pre>	The information about the VIPs in the VPC. The information includes the following fields: items: the returned VIPs. Information about the VIPs: ip: the VIP in the VPC. type: the type of the return value. The field value is fixed as IP, which indicates a VIP. total: the total number of VIPs returned.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeVpcVip
&RegionId=cn-hangzhou
&VpcId=vpc-RSABVqbNiSs****
```

Sample success responses

XML format

```
<DescribeVpcVipResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"items": [{"ip": "192.168.XX.XX", "type": "IP"}], "total": 1}</Result>
</DescribeVpcVipResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "items": [
      {
        "ip": "192.168.XX.XX",
        "type": "IP"
      }
    ],
    "total": 1
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.15. CreateVpcVip

Creates a virtual IP address (VIP) in a specific virtual private cloud (VPC).

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateVpcVip	The operation that you want to perform. Set the value to CreateVpcVip.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
VpcId	String	Yes	vpc-RSABVqbNiSs*** *	The ID of the VPC. You can call the DescribeVpc operation to query the IDs of VPCs.
VSwitchId	String	Yes	vsw-APUjoSJOOBw*** *	The ID of the vSwitch.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"ip": "192.168.XX.XX", "type": "intranet IP"}	The information about the created VIP. The type field indicates the type of the VIP. The field value is fixed as intranet IP , which indicates an internal IP address.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=CreateVpcVip
&RegionId=cn-hangzhou
&VpcId=vpc-RSABVqbNiSs***
&VSwitchId=vsw-APUjoSJOOBw***
```

Sample success responses

XML format

```
<CreateVpcVipResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"ip": "192.168.XX.XX", "type": "intranet IP"}</Result>
</CreateVpcVipResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": "{\"ip\": \"192.168.XX.XX\", \"type\": \"intranet IP\"}"
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.16. DeleteVpcVip

Deletes a virtual IP address (VIP) in a specific virtual private cloud (VPC).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteVpcVip	The operation that you want to perform. Set the value to DeleteVpcVip.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
VpcId	String	Yes	vpc-RSABVqbNiSs***	The ID of the VPC. You can call the DescribeVpc operation to query the IDs of VPCs.
Vip	String	Yes	10.10.XX.XX	The VIP in the VPC. You can call the DescribeVpcVip operation to query the VIPs in a specific VPC.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	None	The returned information. If the call is successful, this value is empty.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DeleteVpcVip
&RegionId=cn-hangzhou
&VpcId=vpc-RSABVqbNiSs***
&Vip=10.10.XX.XX
```

Sample success responses

XML format

```
<DeleteVpcVipResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result></Result>
</DeleteVpcVipResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": ""
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.17. DescribeEcs

Queries the information about the Elastic Compute Service (ECS) instances in a specific virtual private cloud (VPC).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeEcs	The operation that you want to perform. Set the value to DescribeEcs.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
VpcId	String	Yes	vpc-RSABVqbNiSs***	The ID of the VPC. You can call the DescribeVpc operation to query the IDs of VPCs.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	<pre>{ "ecs": [{ "instanceId": "i-tx905fcs7erxox**", "instanceName": "ecs****", "internetIp": "", "intranetIp": "192.168.XX.XX", "eip": "", "natIp": "6.6.XX.XX", "status": "Running", "networkType": "vpc", "vpcId": "vpc-tx94ktgeqccd7l98c****", "vswitchId": "vsw-tx9vktwbt8w3vw6wh****", "securityGroupId": "sg-tx9aps47sy596qwj**", "hostName": "iZtx905fcs7erxoxa****", "osType": "CentOS 7.2", "createTime": 1588838676000 }] }</pre>	The information about the ECS instances in the VPC.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeEcs
&RegionId=cn-hangzhou
&VpcId=vpc-RSABVqbNiSs****
```

Sample success responses

`XML` format

```
<DescribeEcsResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"ecs": [{"instanceId": "i-tx905fcs7erxzox****", "instanceName": "ecs****", "internetIp": "", "intranetIp": "192.168.XX.XX", "eip": "", "natIp": "6.6.XX.XX", "status": "Running", "networkType": "vpc", "vpcId": "vpc-tx94ktgeqccd7l98c****", "vswitchId": "vsw-tx9vktwbt8w3vw6wh****", "securityGroupId": "sg-tx9aps47sy596qwj****", "hostName": "iZtx905fcs7erxzoxa****", "osType": "CentOS 7.2", "createTime": 1588838676000}]}</Result>
</DescribeEcsResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"ecs": [{"instanceId": "i-tx905fcs7erxzox****", "instanceName": "ecs****", "internetIp": "", "intranetIp": "192.168.XX.XX", "eip": "", "natIp": "6.6.XX.XX", "status": "Running", "networkType": "vpc", "vpcId": "vpc-tx94ktgeqccd7l98c****", "vswitchId": "vsw-tx9vktwbt8w3vw6wh****", "securityGroupId": "sg-tx9aps47sy596qwj****", "hostName": "iZtx905fcs7erxzoxa****", "osType": "CentOS 7.2", "createTime": 1588838676000}]}
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.1.18. DescribeSlb

Queries the information about the Server Load Balancer (SLB) instances in a specific virtual private cloud (VPC).

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSlb	The operation that you want to perform. Set the value to DescribeSlb.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
VpcId	String	Yes	vpc-RSABVqbNiSs***	The ID of the VPC. You can call the DescribeVpc operation to query the IDs of VPCs.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"slb": [{"instanceId": "slb-tx9n49pigmazoow4h****", "instanceName": "waf****", "status": "active", "networkType": "intranet", "ip": "192.168.XX.XX", "ipVersion": "ipv4"}]}	The information about the SLB instances in the VPC.

Examples

Sample requests

```
https://semawaf.[ RegionId].aliyuncs.com/?Action=DescribeSlb
&RegionId=cn-hangzhou
&VpcId=vpc-RSABVqbNiSs****
```

Sample success responses

XML format

```
<DescribeSlbResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"slb": [{"instanceId": "slb-tx9n49pigmazoow4h****", "instanceName": "waf****",
"status": "active", "networkType": "intranet", "ip": "192.168.XX.XX", "ipVersion": "ipv4"}]}
</Result>
</DescribeSlbResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"slb": [{"instanceId": "slb-tx9n49pigmazoow4h****", "instanceName": "waf****",
"status": "active", "networkType": "intranet", "ip": "192.168.XX.XX",
"ipVersion": "ipv4"}]}}
```

Error codes

For a list of error codes, see [Error codes](#).

9.2. HTTP flood protection rules

9.2.1. DescribeCCRuleTemplate

Queries the information about HTTP flood protection rules.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCCRuleTemplate	The operation that you want to perform. Set the value to DescribeCCRuleTemplate.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	No	1	The ID of the HTTP flood protection rule.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: 10.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	<pre>{"items": [{"id": 1, "name": "cc-policy-test", "version": 40, "is_enabled": true, "match_method": {"target_type": "CIDR", "period": null, "limit": null, "scope": "URL Prefix", "policy": "www.taobao.com", "scheme": "http"}, "action": {"action": "forbid"}, "create_time": "1594627307", "expire_period": 10, "execution_number": 0, "template_type": "manual", "is_inaccurate": false, "dry_run": false}], "total": 1}</pre>	The returned result of the request. For more information about the match_method parameter in the returned result, see the description of MatchMethod in CreateCCRuleTemplate.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeCCRuleTemplate
&RegionId=cn-hangzhou
&Id=1
&PageSize=20
&PageNumber=1
```

Sample success responses

XML format

```
<DescribeCCRuleTemplateResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"items": [{"id": 1, "name": "cc-policy-test", "version": 40, "is_enabled": true, "match_method": {"target_type": "CIDR", "period": null, "limit": null, "scope": "URL Prefix", "policy": "www.taobao.com", "scheme": "http"}, "action": {"action": "forbid"}, "create_time": "1594627307", "expire_period": 10, "execution_number": 0, "template_type": "manual", "is_inaccurate": false, "dry_run": false}], "total": 1}</Result>
</DescribeCCRuleTemplateResponse>
```

JSON format


```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "items": [
      {
        "id": 1,
        "name": "cc-policy-test",
        "version": 40,
        "is_enabled": true,
        "match_method": {
          "target_type": "CIDR",
          "period": null,
          "limit": null,
          "scope": "URL Prefix",
          "policy": "www.taobao.com",
          "scheme": "http"
        },
        "action": {
          "action": "forbid"
        },
        "create_time": "1594627307",
        "expire_period": 10,
        "execution_number": 0,
        "template_type": "manual",
        "is_inaccurate": false,
        "dry_run": false
      }
    ],
    "total": 1
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.2.2. CreateCCRuleTemplate

Creates an HTTP flood protection rule.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateCCRuleTemplate	The operation that you want to perform. Set the value to CreateCCRuleTemplate.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Name	String	Yes	cc-rule-1	The name of the HTTP flood protection rule.
TemplateType	String	Yes	auto	The type of the rule. Valid values: manual: limits requests based on specific IP addresses or sessions. auto: limits requests that meet specific conditions.
Enable	Boolean	No	true	Specifies whether to enable the rule. Default value: true . Valid values: true: enables the HTTP flood protection rule. false: disables the HTTP flood protection rule.
RuleMode	Boolean	No	false	The mode of the rule. Default value: false . Valid values: true: monitors specific requests. false: blocks specific requests.

Parameter	Type	Required	Example	Description
RuleList	RepeatList	No	["192.168.XX.XX", "192.168.XX.XX/24"]	The IP addresses, classless inter-domain routing (CIDR) blocks, or sessions. If you set TemplateType to manual to limit requests from known sources, this parameter is required
RuleAction	Json	Yes	{"action": "forbid", "limit_rate_limit": 1, "limit_rate_period": 5}	The action on requests. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • action: the action on the requests. This field is required. Data type: string. Valid values: forbid and Limit Rate. The value forbid indicates that the system blocks requests. The value Limit Rate indicates that the system limits the number of requests to handle over a specific period. • limit_rate_limit: the number of requests to handle over a specific period. If you set action to Limit Rate, this field is required. Data type: integer. Valid values: any non-zero positive integer. • limit_rate_period: the period in which the system limits the number of requests to handle. If you set action to Limit Rate, this field is required. Data type: integer. Valid values: any non-zero positive integer.
FuzzyCount	Boolean	No	false	The statistical aggregation method to count requests. Default value: false. Valid values: • true: counts requests with the most occurrence. • false: counts all requests.

Parameter	Type	Required	Example	Description
MatchMethod	Json	Yes	<pre>{"scope": "URL Prefix", "limit": "10", "period": "5", "target_type": "CIDR", "policy": "www.aliyun.com", "scheme": "http"}</pre>	The match conditions. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • scope: the statistical aggregation method to count requests. This field is required. Data type: string. Valid values: URL Prefix, URL, and All. The value URL Prefix indicates that the requests containing the specific URL prefix are counted. The value URL indicates that the requests containing the specific URL are counted. The value All indicates that all requests are counted. • limit: the number of requests to handle over a specific period. If you set RuleAction.action to Limit Rate, this field is required. Data type: integer. Valid values: any non-zero positive integer. • period: the period in which the system limits the number of requests to handle. If you set RuleAction.action to Limit Rate, this field is required. Data type: integer. Valid values: any non-zero positive integer. • target_type: the object type based on which the system limits requests. This field is required. Data type: string. Valid values: CIDR and Session. • policy: the URL or URL prefix based on which requests are counted. If you set scope to URL Prefix or URL, this field is required. • policy: the scheme based on which requests are counted. If you set scope to URL Prefix or URL, this field is required. Valid values: http and https.
ExpirePeriod	Integer	No	86400	The validity period after the rule is triggered. Unit: seconds.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		The returned information.
^L TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task. The ID of the task.
^L Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
^L TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
^L StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
^L SuccessCode	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Parameter	Type	Example	Description
Result	String	<pre>{ "id": 17, "name": "test-cc-rule-1", "version": 65, "is_enabled": true, "match_method": { "target_type": "CIDR", "period": 5, "limit": 5, "scope": "All" }, "action": { "action": "forbid" }, "create_time": "1598337034", "expire_period": null, "execution_number": 0, "template_type": "auto", "is_inaccurate": false, "dry_run": false }</pre>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=CreateCCRuleTemplate
&RegionId=cn-hangzhou
&Name=cc-rule-1
&TemplateType=auto
&Enable=true
&RuleMode=true
&RuleList.1=192.168.XX.XX
&RuleAction={"action":"forbid","limit_rate_limit":1,"limit_rate_period":5}
&FuzzyCount=true
&MatchMethod={"scope":"URL Prefix","limit":"10","period":5,"target_type":"CIDR","policy":"www.aliyun.com","scheme":"http"}
&ExpirePeriod=86400
```

Sample success responses

[XML](#) [format](#)

```
<CreateCCRuleTemplateResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"id": 17, "name": "test-cc-rule-1", "version": 65, "is_enabled": true, "match_method": {"target_type": "CIDR", "period": 5, "limit": 5, "scope": "All"}, "action": {"action": "forbid"}, "create_time": "1598337034", "expire_period": null, "execution_number": 0, "template_type": "auto", "is_inaccurate": false, "dry_run": false}</Result>
  </TaskStatus>
</CreateCCRuleTemplateResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": {"id": 17, "name": "test-cc-rule-1", "version": 65, "is_enabled": true, "match_method": {"target_type": "CIDR", "period": 5, "limit": 5, "scope": "All"}, "action": {"action": "forbid"}, "create_time": "1598337034", "expire_period": null, "execution_number": 0, "template_type": "auto", "is_inaccurate": false, "dry_run": false}
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.2.3. EditCCRuleTemplate

Modifies a specific HTTP flood protection rule.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	EditCCRuleTemplate	The operation that you want to perform. Set the value to EditCCRuleTemplate.
RegionId	String	Yes	cn-hangzhou	The ID of the region.

Parameter	Type	Required	Example	Description
Id	Integer	No	1	The ID of the HTTP flood protection rule. You can call the DescribeCCRuleTemplate operation to query the IDs of HTTP flood protection rules.
Name	String	Yes	cc-rule-1	The name of the HTTP flood protection rule.
Enable	Boolean	No	true	Specifies whether to enable the rule. Default value: true . Valid values: • true: enables the HTTP flood protection rule. • false: disables the HTTP flood protection rule.
RuleMode	Boolean	No	false	The mode of the rule. Default value: false . Valid values: • true: monitors specific requests. • false: blocks specific requests.

Parameter	Type	Required	Example	Description
RuleAction	Json	Yes	<pre>{"action": "forbid", "limit_rate_limit": 1, "limit_rate_period": 5}</pre>	The action on requests. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • action: the action on the requests. This field is required. Data type: string. Valid values: forbid and Limit Rate. The value forbid indicates that the system blocks requests. The value Limit Rate indicates that the system limits the number of requests to handle over a specific period. • limit_rate_limit: the number of requests to handle over a specific period. If you set action to Limit Rate, this field is required. Data type: integer. Valid values: any non-zero positive integer. • limit_rate_period: the period in which the system limits the number of requests to handle. If you set action to Limit Rate, this field is required. Data type: integer. Valid values: any non-zero positive integer.
FuzzyCount	Boolean	No	false	The statistical aggregation method to count requests. Default value: false. Valid values: • true: counts requests with the most occurrence. • false: counts all requests.

Parameter	Type	Required	Example	Description
MatchMethod	Json	Yes	<pre>{ "scope": "URL Prefix", "limit": "10", "period": 5, "target_type": "CIDR", "policy": "www.aliyun.com", "scheme": "http" }</pre>	The match conditions. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • scope: the statistical aggregation method to count requests. This field is required. Data type: string. Valid values: URL Prefix, URL, and All. The value URL Prefix indicates that the requests containing the specific URL prefix are counted. The value URL indicates that the requests containing the specific URL are counted. The value All indicates that all requests are counted. • limit: the number of requests to handle over a specific period. If you set RuleAction.action to Limit Rate, this field is required. Data type: integer. Valid values: any non-zero positive integer. • period: the period in which the system limits the number of requests to handle. If you set RuleAction.action to Limit Rate, this field is required. Data type: integer. Valid values: any non-zero positive integer. • target_type: the object type based on which the system limits requests. This field is required. Data type: string. Valid values: CIDR and Session. • policy: the URL or URL prefix based on which requests are counted. If you set scope to URL Prefix or URL, this field is required. • policy: the scheme based on which requests are counted. If you set scope to URL Prefix or URL, this field is required. Valid values: http and https.
ExpirePeriod	Integer	No	86400	The validity period after the rule is triggered. Unit: seconds.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
^L TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
^L Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
^L TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
^L StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
^L SuccessCode	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Parameter	Type	Example	Description
Result	String	<pre>{ "id": 1, "name": "test-cc-rule-1", "version": 65, "is_enabled": true, "match_method": { "target_type": "CIDR", "period": 5, "limit": 5, "scope": "All"}, "action": { "action": "forbid"}, "create_time": "1598337034", "expire_period": null, "execution_number": 0, "template_type": "auto", "is_inaccurate": false, "dry_run": false} </pre>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=EditCCRuleTemplate
&RegionId=cn-hangzhou
&Id=1
&Name=cc-rule-1
&Enable=true
&RuleMode=true
&RuleAction={"action":"forbid","limit_rate_limit":1,"limit_rate_period":5}
&FuzzyCount=true
&MatchMethod={"scope":"URL Prefix","limit":"10","period":5,"target_type":"CIDR","policy":"www.aliyun.com","scheme":"http"}
&ExpirePeriod=86400
```

Sample success responses

XML format

```
<EditCCRuleTemplateResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"id": 1, "name": "test-cc-rule-1", "version": 65, "is_enabled": true, "match_method": {"target_type": "CIDR", "period": 5, "limit": 5, "scope": "All"}, "action": {"action": "forbid"}, "create_time": "1598337034", "expire_period": null, "execution_number": 0, "template_type": "auto", "is_inaccurate": false, "dry_run": false}</Result>
  </TaskStatus>
</EditCCRuleTemplateResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": {"id": 1, "name": "test-cc-rule-1", "version": 65, "is_enabled": true, "match_method": {"target_type": "CIDR", "period": 5, "limit": 5, "scope": "All"}, "action": {"action": "forbid"}, "create_time": "1598337034", "expire_period": null, "execution_number": 0, "template_type": "auto", "is_inaccurate": false, "dry_run": false}
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.2.4. ToggleCCRuleTemplate

Enables or disables a specific HTTP flood protection rule.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ToggleCCRuleTemplate	The operation that you want to perform. Set the value to ToggleCCRuleTemplate.
RegionId	String	Yes	cn-hangzhou	The ID of the region.

Parameter	Type	Required	Example	Description
IdList	RepeatList	Yes	[1, 2]	The ID of the HTTP flood protection rule. You can enter multiple IDs. You can call the DescribeCCRuleTemplate operation to query the IDs of HTTP flood protection rules.
ToggleAction	String	Yes	disable	Specifies the status of the HTTP flood protection rule. Valid values: • enable • disable

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
LTaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
LTime	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
LTaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
LStatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
LSuccessCode	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=ToggleCCRuleTemplate
&RegionId=cn-hangzhou
&IdList.1=1
&ToggleAction=disable
```

Sample success responses

XML format

```
<ToggleCCRuleTemplateResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</ToggleCCRuleTemplateResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": "[\"Website-related configuration generation\", \"Policy-related configuration generation\"]",
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.2.5. DeleteCCRuleTemplate

Deletes a specific HTTP flood protection rule.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteCCRuleTemplate	The operation that you want to perform. Set the value to DeleteCCRuleTemplate.

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-hangzhou	The ID of the region.
IdList	RepeatList	Yes	[1, 2]	The ID of the HTTP flood protection rule. You can enter multiple IDs. You can call the DescribeCCRuleTemplate operation to query the IDs of HTTP flood protection rules.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
└Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
└TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
└StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
└SuccessCode	String	1	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DeleteCCRuleTemplate
&RegionId=cn-hangzhou
&IdList.1=1
```

Sample success responses

XML format

```
<DeleteCCRuleTemplateResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</DeleteCCRuleTemplateResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.2.6. ClearCCRestrictionList

Removes the restricted users in a specific HTTP flood protection rule.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ClearCCRestrictionList	The operation that you want to perform. Set the value to ClearCCRestrictionList.
RegionId	String	Yes	cn-hangzhou	The ID of the region.

Parameter	Type	Required	Example	Description
CCRuleTemplateId	Integer	Yes	35	The ID of the HTTP flood protection rule. You can call the DescribeCCRuleTemplate operation to query the IDs of HTTP flood protection rules.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
LTaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
LTime	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
LTaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
LStatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
LSuccessCode	String	1	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=ClearCCRestrictionList
&RegionId=cn-hangzhou
&CCRuleTemplateId=35
```

Sample success responses

XML format

```
<ClearCCRestrictionListResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</ClearCCRestrictionListResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": "[\"Website-related configuration generation\", \"Policy-related configuration generation\"]",
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.2.7. DescribeCCWhitelist

Queries the information about HTTP flood protection whitelists.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeCCWhitelist	The operation that you want to perform. Set the value to DescribeCCWhitelist.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	No	1	The ID of the HTTP flood protection whitelist.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: 10.

Parameter	Type	Required	Example	Description
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.
TargetTypeFilter	RepeatList	No	["CIDR", "Session"]	The type to filter whitelists. You can enter multiple types. Valid values: - CIDR - Session
CommentFilter	RepeatList	No	["cc-whitelist-1", "cc-whitelist-2"]	The remarks to filter whitelists. You can enter multiple remarks.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"items": [{"id": 5, "target": "10.12.XX.XX", "target_type": "CIDR", "target_ip_group": null, "comment": "", "create_time": "1594627457"}], "total": 1}	

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeCCWhitelist
&RegionId=cn-hangzhou
&PageSize=10
&PageNumber=1
&TargetTypeFilter.1=CIDR
&CommentFilter.1=cc-whitelist-1
```

Sample success responses

XML format

```
<DescribeCCWhitelistResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"items": [{"id": 5, "target": "10.12.XX.XX", "target_type": "CIDR", "target_ip_group": null, "comment": "", "create_time": "1594627457"}], "total": 1}</Result>
</DescribeCCWhitelistResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"items": [{"id": 5, "target": "10.12.XX.XX", "target_type": "CIDR", "target_ip_group": null, "comment": "", "create_time": "1594627457"}], "total": 1}
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.2.8. CreateCCWhitelist

Creates an HTTP flood protection whitelist.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateCCWhitelist	The operation that you want to perform. Set the value to CreateCCWhitelist.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
TargetType	String	Yes	auto	The type of the HTTP flood protection whitelist. Valid values: - CIDR - Session
Comment	String	Yes	Whitelist-192168100200	The remarks of the whitelist.
TargetList	RepeatList	Yes	["10.10.XX.XX", "10.10.XX.XX/24"]	The IP address, CIDR block, or session in the whitelist. You can enter multiple IP addresses, CIDR blocks, or sessions.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		The returned information.
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task. The ID of the task.
└Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
└TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
└StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
└SuccessCode	String	1	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.
└Result	String	{["id": null, "target": "10.10.XX.XX", "target_type": "CIDR", "target_ip_group": null, "comment": "", "create_time": "1598337455"]}	The information about the created whitelist.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=CreateCCWhitelist
&RegionId=cn-hangzhou
&TargetType=CIDR
&Comment=Whitelist-192168100200
&TargetList.1=10.10.XX.XX
```

Sample success responses

XML format

```
<CreateCCWhitelistResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>[{ "id": null, "target": "10.10.XX.XX", "target_type": "CIDR", "target_ip_group": null, "comment": "", "create_time": "1598337455" }]</Result>
  </TaskStatus>
</CreateCCWhitelistResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": "[\"Website-related configuration generation\", \"Policy-related configuration generation\"]",
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": "[{ \"id\": null, \"target\": \"10.10.XX.XX\", \"target_type\": \"CIDR\", \"target_ip_group\": null, \"comment\": \"\", \"create_time\": \"1598337455\" }]"
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.2.9. DeleteCCWhitelist

Deletes a specific HTTP flood protection whitelist.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteCCWhitelist	The operation that you want to perform. Set the value to DeleteCCWhitelist.
RegionId	String	Yes	cn-hangzhou	The ID of the region.

Parameter	Type	Required	Example	Description
IdList	RepeatList	Yes	[1, 2]	The ID of the HTTP flood protection whitelist. You can enter multiple IDs. You can call the DescribeCCWhitelist operation to query the IDs of HTTP flood protection whitelists.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task. The ID of the task.
└Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
└TaskList	String	["Generated website configurations", "Generated policy configurations"]	The descriptions of the task. This value is returned only for asynchronous tasks.
└StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
└SuccessCode	String	1	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DeleteCCWhitelist
&RegionId=cn-hangzhou
&IdList.1=1
```

Sample success responses

XML format

```
<DeleteCCWhitelistResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Generated website configurations", "Generated policy configurations"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</DeleteCCWhitelistResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": "[\"Generated website configurations\", \"Generated policy configurations\"]",
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3. Custom rules

9.3.1. DescribePolicyRule

Queries the information about custom rules.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePolicyRule	The operation that you want to perform. Set the value to DescribePolicyRule.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	No	1	The ID of the custom rule.

Parameter	Type	Required	Example	Description
Enable	Boolean	No	true	Specifies whether to filter custom rules.
RiskLevelFilter	RepeatList	No	[1, 2]	The risk level to filter rules. You can enter multiple values. Valid values: • 0: no risks • 1: low • 2: medium • 3: high
AttackTypeFilter	RepeatList	No	[1, 2, 3]	The attack type to filter rules. You can enter multiple values. Valid values: -1 (non-web attacks), 0 (SQL injection attacks), 1 (XSS attacks), 2 (CSRF attacks), 3 (SSRF attacks), 4 (denial of service attacks), 5 (backdoors), 6 (deserialization attacks), 7 (code executions), 8 (code injection attacks), 9 (command injection attacks), 10 (file uploads), 11 (file inclusions), 12 (redirection attacks), 13 (improper authorization), 14 (information leaks), 15 (unauthorized access), 16 (insecure configurations), 17 (XXE attacks), 18 (XPath injection attacks), 19 (LDAP injection attacks), 20 (path traversal attacks), 21 (scanners), 22 (horizontal authorization bypass), 23 (vertical authorization bypass), 24 (file modifications), 25 (file reads), 26 (file deletions), 27 (logical errors), 28 (CRLF injection attacks), 29 (template injection attacks), 30 (click hijacking attacks), 31 (buffer overflows), 32 (integer overflows), 33 (format string attacks), 34 (race condition attacks), 61 (timeout errors), and 62 (unknown attacks).

Parameter	Type	Required	Example	Description
PolicyActionFilter	RepeatList	No	["deny", "allow"]	The action to filter rules. You can enter multiple values. Valid values: deny, allow, dry_run, and modify_module. The value dry_run indicates the rules that monitor requests. The value modify_module indicates the rules that are intended for detection modules.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	<pre>{ "id": 19, "version": "19@time-1594205736", "websites": [1746], "target": "logic_expr", "pattern": { "\$AND": { "infix": { "decoded_path": "asda" } }, "action": "deny", "is_enabled": true, "is_expired": false, "comment": "1111", "attack_type": -1, "log_option": "Persistence", "create_time": "1594205736", "last_update_time": "1594205736", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": null, "risk_level": 0, "extra": null } }</pre>	The returned result of the request. For more information about the pattern parameter in the returned result, see Fields in match conditions.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribePolicyRule
&RegionId=cn-hangzhou
&Id=1
&Enable=true
&RiskLevelFilter.1=1
&AttackTypeFilter.1=1
&PolicyActionFilter.1=deny
```

Sample success responses

XML format

```
<DescribePolicyRuleResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>[{ "id": 19, "version": "19@time-1594205736", "websites": [1746], "target": "logic_expr", "pattern": { "$AND": [ { "infix": { "decoded_path": "asda" } } ] }, "action": "deny", "is_enabled": true, "is_expired": false, "comment": "1111", "attack_type": -1, "log_option": "Persistence", "create_time": "1594205736", "last_update_time": "1594205736", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": null, "risk_level": 0, "extra": null } ]</Result>
</DescribePolicyRuleResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": [ { "id": 19, "version": "19@time-1594205736", "websites": [1746], "target": "logic_expr", "pattern": { "$AND": [ { "infix": { "decoded_path": "asda" } } ] }, "action": "deny", "is_enabled": true, "is_expired": false, "comment": "1111", "attack_type": -1, "log_option": "Persistence", "create_time": "1594205736", "last_update_time": "1594205736", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": null, "risk_level": 0, "extra": null } ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.2. CreatePolicyRule

Creates a custom rule to deny, allow, or monitor requests.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreatePolicyRule	The operation that you want to perform. Set the value to CreatePolicyRule.

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-hangzhou	The ID of the region.
ForbiddenPageConfig	Json	No	<pre>{"status_code": 405, "action": "response", "path": ""}</pre>	The configurations to block requests. The value is a string that consists of a JSON struct. The JSON struct contains the following fields: • status_code: the status code. This field is required. Data type: integer. Valid values: 200, 301, 302, 307, 400, 403, 404, 501, and 502. • action: the method to respond to the requests. This field is required. Data type: string. Valid values: redirect and response. The value redirect indicates that the system redirects the requests. The value response indicates that the system returns specific content. If status_code is set to 301 or 302, set action to redirect. If status_code is set to a different value, set action to response. • path: the destination address for redirection. Data type: string. If action is set to redirect, this field is required. Otherwise, leave this field empty.
Comment	String	Yes	policy-rule-1	The description of the rule.
Enable	Boolean	No	true	Specifies whether to enable the custom rule. Default value: true .
PolicyAction	String	Yes	deny	The action on requests. Valid values: deny , allow , and dry_run . The value dry_run indicates that the system allows and monitors the requests.

Parameter	Type	Required	Example	Description
AttackType	Integer	Yes	-1	The attack type in the custom rule. Valid values: -1 (non-web attacks), 0 (SQL injection attacks), 1 (XSS attacks), 2 (CSRF attacks), 3 (SSRF attacks), 4 (denial of service attacks), 5 (backdoors), 6 (deserialization attacks), 7 (code executions), 8 (code injection attacks), 9 (command injection attacks), 10 (file uploads), 11 (file inclusions), 12 (redirection attacks), 13 (improper authorization), 14 (information leaks), 15 (unauthorized access), 16 (insecure configurations), 17 (XXE attacks), 18 (XPath injection attacks), 19 (LDAP injection attacks), 20 (path traversal attacks), 21 (scanners), 22 (horizontal authorization bypass), 23 (vertical authorization bypass), 24 (file modifications), 25 (file reads), 26 (file deletions), 27 (logical errors), 28 (CRLF injection attacks), 29 (template injection attacks), 30 (click hijacking attacks), 31 (buffer overflows), 32 (integer overflows), 33 (format string attacks), 34 (race condition attacks), 61 (timeout errors), and 62 (unknown attacks).
RiskLevel	Integer	Yes	3	The risk level in the custom rule. Valid values: 0: no risks 1: low 2: medium 3: high
LogOption	String	Yes	log	The logging operation. Valid values: log and drop . The value log indicates that matched requests are logged. The value drop indicates that matched requests are not logged.
Pattern	Json	Yes	<pre>{"\$AND": [{"\$NOT": [{"infix": {"urlpath": "admin"}}]}</pre>	The match conditions. The value is a string that consists of a JSON struct. For information about the JSON struct, see Fields in match conditions .

Parameter	Type	Required	Example	Description
ExpireTime	Long	No	1594982409	The UNIX timestamp of when the custom rule expires. Unit: seconds. If you leave this parameter empty or set it to 0, the rule does not expire.
WebsiteldList	RepeatList	No	[1, 2]	The ID of the website to which the custom rule applies. You can enter multiple IDs. You can call the DescribePolicyRule operation to query the IDs of websites.

Fields in match conditions

The match conditions of a custom rule are specified in a string that consists of a JSON struct. The JSON struct contains the following fields:

```

{
  "$AND": [
    //The match conditions. This field is required. Data type: list. You can specify the field value in the following default format:
    {
      "Operator": //This field is required. Data type: string.
      "Match field": "Match content", //This field is required. Data type: string. If the match content is a value, use this format.
      "Match field": { //This field is required. Data type: string.
        //If the match content is a key-value pair, use this format.
        "key": "Match field", //This field is required. Data type: string.
        "value": "Match content" //This field is required. Data type: string.
      }
    },
    {
      "$NOT": //If the operator is prefixed with not, this field is required. Data type: string. You must specify the field value in the following default format:
      {
        "Operator": { //This field is required. Data type: string.
          "Match field": "Match content", //This field is required. Data type: string. If the match content is a value, use this format. If the operator is prefixed with not, remove not.
          "Match field": { //This field is required. Data type: string. If the match content is a key-value pair, use this format. If the operator is prefixed with not, remove not.
            "key": "Match field", //This field is required. Data type: string.
            "value": "Match content" //This field is required. Data type: string.
          }
        }
      }
    ]
  ]
}

```

Operators and match fields

The following lists describe the operators and match fields. The system does not support custom operators or match fields.

• Operators

- **infix**: inclusion
- **notinfix**: exclusion
- **str**: exact match
- **notstr**: fuzzy match
- **re**: match based on regular expressions
- **notre**: reverse match based on regular expressions

- **Match fields and match content types**

- **urlpath**: the original URI in the request, which is not decoded. Match content type: value.
Example: `/query%20news?q=1%20or%201%3D1`.
- **decoded_path**: the path after decoding. Match content type: value. The path is the content from the forward slash (/) to the question mark (?) in the URL. The path must be URL-decoded.
Example: `/query news`.
- **decoded_query**: the query string in the URL. Match content type: value. The query string is the content from the question mark (?) to the end of the URL. The query string must be URL-decoded.
Example: `q=1` or `1=1`.
- **query**: the parameters in the query string. Match content type: key-value pair. The parameters are obtained by splitting the content from the question mark (?) to the end of the URL into key-value pairs. The parameters must be URL-decoded. Example: Parameter name `q` Parameter value `1` or `1=1`.
- **method**: the method of the HTTP request. Match content type: value. Example: `GET` or `POST`.
- **host**: the Host field in the HTTP request header. Match content type: value.
- **cookie_raw**: the Cookie field that is not split into key-value pairs. Match content type: value.
- **cookie**: the cookies that are obtained by splitting the Cookie field into key-value pairs. Match content type: key-value pair.
- **user_agent**: The User-Agent field in the HTTP request header. Match content type: value.
- **referer**: the Referrer field in the HTTP request header. Match content type: value.
- **content_type**: the Content-Type field in the HTTP request header. Match content type: value.
- **remote_addr**: the actual IP address of the client. Match content type: value.
- **x_forwarded_for**: the X-Forwarded-For field in the HTTP request header. Match content type: value.
- **origin**: the Origin field in the HTTP request header. Match content type: value.
- **session**: the Session content. You can configure this field only after you configure the session settings for your website. Match content type: value.
- **request_header**: the complete header of the original HTTP request. Match content type: value.
- **custom_header**: the HTTP request header that is split into key-value pairs. Match content type: key-value pair.
- **request_header_length**: the length of the HTTP request header. Match content type: value.
- **request_body_length**: the length of the HTTP request body. Match content type: value.
- **form**: the form data in the HTTP request body. The data must be split into key-value pairs and URL-decoded. Match content type: key-value pair.
- **file_name**: the name of the file that you want to upload in the HTTP request. Match content type: value.
- **request_body**: the complete body of the HTTP request. Match content type: value.
- **response_status**: the HTTP status code that the server returns. Match content type: value.
- **response_header**: the HTTP response header that is split into key-value pairs. Match content type: key-value pair.
- **response_body**: the complete response that the server returns. Match content type: value.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task. The ID of the task.
└Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
└TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
└StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
└SuccessCode	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Parameter	Type	Example	Description
L-Result	String	<pre>{ "id": 57, "version": "57@time-1598336466", "websites": [781], "target": "logic_expr", "pattern": { "\$AND": [{ "infix": { "urlpath": "abcedfgh" } }] }, "action": "deny", "is_enabled": true, "is_expired": false, "comment": "test-policy-rule-1", "attack_type": -1, "log_option": "Persistence", "create_time": "1598336466", "last_update_time": "1598336466", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": null, "risk_level": 0, "extra": null }</pre>	The information about the added website.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=CreatePolicyRule
&RegionId=cn-hangzhou
&ForbiddenPageConfig={"status_code":405,"action":"response","path":""}
&Comment=policy-rule-1
&Enable=true
&PolicyAction=deny
&AttackType=-1
&RiskLevel=3
&LogOption=log
&Pattern={"$AND":[{"$NOT":[{"infix":{"urlpath":"admin"}}]}}
&ExpireTime=1594982409
&WebsiteIdList.1=1
```

Sample success responses

XML format

```
<CreatePolicyRuleResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"id": 57, "version": "57@time-1598336466", "websites": [781], "target": "logic_expr", "pattern": {"$AND": [{"infix": {"urlpath": "abcdefgh"}}]}, "action": "deny", "is_enabled": true, "is_expired": false, "comment": "test-policy-rule-1", "attack_type": -1, "log_option": "Persistence", "create_time": "1598336466", "last_update_time": "1598336466", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": null, "risk_level": 0, "extra": null}</Result>
  </TaskStatus>
</CreatePolicyRuleResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": {"id": 57, "version": "57@time-1598336466", "websites": [781], "target": "logic_expr", "pattern": {"$AND": [{"infix": {"urlpath": "abcdefgh"}}]}, "action": "deny", "is_enabled": true, "is_expired": false, "comment": "test-policy-rule-1", "attack_type": -1, "log_option": "Persistence", "create_time": "1598336466", "last_update_time": "1598336466", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": null, "risk_level": 0, "extra": null}
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.3. EditPolicyRule

Modifies a specific custom rule.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	EditPolicyRule	The operation that you want to perform. Set the value to EditPolicyRule.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
ForbiddenPageConfig	Json	No	<pre>{"status_code": 405, "action": "response", "path": ""}</pre>	The configurations to block requests. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • status_code: the status code in the responses. This field is required. Data type: integer. Valid values: 200, 301, 302, 307, 400, 403, 404, 501, and 502. • action: the method to respond to the requests. This field is required. Data type: string. Valid values: redirect and response. The value redirect indicates that the system redirects the requests. The value response indicates that the system returns specific content. If status_code is set to 301 or 302, set action to redirect. If status_code is set to another value, set action to response. • path: the destination address for redirection. Data type: string. If action is set to redirect, this field is required. In other cases, leave this field unspecified.
Comment	String	Yes	policy-rule-1	The remarks.
Enable	Boolean	No	true	Specifies whether to enable the custom rule. Default value: true .
PolicyAction	String	Yes	deny	The action on requests. Valid values: deny , allow , and dry_run . The value dry_run indicates that the system allows and monitors the requests.

Parameter	Type	Required	Example	Description
AttackType	Integer	Yes	-1	The attack type in the custom rule. Valid values: -1 (non-web attacks), 0 (SQL injection attacks), 1 (XSS attacks), 2 (CSRF attacks), 3 (SSRF attacks), 4 (denial of service attacks), 5 (backdoors), 6 (deserialization attacks), 7 (code executions), 8 (code injection attacks), 9 (command injection attacks), 10 (file uploads), 11 (file inclusions), 12 (redirection attacks), 13 (improper authorization), 14 (information leaks), 15 (unauthorized access), 16 (insecure configurations), 17 (XXE attacks), 18 (XPath injection attacks), 19 (LDAP injection attacks), 20 (path traversal attacks), 21 (scanners), 22 (horizontal authorization bypass), 23 (vertical authorization bypass), 24 (file modifications), 25 (file reads), 26 (file deletions), 27 (logical errors), 28 (CRLF injection attacks), 29 (template injection attacks), 30 (click hijacking attacks), 31 (buffer overflows), 32 (integer overflows), 33 (format string attacks), 34 (race condition attacks), 61 (timeout errors), and 62 (unknown attacks).

Parameter	Type	Required	Example	Description
RiskLevel	Integer	Yes	3	Valid values: 0: no risks 1: low 2: medium 3: high
LogOption	String	Yes	log	The logging operation. Valid values: log and drop . The value log indicates that matched requests are logged. The value drop indicates that matched requests are not logged.
Pattern	Json	Yes	<pre>{"\$AND": [{"\$NOT": [{"infix": {"urlpath": "admin"}]}]}</pre>	The match conditions. This parameter is a string consisting of JSON structs. For information about the JSON structs, see Fields in match conditions .
ExpireTime	Long	No	1594982409	The expiration time of the custom rule. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC. If you leave this parameter unspecified or set it to 0, the rule does not expire.
WebsiteldList	RepeatList	No	[1, 2]	The ID of the website to which the custom rule applies. You can enter multiple IDs. You can call the DescribePolicyRule operation to query the IDs of websites.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task. The ID of the task.

Parameter	Type	Example	Description
L-Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
L-TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
L-StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
L-SuccessCode	String	1	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.
L-Result	String	{ "id": 57, "version": "57@time-1598336466", "websites": [781], "target": "logic_expr", "pattern": {"\$AND": [{"infix": {"urlpath": "abcdefgh"}}]}, "action": "deny", "is_enabled": true, "is_expired": false, "comment": "test-policy-rule-1", "attack_type": -1, "log_option": "Persistence", "create_time": "1598336466", "last_update_time": "1598336466", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": null, "risk_level": 0, "extra": null }	The information about the added website.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=EditPolicyRule
&RegionId=cn-hangzhou
&Id=1
&ForbiddenPageConfig={"status_code":405,"action":"response","path":""}
&Comment=policy-rule-1
&Enable=true
&PolicyAction=deny
&AttackType=-1
&RiskLevel=3
&LogOption=log
&Pattern={"$AND":[{"$NOT":[{"infix":{"urlpath":"admin"}}]}}
&ExpireTime=1594982409
&WebsiteIdList.1=1
```

Sample success responses

XML format

```
<EditPolicyRuleResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"id": 57, "version": "57@time-1598336466", "websites": [781], "target": "logic_expr", "pattern": {"$AND": [{"infix": {"urlpath": "abcdefgh"}}]}, "action": "deny", "is_enabled": true, "is_expired": false, "comment": "test-policy-rule-1", "attack_type": -1, "log_option": "Persistence", "create_time": "1598336466", "last_update_time": "1598336466", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": null, "risk_level": 0, "extra": null}</Result>
  </TaskStatus>
</EditPolicyRuleResponse>
```

JSON format


```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": {
      "id": 57,
      "version": "57@time-1598336466",
      "websites": [781],
      "target": {
        "logic_expr": {
          "pattern": {
            "$AND": [
              {
                "infix": {
                  "urlpath": "abcedfgh"
                }
              }
            ]
          },
          "action": "deny",
          "is_enabled": true,
          "is_expired": false,
          "comment": "test-policy-rule-1",
          "attack_type": -1,
          "log_option": "Persistence",
          "create_time": "1598336466",
          "last_update_time": "1598336466",
          "expire_time": null,
          "is_global": false,
          "forbidden_page_config": null,
          "priority": 0,
          "module_management": null,
          "risk_level": 0,
          "extra": null
        }
      }
    }
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.4. TogglePolicyRule

Enables or disables a specific custom rule.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	TogglePolicyRule	The operation that you want to perform. Set the value to TogglePolicyRule.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
IdList	RepeatList	Yes	[1, 2]	The ID of the custom rule. You can enter multiple IDs. You can call the DescribePolicyRule operation to query the IDs of custom rules.
ToggleAction	String	Yes	disable	Specifies the status of the custom rule. Valid values: - enable - disable

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		The returned information.
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
└Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
└TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
└StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
└SuccessCode	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=TogglePolicyRule
&RegionId=cn-hangzhou
&IdList.1=1
&ToggleAction=disable
```

Sample success responses

XML format

```
<TogglePolicyRuleResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</TogglePolicyRuleResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.5. DeletePolicyRule

Deletes a specific custom rule.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeletePolicyRule	The operation that you want to perform. Set the value to DeletePolicyRule.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
IdList	RepeatList	Yes	[1, 2]	The ID of the custom rule. You can enter multiple IDs. You can call the DescribePolicyRule operation to query the IDs of custom rules.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
L-TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
L-Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
L-TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
L-StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
L-SuccessCode	String	1	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DeletePolicyRule
&RegionId=cn-hangzhou
&IdList.1=1
```

Sample success responses

XML format

```
<DeletePolicyRuleResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</DeletePolicyRuleResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.6. EditPolicyRulePriority

Modifies the priorities of custom rules for a specific website. The rules in PolicyRuleIdList are prioritized in descending order.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	EditPolicyRulePriority	The operation that you want to perform. Set the value to EditPolicyRulePriority.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
WebsiteId	Integer	No	101	The ID of the website for which you want to modify custom rule priorities.

Parameter	Type	Required	Example	Description
PolicyRuleIdList	Integer	No	10	The ID of the custom rule. You can enter multiple IDs. You can call the DescribePolicyRule operation to query the IDs of custom rules.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
└Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
└TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
└StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
└SuccessCode	└Result	String	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.
└Result	String	{"website": 12, "policy_rule_ids": [12, 17]}	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=EditPolicyRulePriority
&RegionId=cn-hangzhou
&WebsiteId=101
&PolicyRuleIdList.1=3
```

Sample success responses

XML format

```
<EditPolicyRulePriorityResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"website": 12, "policy_rule_ids": [12, 17]}</Result>
  </TaskStatus>
</EditPolicyRulePriorityResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": "{\"website\": 12, \"policy_rule_ids\": [12, 17]}"
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.7. GenerateFalsePositiveRuleCorrection

Generates correction rules based on false positives.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	GenerateFalsePositiveRuleCorrection	The operation that you want to perform. Set the value to GenerateFalsePositiveRuleCorrection.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
LogId	String	Yes	1e23f8d1-a9d2-4dd9-b7e2-424b9832183f	The ID of the log.
RuleId	String	Yes	m_sqli	The ID of the rule.
UrlPath	String	Yes	/	The path of the URL.
Host	String	Yes	www.taobao.com	The domain name.
SourceIpAddresses	String	Yes	10.17.XX.XX	The source IP address.
DestinationIp	String	Yes	43.17.XX.XX	The destination IP address.
DestinationPort	Integer	Yes	80	The destination port.
RequestBody	String	No		The body of the request.
RawRequestHeader	String	Yes	GET /? id=1 or 1=1 HTTP/1.1\r\nUser-Agent: curl/7.29.0\r\nAccept: /\r\nhost: www.taobao.com\r\n\r\n	The original header of the request.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	<pre>{"pattern": {"decoded_path": "/", "host": "40.73.XX.XX", "remote_addr": "139.162.XX.XX"}, "action": "allow", "comment": "Clear false positives - 550877"}</pre>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[ RegionId].aliyuncs.com/?Action=GenerateFalsePositiveRuleCorrection  
&RegionId=cn-hangzhou  
&LogId=1e23f8d1-a9d2-4dd9-b7e2-424b9832183f  
&RuleId=m_sqli  
&UrlPath=/  
&Host=www.taobao.com  
&SourceIpAddress=10.17.XX.XX  
&DestinationIp=43.17.XX.XX  
&DestinationPort=80  
&RequestBody=  
&RawRequestHeader=GET /? id=1 or 1=1 HTTP/1.1\r\nUser-Agent: curl/7.29.0\r\nAccept: */*\r\nhost: www.taobao.com\r\n\r\n
```

Sample success responses

XML format

```
<GenerateFalsePositiveRuleCorrectionResponse>  
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>  
  <Result>{"pattern": {"decoded_path": "/", "host": "40.73.XX.XX", "remote_addr": "139.16  
2.XX.XX"}, "action": "allow", "comment": "Clear false positives - 550877"}</Result>  
</GenerateFalsePositiveRuleCorrectionResponse>
```

JSON format

```
{  
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",  
  "Result": {"pattern": {"decoded_path": "/", "host": "40.73.XX.XX", "remote_add  
r": "139.162.XX.XX"}, "action": "allow", "comment": "Clear false positives - 5508  
77"}  
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.8. CreateDetectionModuleRule

Creates a rule for detection module control.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateDetectionModuleRule	The operation that you want to perform. Set the value to CreateDetectionModuleRule.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
ForbiddenPageConfig	Json	No	<pre>{"status_code": 405, "action": "response", "path": ""}</pre>	The configurations to block requests. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • status_code: the status code in the responses. This field is required. Data type: integer. Valid values: 200, 301, 302, 307, 400, 403, 404, 501, and 502. • action: the method to respond to the requests. This field is required. Data type: string. Valid values: redirect and response. The value redirect indicates that the system redirects the requests. The value response indicates that the system returns specific content. If status_code is set to 301 or 302, set action to redirect. If status_code is set to another value, set action to response. • path: the destination address for redirection. Data type: string. If action is set to redirect, this field is required. In other cases, leave this field unspecified.
Comment	String	Yes	detection-module-rule-1	The remarks.
PolicyAction	String	Yes	modify_module	The action in the rule. Set the value to modify_module , which indicates detection module control.
Enable	Boolean	No	true	Specifies whether to enable the rule for detection module control. Default value: true .

Parameter	Type	Required	Example	Description
ModuleManagement	Json	Yes	<pre>{"disabled": ["m_xss"],"enabled":[]}</pre>	Specifies whether to enable detection module control. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: disabled: disables detection module control. This field is required. Data type: list. enabled: enables detection module control. This field is required. Data type: list. For more information about detection modules, see Module description .
LogOption	String	Yes	log	The logging operation. Valid values: log and drop . The value log indicates that matched requests are logged. The value drop indicates that matched requests are not logged.
Pattern	Json	Yes	<pre>{"\$AND": [{"\$NOT": [{"infix": {"urlpath":"admin"}]}]}</pre>	The match conditions. This parameter is a string consisting of JSON structs. For more information about the JSON structs, see Fields in match conditions .
ExpireTime	Long	No	1594982409	The expiration time of the custom rule. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC. If you leave this parameter unspecified or set it to 0, the rule does not expire.
WebsiteldList	RepeatList	No	[1, 2]	The ID of the website to which the custom rule applies. You can enter multiple IDs. You can call the DescribePolicyRule operation to query the IDs of websites.

Module description

Code	Description
m_sqli	SQL Injection Detection Module

Code	Description
m_xss	XSS Detection Module
m_rule	Intelligence Module
m_csrf	CSRF Detection Module
m_ssrf	SSRF Detection Module
m_php_unserialize	PHP Deserialization Detection Module
m_java_unserialize	Java Deserialization Detection Module
m_file_upload	File Upload Attack Detection Module
m_file_include	File Inclusion Attack Detection Module
m_php_code_injection	PHP Code Injection Detection Module
m_java	Java Code Injection Detection Module
m_cmd_injection	Command Injection Detection Module
m_response	Server Response Detection Module
m_scanner	Robot Detection Module
m_asp_code_injection	ASP Code Injection Detection Module
m_ssti	Template Injection Detection Module

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task. The ID of the task.
Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Example	Description
<code>L-TaskList</code>	String	<code>["Website-related configuration generation", "Policy-related configuration generation"]</code>	The descriptions of the task. This value is returned only for asynchronous tasks.
<code>L-StatusMessage</code>	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
<code>L-SuccessCode</code>	String	1	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.
<code>L-Result</code>	String	<code>{ "id": 58, "version": "58@time-1598338353", "websites": [], "target": "logic_expr", "pattern": {"\$AND": [{"infix": {"urlpath": "1234567"}}]}, "action": "modify_module", "is_enabled": true, "is_expired": false, "comment": "test-module-rule-1", "attack_type": -1, "log_option": "Persistence", "create_time": "1598338348", "last_update_time": "1598338353", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": {"disabled": ["m_sqli"], "enabled": []}, "risk_level": 0, "extra": null }</code>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=CreateDetectionModuleRule
&RegionId=cn-hangzhou
&ForbiddenPageConfig={"status_code":405,"action":"response","path":""}
&Comment=detection-module-rule-1
&PolicyAction=modify_module
&Enable=true
&ModuleManagement={"disabled":["m_xss"],"enabled":[]}
&LogOption=log
&Pattern={"$AND":[{"$NOT":[{"infix":{"urlpath":"admin"}}]}}
&ExpireTime=1594982409
&WebsiteIdList.1=1
```

Sample success responses

XML format

```
<CreateDetectionModuleRuleResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"id": 58, "version": "58@time-1598338353", "websites": [], "target": "logic_expr", "pattern": {"$AND": [{"infix": {"urlpath": "1234567"}}]}, "action": "modify_module", "is_enabled": true, "is_expired": false, "comment": "test-module-rule-1", "attack_type": -1, "log_option": "Persistence", "create_time": "1598338348", "last_update_time": "1598338353", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": {"disabled": ["m_sqli"], "enabled": []}, "risk_level": 0, "extra": null}</Result>
  </TaskStatus>
</CreateDetectionModuleRuleResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": {
      "id": 58,
      "version": "58@time-1598338353",
      "websites": [],
      "target": {
        "logic_expr": {
          "pattern": {
            "$AND": [
              {
                "infix": {
                  "urlpath": "1234567"
                }
              }
            ]
          },
          "action": "modify_module",
          "is_enabled": true,
          "is_expired": false,
          "comment": "test-module-rule-1",
          "attack_type": -1,
          "log_option": "Persistence",
          "create_time": "1598338348",
          "last_update_time": "1598338353",
          "expire_time": null,
          "is_global": false,
          "forbidden_page_config": null,
          "priority": 0,
          "module_management": {
            "disabled": [
              "mysqli"
            ],
            "enabled": [],
            "risk_level": 0,
            "extra": null
          }
        }
      }
    }
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.9. EditDetectionModuleRule

Modifies a specific rule for detection module control.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	EditDetectionModuleRule	The operation that you want to perform. Set the value to EditDetectionModuleRule.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	Yes	1	The ID of the rule for detection module control.

Parameter	Type	Required	Example	Description
ForbiddenPageConfig	Json	No	<pre>{"status_code": 405, "action": "response", "path": ""}</pre>	The configurations to block requests. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • status_code: the status code in the responses. This field is required. Data type: integer. Valid values: 200, 301, 302, 307, 400, 403, 404, 501, and 502. • action: the method to respond to the requests. This field is required. Data type: string. Valid values: redirect and response. The value redirect indicates that the system redirects the requests. The value response indicates that the system returns specific content. If status_code is set to 301 or 302, set action to redirect. If status_code is set to another value, set action to response. • path: the destination address for redirection. Data type: string. If action is set to redirect, this field is required. In other cases, leave this field unspecified.
Comment	String	Yes	detection-module-rule-1	The remarks.
PolicyAction	String	Yes	modify_module	The action in the rule. Set the value to modify_module , which indicates detection module control.
Enable	Boolean	No	true	Specifies whether to enable the rule for detection module control. Default value: true .

Parameter	Type	Required	Example	Description
ModuleManagement	Json	Yes	<pre>{"disabled": ["m_xss"],"enabled":[]}</pre>	Specifies whether to enable detection module control. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • disabled: disables detection module control. This field is required. Data type: list. • enabled: enables detection module control. This field is required. Data type: list. For more information about detection modules, see Module description.
LogOption	String	Yes	log	The logging operation. Valid values: log and drop . The value log indicates that matched requests are logged. The value drop indicates that matched requests are not logged.
Pattern	Json	Yes	<pre>{"\$AND": [{"\$NOT": [{"infix": {"urlpath":"admin"}]}]}</pre>	The match conditions. This parameter is a string consisting of JSON structs. For more information about the JSON structs, see Fields in match conditions .
ExpireTime	Long	No	1594982409	The expiration time of the custom rule. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC. If you leave this parameter unspecified or set it to 0, the rule does not expire.
WebsiteldList	RepeatList	No	[1, 2]	The ID of the website to which the custom rule applies. You can enter multiple IDs. You can call the DescribePolicyRule operation to query the IDs of websites.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
^L TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task. The ID of the task.
^L Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
^L TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
^L StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
^L SuccessCode	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Parameter	Type	Example	Description
Result	String	<pre>{ "id": 58, "version": "58@time-1598338353", "websites": [], "target": "logic_expr", "pattern": { "\$AND": [{ "infix": { "urlpath": "1234567" } }] }, "action": "modify_module", "is_enabled": true, "is_expired": false, "comment": "test-module-rule-1", "attack_type": -1, "log_option": "Persistence", "create_time": "1598338348", "last_update_time": "1598338353", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": { "disabled": ["m_sqli"], "enabled": [] }, "risk_level": 0, "extra": null }</pre>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=EditDetectionModuleRule
&RegionId=cn-hangzhou
&Id=1
&ForbiddenPageConfig={"status_code":405,"action":"response","path":""}
&Comment=detection-module-rule-1
&PolicyAction=modify_module
&Enable=true
&ModuleManagement={"disabled":["m_xss"],"enabled":[]}
&LogOption=log
&Pattern={"$AND":[{"$NOT":[{"infix":{"urlpath":"admin"}}]}}
&ExpireTime=1594982409
&WebsiteIdList.1=1
```

Sample success responses

XML format

```
<EditDetectionModuleRuleResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"id": 58, "version": "58@time-1598338353", "websites": [], "target": "logic_expr", "pattern": {"$AND": [{"infix": {"urlpath": "1234567"}}]}, "action": "modify_module", "is_enabled": true, "is_expired": false, "comment": "test-module-rule-1", "attack_type": -1, "log_option": "Persistence", "create_time": "1598338348", "last_update_time": "1598338353", "expire_time": null, "is_global": false, "forbidden_page_config": null, "priority": 0, "module_management": {"disabled": ["m_sqli"], "enabled": []}, "risk_level": 0, "extra": null}</Result>
  </TaskStatus>
</EditDetectionModuleRuleResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": "{\"id\": 58, \"version\": \"58@time-1598338353\", \"websites\": [], \"target\": \"logic_expr\", \"pattern\": {\"$AND\": [{\"infix\": {\"urlpath\": \"1234567\"}}]}, \"action\": \"modify_module\", \"is_enabled\": true, \"is_expired\": false, \"comment\": \"test-module-rule-1\", \"attack_type\": -1, \"log_option\": \"Persistence\", \"create_time\": \"1598338348\", \"last_update_time\": \"1598338353\", \"expire_time\": null, \"is_global\": false, \"forbidden_page_config\": null, \"priority\": 0, \"module_management\": {\"disabled\": [\"m_sqli\"], \"enabled\": []}, \"risk_level\": 0, \"extra\": null}"
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.10. EditPolicyRuleWebsiteBinding

Modifies the binding relationship between a specific website and its custom rules.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	EditPolicyRuleWebsiteBinding	The operation that you want to perform. Set the value to EditPolicyRuleWebsiteBinding.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
WebsiteId	Integer	No	101	The ID of the website for which you want to modify the binding relationship.
PolicyRuleIdList	Integer	No	10	The ID of the custom rule. You can enter multiple IDs. You can call the DescribePolicyRule operation to query the IDs of custom rules.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
└Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
└TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
└StatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.

Parameter	Type	Example	Description
<code>L-SuccessCode</code>	<code>L-Result</code>	String	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.
<code>L-Result</code>	String	<code>{"website": 12, "policy_rule_ids": [12, 17]}</code>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=EditPolicyRuleWebsiteBinding
&RegionId=cn-hangzhou
&WebsiteId=101
&PolicyRuleIdList.1=3
```

Sample success responses

XML format

```
<EditPolicyRuleWebsiteBindingResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
    <Result>{"website": 12, "policy_rule_ids": [12, 17]}</Result>
  </TaskStatus>
</EditPolicyRuleWebsiteBindingResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect.",
    "Result": "{\"website\": 12, \"policy_rule_ids\": [12, 17]}"
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.3.11. DeletePolicyRuleWebsiteBinding

Deletes the binding relationship between a specific website and specific custom rules.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeletePolicyRuleWebsiteBinding	The operation that you want to perform. Set the value to DeletePolicyRuleWebsiteBinding.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
WebsiteId	Integer	No	101	The ID of the website for which you want to modify the binding relationship.
PolicyRuleIdList	Integer	No	10	The ID of the custom rule. You can enter multiple IDs. You can call the DescribePolicyRule operation to query the IDs of custom rules.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
└Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Example	Description
LTaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
LStatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
LSuccessCode	LResult	String	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DeletePolicyRuleWebsiteBinding
&RegionId=cn-hangzhou
&WebsiteId=101
&PolicyRuleId=12
```

Sample success responses

XML format

```
<DeletePolicyRuleWebsiteBindingResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</DeletePolicyRuleWebsiteBindingResponse>
```

JSON format


```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": "[\"Website-related configuration generation\", \"Policy-related configuration generation\"]",
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.4. Protection policies

9.4.1. DescribePolicyGroup

Queries the information about protection policies.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePolicyGroup	The operation that you want to perform. Set the value to DescribePolicyGroup.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	No	101	The ID of the protection policy.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
		DescribePolicyGroup: [{"id": 6, "is_timeout_enabled": true, "name": "Default Policy Strategy", "create_time": "1589275411", "last_update_time": "1594607697", "is_default": true, "modules_state": true, "response_detection_state": true, "response_detection_max_body_size": 1024, "response_detection_generate_log": false, "request_detection_max_body_size": 1024, "detection_timeout_threshold": 1000, "log_detection_timeout_event": true, "forbidden_page_config": {"action": "response",	

Parameter	Type	Example	Description
Result	String	<pre> "status_code": 405, "path": ""}, "modules_detection_config": {"m_cmd_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_scanner": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"robot_types": ["scanner"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_include": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_code_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_response": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"error_types": ["directory indexing", "SQL execution error", "server exception"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_sql": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_non_injection_sql": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_csrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_upload": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_rule": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"info_leak_types": ["test file", "backup file", "code repository", "server sensitive file"], "check_info_leak_by_rsp": false, "detection_config": ["detect_phpinfo", "detect_admin_page", </pre>	The returned result of the request.

Parameter	Type	Description
		Example <pre>"detect_backdoor", "detect_php_vuln", "detect_nginx", "detect_dedecms", "detect_apache", "detect_xml", "detect_struts2", "detect_java_vuln", "detect_php168", "detect_wordpress", "detect_directory_traversal", "detect_iis", "detect_gogs_gitea", "detect_thinkphp", "detect_jenkins", "detect_ecshop", "detect_nexus", "detect_drupal", "detect_ghostscript", "detect_atlassian", "detect_weblogic", "detect_coremail", "detect_phpcms", "detect_spring", "detect_southidc", "detect_fastjson", "detect_tbk_dvr", "detect_joomla", "detect_ecology_oa", "detect_jackson", "detect_xstream", "detect_activemq", "detect_solr"}}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny", "m_ssrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_xss": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_complete_html": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_asp_code_injection": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}, "m_ssti": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}, "misc_detection_config": {"decode_config": {"decode_methods": ["url decode", "JSON", "base64", "hex", "eval", "XML", "utf7"]}}}}</pre>

Examples

Sample requests

```
https://semawaf.[ RegionId].aliyuncs.com/?Action=DescribePolicyGroup
&RegionId=cn-hangzhou
&Id=1
```

Sample success responses

XML format

```
<DescribePolicyGroupResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>DescribePolicyGroup": [{"id": 6, "is_timeout_enabled": true, "name": "Default
Policy Strategy", "create_time": "1589275411", "last_update_time": "1594607697", "is_defaul
t": true, "modules_state": true, "response_detection_state": true, "response_detection_max
body_size": 1024, "response_detection_generate_log": false, "request_detection_max_body_siz
e": 1024, "detection_timeout_threshold": 1000, "log_detection_timeout_event": true, "forbid
den_page_config": {"action": "response", "status_code": 405, "path": ""}, "modules_detectio
n_config": {"m_cmd_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_r
isk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_ris
```

```

k_enable_log": 1, "high_risk_action": "deny"}, "m_scanner": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"robot_types": ["scanner"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_include": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_code_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_response": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"error_types": ["directory indexing", "SQL execution error", "server exception"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_sqli": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_non_injection_sql": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_csrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_upload": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_rule": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"info_leak_types": ["test file", "backup file", "code repository", "server sensitive file"], "check_info_leak_by_rsp": false, "detection_configure": ["detect_phpinfo", "detect_admin_page", "detect_backdoor", "detect_php_vuln", "detect_nginx", "detect_dedecms", "detect_apache", "detect_xml", "detect_struts2", "detect_java_vuln", "detect_php168", "detect_wordpress", "detect_directory_traversal", "detect_iis", "detect_gogs_gitea", "detect_thinkphp", "detect_jenkins", "detect_ecshop", "detect_nexus", "detect_drupal", "detect_ghostscript", "detect_atlassian", "detect_weblogic", "detect_coremail", "detect_phpcms", "detect_spring", "detect_southidc", "detect_fastjson", "detect_tbk_dvr", "detect_joomla", "detect_ecology_oa", "detect_jackson", "detect_xstream", "detect_activemq", "detect_solr"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_ssrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_xss": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_complete_html": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_asp_code_injection": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}, "m_ssti": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}, "misc_detection_config": {"decode_config": {"decode_methods": ["url decode", "JSON", "base64", "hex", "eval", "XML", "utf7"]}}}]</Result>
</DescribePolicyGroupResponse>

```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": "DescribePolicyGroup": {
    "id": 6,
    "is_timeout_enabled": true,
    "name": "Default Policy Strategy",
    "create_time": "1589275411",
    "last_update_time": "1594607697",
    "is_default": true,
    "modules_state": true,
    "response_detection_state": true,
    "response_detection_max_body_size": 1024,
    "response_detection_generate_log": false,
    "request_detection_max_body_size": 1024,
    "detection_timeout_threshold": 1000,
    "log_detection_timeout_event": true,
    "forbidden_page_config": {
      "action": "response",
      "status_code": 405,
      "path": ""
    },
    "modules_detection_config": {
      "m_cmd_injection": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "disabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_scanner": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "robot_types": ["scanner"]
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "disabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_file_include": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_php_code_injection": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "detect_upload_file": true
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_response": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "error_types": ["directory indexing", "SQL execution error", "server exception"]
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "disabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_java_unserialize": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_sql_i": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "detect_non_injection_sql": true
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_csrf": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_java": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "detect_upload_file": true
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_file_upload": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_php_unserialize": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_rule": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "info_leak_types": ["test file", "backup file", "code repository", "server sensitive file"],
          "check_info_leak_by_rsp": false,
          "detection_configure": [
            "detect_phpinfo",
            "detect_admin_page",
            "detect_backdoor",
            "detect_php_vuln",
            "detect_nginx",
            "detect_dedecms",
            "detect_apache",
            "detect_xml",
            "detect_struts2",
            "detect_java_vuln",
            "detect_php168",
            "detect_wordpress",
            "detect_directory_traversal",
            "detect_iis",
            "detect_gogs_gitea",
            "detect_thinkphp",
            "detect_jenkins",
            "detect_ecshop",
            "detect_nexus",
            "detect_drupal",
            "detect_ghostscript",
            "detect_atlassian",
            "detect_weblogic",
            "detect_coremall",
            "detect_phpcms",
            "detect_spring",
            "detect_southidc",
            "detect_fastjson",
            "detect_tbk_dvr",
            "detect_joomla",
            "detect_ecology_oa",
            "detect_jackson",
            "detect_xstream",
            "detect_activemq",
            "detect_solr"
          ]
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      }
    }
  }
}
```

```
um_risk_action\": \"continue\", \"state\": \"enabled\", \"medium_risk_enable_log\": 1, \"high_risk_action\": \"deny\"}, \"m_ssrf\": {\"low_risk_enable_log\": 1, \"high_risk_enable_log\": 1, \"low_risk_action\": \"continue\", \"medium_risk_action\": \"continue\", \"state\": \"enabled\", \"medium_risk_enable_log\": 1, \"high_risk_action\": \"deny\"}, \"m_xss\": {\"low_risk_enable_log\": 1, \"high_risk_enable_log\": 1, \"detect_config\": {\"detect_complete_html\": true}, \"low_risk_action\": \"continue\", \"medium_risk_action\": \"continue\", \"state\": \"enabled\", \"medium_risk_enable_log\": 1, \"high_risk_action\": \"deny\"}, \"m_asp_code_injection\": {\"state\": \"disabled\", \"high_risk_action\": \"deny\", \"high_risk_enable_log\": 1, \"medium_risk_action\": \"continue\", \"medium_risk_enable_log\": 1, \"low_risk_action\": \"continue\", \"low_risk_enable_log\": 1, \"detect_config\": {}}, \"m_ssti\": {\"state\": \"disabled\", \"high_risk_action\": \"deny\", \"high_risk_enable_log\": 1, \"medium_risk_action\": \"continue\", \"medium_risk_enable_log\": 1, \"low_risk_action\": \"continue\", \"low_risk_enable_log\": 1, \"detect_config\": {}}, \"misc_detection_config\": {\"decode_config\": {\"decode_methods\": [\"url decode\", \"JSON\", \"base64\", \"hex\", \"eval\", \"XML\", \"utf7\"]}}}]\"}
```

Error codes

For a list of error codes, see [Error codes](#).

9.4.2. CreatePolicyGroup

Creates a protection policy.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	CreatePolicyGroup	The operation that you want to perform. Set the value to CreatePolicyGroup.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
PolicyGroupName	String	Yes	Loose protection policy	The name of the protection policy.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
		{\"id\": 75, \"is_timeout_enabled\": true, \"name\": \"policy-group-test\", \"create_time\": \"1594695152\", \"last_update_time\": \"1594695152\", \"is_default\": false, \"modules_state\": true, \"response_detection_state\": true, \"response_detection_max_body_size\": 1024, \"response_detection_generate_log\": false, \"request_detection_max_body_size\": 1024,	

Parameter	Type	Example	Description
Result	String	<pre> "detection_timeout_threshold": 1000, "log_detection_timeout_event": true, "forbidden_page_config": {"action": "response", "status_code": 405, "path": ""}, "modules_detection_config": {"m_cmd_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_scanner": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"robot_types": ["scanner"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_include": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_code_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_response": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"error_types": ["directory indexing", "SQL execution error", "server exception"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_sql": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_non_injection_sql": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_csrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_upload": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_rule": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"info_leak_types": ["test file", "backup </pre>	The returned result of the request.

Parameter	Type	Example	Description
		<pre>file", "code repository", "server sensitive file"], "check_info_leak_by_rsp": false, "detection_configure": ["detect_phpinfo", "detect_admin_page", "detect_backdoor", "detect_php_vuln", "detect_nginx", "detect_dedecms", "detect_apache", "detect_xml", "detect_struts2", "detect_java_vuln", "detect_php168", "detect_wordpress", "detect_directory_traversal", "detect_iis", "detect_gogs_gitea", "detect_thinkphp", "detect_jenkins", "detect_ecshop", "detect_nexus", "detect_drupal", "detect_ghostscript", "detect_atlassian", "detect_weblogic", "detect_coremail", "detect_phpcms", "detect_spring", "detect_southidc", "detect_fastjson", "detect_tbk_dvr", "detect_joomla", "detect_ecology_oa", "detect_jackson", "detect_xstream", "detect_activemq", "detect_solr"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_ssrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_xss": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_complete_html": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_asp_code_injection": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}, "m_ssti": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}, "misc_detection_config": {"decode_config": {"decode_methods": ["url decode", "JSON", "base64", "hex", "eval", "XML", "utf7"]}}}</pre>	

Examples

Sample requests

```
https://semawaf.[ RegionId].aliyuncs.com/?Action=CreatePolicyGroup
&RegionId=cn-hangzhou
&PolicyGroupName=Loose protection policy
```

Sample success responses

XML format

```
<CreatePolicyGroupResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"id": 75, "is_timeout_enabled": true, "name": "policy-group-test", "create_time": "1594695152", "last_update_time": "1594695152", "is_default": false, "modules_state": true, "response_detection_state": true, "response_detection_max_body_size": 1024, "response_detection_generate_log": false, "request_detection_max_body_size": 1024, "detection_timeout_threshold": 1000, "log_detection_timeout_event": true, "forbidden_page_config": {"action":
```



```
"response", "status_code": 405, "path": "", "modules_detection_config": {"m_cmd_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_scanner": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"robot_types": ["scanner"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_include": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_code_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_response": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"error_types": ["directory indexing", "SQL execution error", "server exception"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_sqli": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_non_injection_sql": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_csrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_upload": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_rule": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"info_leak_types": ["test file", "backup file", "code repository", "server sensitive file"], "check_info_leak_by_rsp": false, "detection_configure": ["detect_phpinfo", "detect_admin_page", "detect_backdoor", "detect_php_vuln", "detect_nginx", "detect_dedecms", "detect_apache", "detect_xml", "detect_struts2", "detect_java_vuln", "detect_php168", "detect_wordpress", "detect_directory_traversal", "detect_iis", "detect_gogs_gitea", "detect_thinkphp", "detect_jenkins", "detect_ecshop", "detect_nexus", "detect_drupal", "detect_ghostscript", "detect_atlassian", "detect_weblogic", "detect_coremail", "detect_phpcms", "detect_spring", "detect_southidc", "detect_fastjson", "detect_tbk_dvr", "detect_joomla", "detect_ecology_oa", "detect_jackson", "detect_xstream", "detect_activemq", "detect_solr"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_ssrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_xss": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_complete_html": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_asp_code_injection": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}, "m_ssti": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}}, "misc_detection_config": {"decode_config": {"decode_methods": ["url decode", "JSON", "base64", "hex", "eval", "XML", "utf7"]}}}</Result></CreatePolicyGroupResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "id": 75,
    "is_timeout_enabled": true,
    "name": "policy-group-test",
    "create_time": "1594695152",
    "last_update_time": "1594695152",
    "is_default": false,
    "modules_state": true,
    "response_detection_state": true,
    "response_detection_max_body_size": 1024,
    "response_detection_generate_log": false,
    "request_detection_max_body_size": 1024,
    "detection_timeout_threshold": 1000,
    "log_detection_timeout_event": true,
    "forbidden_page_config": {
      "action": "response",
      "status_code": 405,
      "path": ""
    },
    "modules_detection_config": {
      "m_cmd_injection": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "disabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_scanner": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "robot_types": ["scanner"]
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "disabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_file_include": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_php_code_injection": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "detect_upload_file": true
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_response": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "error_types": ["directory indexing", "SQL execution error", "server exception"]
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "disabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_java_unserialize": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_sql": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "detect_non_injection_sql": true
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_csrf": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_java": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "detect_upload_file": true
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_file_upload": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_php_unserialize": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "low_risk_action": "continue",
        "medium_risk_action": "continue",
        "state": "enabled",
        "medium_risk_enable_log": 1,
        "high_risk_action": "deny"
      },
      "m_rule": {
        "low_risk_enable_log": 1,
        "high_risk_enable_log": 1,
        "detect_config": {
          "info_leak_types": ["test file", "backup file", "code repository", "server sensitive file"],
          "check_info_leak_by_rsp": false,
          "detection_configure": [
            "detect_phpinfo",
            "detect_admin_page",
            "detect_backdoor",
            "detect_php_vuln",
            "detect_nginx",
            "detect_dedecms",
            "detect_apache",
            "detect_xml",
            "detect_struts2",
            "detect_java_vuln",
            "detect_php168",
            "detect_wordpress",
            "detect_directory_traversal",
            "detect_iis",
            "detect_gogs_gitea",
            "detect_thinkphp",
            "detect_jenkins",
            "detect_ecshop",
            "detect_nexus",
            "detect_drupal",
            "detect_ghosts_cript",
            "detect_atlassian",
            "detect_weblogic",
            "detect_coremail",
            "detect_phpcms",
            "detect_spring",
            "detect_southidc",
            "detect_fastjson",
            "detect_tbk_dvr",
            "detect_joomla",
            "detect_ecology_oa",
            "detect_jackson",
            "detect_xstream",
            "detect_activemq",
            "detect_solr"
          ]
        },
        "low_risk_action": "continue",
        "medium_risk_action": "continue"
      }
    }
  }
}
```

```
"", \"state\": \"enabled\", \"medium_risk_enable_log\": 1, \"high_risk_action\": \"deny\"},
\"m_ssrf\": {\"low_risk_enable_log\": 1, \"high_risk_enable_log\": 1, \"low_risk_action\":
\"continue\", \"medium_risk_action\": \"continue\", \"state\": \"enabled\", \"medium_risk_e
nable_log\": 1, \"high_risk_action\": \"deny\"}, \"m_xss\": {\"low_risk_enable_log\": 1, \"
high_risk_enable_log\": 1, \"detect_config\": {\"detect_complete_html\": true}, \"low_risk_
action\": \"continue\", \"medium_risk_action\": \"continue\", \"state\": \"enabled\", \"med
ium_risk_enable_log\": 1, \"high_risk_action\": \"deny\"}, \"m_asp_code_injection\": {\"sta
te\": \"disabled\", \"high_risk_action\": \"deny\", \"high_risk_enable_log\": 1, \"medium_r
isk_action\": \"continue\", \"medium_risk_enable_log\": 1, \"low_risk_action\": \"continue\
", \"low_risk_enable_log\": 1, \"detect_config\": {}}, \"m_ssti\": {\"state\": \"disabled\"
, \"high_risk_action\": \"deny\", \"high_risk_enable_log\": 1, \"medium_risk_action\": \"co
ntinue\", \"medium_risk_enable_log\": 1, \"low_risk_action\": \"continue\", \"low_risk_enab
le_log\": 1, \"detect_config\": {}}, \"misc_detection_config\": {\"decode_config\": {\"dec
ode_methods\": [\"url decode\", \"JSON\", \"base64\", \"hex\", \"eval\", \"XML\", \"utf7\"]
}}}"
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.4.3. EditPolicyGroup

Modifies a specific protection policy.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	EditPolicyGroup	The operation that you want to perform. Set the value to EditPolicyGroup.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	Yes	1	The ID of the protection policy. You can call the DescribePolicyGroup operation to query the IDs of protection policies.

Parameter	Type	Required	Example	Description
ForbiddenPageConfig	Json	Yes	<code>{"status_code":405,"action":"response","path":""}</code>	The configurations to block requests. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • status_code: the status code in the responses. This field is required. Data type: integer. Valid values: 200, 301, 302, 307, 400, 403, 404, 501, and 502. • action: the method to respond to the requests. This field is required. Data type: string. Valid values: redirect and response. The value redirect indicates that the system redirects the requests. The value response indicates that the system returns specific content. If status_code is set to 301 or 302, set action to redirect. If status_code is set to another value, set action to response. • path: the destination address for redirection. Data type: string. If action is set to redirect, this field is required. In other cases, leave this field unspecified.

Parameter	Type	Required	Example	Description
ResponseDetection	Boolean	Yes	true	Specifies whether to enable response detection. Valid values: • true • false
ResponseDetectionLog	Boolean	No	false	Specifies whether to record response content in attack detection logs. Default value: false . Valid values: • true • false
ResponseDetectionMaxBody	Integer	Yes	1024	The maximum size of a response body for detection. Unit: KB.
RequestDetectionMaxBody	Integer	Yes	1024	The maximum size of a request body for detection. Unit: KB.
DetectionTimeout	Boolean	Yes	true	Specifies whether to enable detection timeout. Valid values: • true • false
DetectionTimeoutThreshold	Integer	Yes	1000	The detection timeout period. Unit: ms. If the DetectionTimeout parameter is set to true , this parameter is required.
DetectionTimeoutLog	Boolean	Yes	true	Specifies whether to record detection timeout in attack detection logs. If the DetectionTimeout parameter is set to false , this parameter is unavailable.
				The configurations of the attack detection module.

Parameter	Type	Required	Example	You can call the DescribePolicyGroup operation to query the configurations. We recommend that you use the configurations in the query result. The value is a string that consists of a JSON struct. The JSON struct contains the following fields: • detect_config: the configurations of the attack detection module. This field is required. Data type: string. • high_risk_action: the action on requests when the upper threshold for blocking is triggered. This field is required. Data type: string. Valid values: deny and continue. The value deny indicates that requests are blocked. The value continue indicates that requests are not blocked. If the high_risk_action, medium_risk_action, and low_risk_action fields are all set to deny, all requests are blocked. If all the three fields are set to continue, no requests are blocked. • medium_risk_action: the action on requests when the medium threshold for blocking is triggered. This field is required. Data
			<pre> {"m_cmd_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_scanner": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"robot_types": ["scanner"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_include": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_code_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_response": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"error_types": ["directory indexing", "SQL </pre>	

Parameter	Type	Required	Example	Description
DetectionModule Config	Json	Yes	<pre> execution error", "server exception"}], "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_sql": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_non_injection_sql": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_csrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_upload": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_rule": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, </pre>	type: string. Valid values: deny and continue. The value deny indicates that requests are blocked. The value continue indicates that requests are not blocked. If the high_risk_action and medium_risk_action fields are set to deny and the low_risk_action field is set to continue, high-risk and medium-risk requests are blocked. If all the three fields are set to continue, no requests are blocked. • low_risk_action: the action on requests when the lower threshold for blocking is triggered. This field is required. Data type: string. Valid values: deny and continue. The value deny indicates that requests are blocked. The value continue indicates that requests are not blocked. If the high_risk_action field is set to deny and the medium_risk_action and low_risk_action fields are set to continue, high-risk requests are blocked. If all the three fields are set to continue, no requests are blocked.

Parameter	Type	Required	Example	Description
			<pre> "detect_config": { "info_leak_types": ["test file", "backup file", "code repository", "server sensitive file"], "check_info_leak_by_rsp": false, "detection_configure": ["detect_phpinfo", "detect_admin_page", "detect_backdoor", "detect_php_vuln", "detect_nginx", "detect_dedecms", "detect_apache", "detect_xml", "detect_struts2", "detect_java_vuln", "detect_php168", "detect_wordpress", "detect_directory_traversal", "detect_iis", "detect_gogs_gitea", "detect_thinkphp", "detect_jenkins", "detect_ecshop", "detect_nexus", "detect_drupal", "detect_ghostscript", "detect_atlassian", "detect_weblogic", "detect_coremail", "detect_phpcms", "detect_spring", "detect_southidc", "detect_fastjson", "detect_tbk_dvr", "detect_joomla", "detect_ecology_oa", "detect_jackson", "detect_xstream", "detect_activemq", "detect_solr"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny", "m_ssrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_xss": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": { "detect_complete_html": true, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_asp_code_injection": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, </pre>	• high_risk_enable_log: specifies whether to enable logging when the upper threshold is triggered. This field is required. Data type: integer. Valid values: 0 and 1. The value 0 indicates that logs are not recorded. The value 1 indicates that logs are recorded. If the high_risk_enable_log, medium_risk_enable_log, and low_risk_enable_log fields are all set to 1, all logs are recorded. If all the three fields are set to 0, no logs are recorded. • medium_risk_enable_log: specifies whether to enable logging when the medium threshold is triggered. This field is required. Data type: integer. Valid values: 0 and 1. The value 0 indicates that logs are not recorded. The value 1 indicates that logs are recorded. If the high_risk_enable_log and medium_risk_enable_log fields are set to 1 and the low_risk_enable_log field is set to 0, high-risk and medium-risk logs are recorded. If all the three fields are set to 0, no logs are recorded. • low_risk_enable_log: specifies

Parameter	Type	Required	Example	Description
			<pre> "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}, "m_ssti": {"state": "disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}</pre>	whether to enable logging when the lower threshold is triggered. This field is required. Data type: integer. Valid values: 0 and 1. The value 0 indicates that logs are not recorded. The value 1 indicates that logs are recorded. If the high_risk_enable_log field is set to 1 and the medium_risk_enable_log and low_risk_enable_log fields are set to 0, high-risk logs are recorded. If all the three fields are set to 0, no logs are recorded. • state: specifies whether to enable the attack detection module. This field is required. Data type: string. Valid values: enabled and disabled.

Parameter	Type	Required	Example	Description
MiscModuleConfig	Json	Yes	<pre>{ "decode_config": { "decode_methods": ["url_decode", "JSON", "base64", "hex", "eval", "XML", "PHP deserialize", "utf7"] } }</pre>	The configurations of other modules. The value is a string that consists of JSON arrays. The value is a string that consists of a JSON struct. The JSON struct contains the following fields: decode_methods: This field is required. Valid values: url_decode (URL decoding), JSON (JSON parsing), base64 (Base64 decoding), hex (hexadecimal conversion), eval (slash unescaping), XML (XML parsing), PHP deserialize (parsing of PHP serialized objects), and utf7 (UTF-7 decoding).

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		The returned information.
TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task. The ID of the task.
Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Example	Description
LTaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
LStatusMessage	String	The configuration is in effect.	The status message of the task. You can ignore this reserved parameter.
LSuccessCode	String	1	The status code of the task. Valid values: • 0: The task fails. • 1: The task is successful. • 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=EditPolicyGroup
&RegionId=cn-hangzhou
&Id=1
&ForbiddenPageConfig={"status_code":405,"action":"response","path":""}
&ResponseDetection=true
&ResponseDetectionLog=true
&ResponseDetectionMaxBody=1024
&RequestDetectionMaxBody=1024
&DetectionTimeout=true
&DetectionTimeoutThreshold=1000
&DetectionTimeoutLog=true
&DetectionModuleConfig={"m_cmd_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_scanner": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"robot_types": ["scanner"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_include": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_code_injection": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_response": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"error_types": ["directory indexing", "SQL execution error", "server exception"]}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java_unserialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_sql_i": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_non_injection_sql": true}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_csrf": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "disabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}}
```

```
{
  "_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "state":
  "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_java": {"low_risk_e
  nable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_upload_file": true}, "l
  ow_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium
  risk_enable_log": 1, "high_risk_action": "deny"}, "m_file_upload": {"low_risk_enable_log":
  1, "high_risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continu
  e", "state": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_php_un
  serialize": {"low_risk_enable_log": 1, "high_risk_enable_log": 1, "low_risk_action": "conti
  nue", "medium_risk_action": "continue", "state": "enabled", "medium_risk_enable_log": 1, "h
  igh_risk_action": "deny"}, "m_rule": {"low_risk_enable_log": 1, "high_risk_enable_log": 1,
  "detect_config": {"info_leak_types": ["test file", "backup file", "code repository", "serve
  r sensitive file"], "check_info_leak_by_rsp": false, "detection_configure": ["detect_phpinfo",
  "detect_admin_page", "detect_backdoor", "detect_php_vuln", "detect_nginx", "detect_dede
  cms", "detect_apache", "detect_xml", "detect_struts2", "detect_java_vuln", "detect_php168",
  "detect_wordpress", "detect_directory_traversal", "detect_iis", "detect_gogs_gitea", "detc
  t_thinkphp", "detect_jenkins", "detect_ecshop", "detect_nexus", "detect_drupal", "detect_gh
  ostscript", "detect_atlassian", "detect_weblogic", "detect_coremail", "detect_phpcms", "det
  ect_spring", "detect_southidc", "detect_fastjson", "detect_tbk_dvr", "detect_joomla", "dete
  ct_ecology_oa", "detect_jackson", "detect_xstream", "detect_activemq", "detect_solr"]}, "lo
  w_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "medium_r
  isk_enable_log": 1, "high_risk_action": "deny"}, "m_ssrf": {"low_risk_enable_log": 1, "high
  _risk_enable_log": 1, "low_risk_action": "continue", "medium_risk_action": "continue", "sta
  te": "enabled", "medium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_xss": {"low_r
  isk_enable_log": 1, "high_risk_enable_log": 1, "detect_config": {"detect_complete_html": tru
  e}, "low_risk_action": "continue", "medium_risk_action": "continue", "state": "enabled", "m
  edium_risk_enable_log": 1, "high_risk_action": "deny"}, "m_asp_code_injection": {"state": "
  disabled", "high_risk_action": "deny", "high_risk_enable_log": 1, "medium_risk_action": "co
  ntinue", "medium_risk_enable_log": 1, "low_risk_action": "continue", "low_risk_enable_log":
  1, "detect_config": {}}, "m_ssti": {"state": "disabled", "high_risk_action": "deny", "high
  risk_enable_log": 1, "medium_risk_action": "continue", "medium_risk_enable_log": 1, "low_r
  isk_action": "continue", "low_risk_enable_log": 1, "detect_config": {}}}
  &MiscModuleConfig={"decode_config":{"decode_methods":["url decode","JSON","base64","hex","e
  val","XML","PHP deserialize","utf7"]}}
```

Sample success responses

XML format

```
<EditPolicyGroupResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuratio
  n generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</EditPolicyGroupResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.4.4. DeletePolicyGroup

Deletes a specific protection policy.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeletePolicyGroup	The operation that you want to perform. Set the value to DeletePolicyGroup.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
IdList	RepeatList	Yes	[1, 2]	The ID of the protection policy. You can enter multiple IDs. You can call the DescribePolicyGroup operation to query the IDs of protection policies.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String		The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DeletePolicyGroup
&RegionId=cn-hangzhou
&IdList.1=1
```

Sample success responses

XML format

```
<DeletePolicyGroupResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result></Result>
</DeletePolicyGroupResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": ""
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.5. Protection logs

9.5.1. QueryAsyncTaskStatus

Queries the status of an asynchronous task.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryAsyncTaskStatus	The operation that you want to perform. Set the value to QueryAsyncTaskStatus.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
TaskId	String	Yes	11c745fc-1d66-40ea-90d7-7e9a12b987b2	The ID of the asynchronous task.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
TaskStatus	Struct		
└TaskId	String	c68646a1-58f8-4b75-828a-a2d3b19b382a	The ID of the task.
└Time	String	1593593692	The time when the task status message was generated. This value is a UNIX timestamp representing the number of seconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
└TaskList	String	["Website-related configuration generation", "Policy-related configuration generation"]	The descriptions of the task. This value is returned only for asynchronous tasks.
└StatusMessage	String	The configuration is in effect.	The status message of the task.
└SuccessCode	String	1	The status code of the task. Valid values: 0: The task fails. 1: The task is successful. 2: The task is not started.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=QueryAsyncTaskStatus
&RegionId=cn-hangzhou
&TaskId=11c745fc-1d66-40ea-90d7-7e9a12b987b2
```

Sample success responses

XML format

```
<QueryAsyncTaskStatusResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <TaskStatus>
    <TaskId>c68646a1-58f8-4b75-828a-a2d3b19b382a</TaskId>
    <Time>1593593692</Time>
    <TaskList>["Website-related configuration generation", "Policy-related configuration generation"]</TaskList>
    <StatusMessage>The configuration is in effect.</StatusMessage>
    <SuccessCode>1</SuccessCode>
  </TaskStatus>
</QueryAsyncTaskStatusResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "TaskStatus": {
    "TaskId": "c68646a1-58f8-4b75-828a-a2d3b19b382a",
    "TaskList": ["Website-related configuration generation", "Policy-related configuration generation"],
    "SuccessCode": "1",
    "Time": "1593593692",
    "StatusMessage": "The configuration is in effect."
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.5.2. QueryAttackDetectionLog

Queries attack detection logs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryAttackDetectionLog	The operation that you want to perform. Set the value to QueryAttackDetectionLog.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: 10.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.
TimestampRangeFilter	RepeatList	No	["1594656000-1596729600"]	The time range to filter logs. You can enter multiple time ranges.

Parameter	Type	Required	Example	Description
RiskLevelFilter	RepeatList	No	[1, 2]	
AttackTypeFilter	RepeatList	No	[1, 2, 3]	
ActionFilter	RepeatList	No	[1, 2]	The action to filter logs. You can enter multiple actions. Valid values: 1, 0, and 2. The value 1 specifies block, the value 0 specifies allow, and the value 2 specifies that all attack detection logs are returned.
ProtocolFilter	RepeatList	No	[0, 1]	The protocol to filter logs. You can enter multiple protocols. Valid values: 0: HTTP 1: HTTPS
				The country or region to filter logs. You can enter multiple countries or regions. Valid values: CN (China), AD (Andorra), AE (United Arab Emirates), AF (Afghanistan), AG (Antigua and Barbuda), AI (Anguilla), AL (Albania), AM (Armenia), AO (Angola), AQ (Antarctica), AR (Argentina), AS (American Samoa), AT (Austria), AU (Australia), AW (Aruba), AX (Åland Islands), AZ (Azerbaijan), BA (Bosnia and Herzegovina), BB (Barbados), BD (Bangladesh), BE (Belgium), BF (Burkina Faso), BG (Bulgaria), BH (Bahrain), BI (Burundi), BJ (Benin), BL (Saint Barthelemy), BM (Bermuda), BN (Brunei), BO (Bolivia), BQ (Caribbean Netherlands), BR (Brazil), BS (Bahamas), BT (Bhutan), BV (Bouvet Island), BW (Botswana), BY (Belarus), BZ (Belize), CA (Canada), CC (Cocos (Keeling) Islands), CD (Democratic Republic of the Congo), CF (Central Africa Republic), CG (Republic of the Congo), CH (Switzerland), CI (Côte d'Ivoire), CK (Cook Islands), CL (Chile), CM (Cameroon), CO (Colombia), CR (Costa Rica), CU (Cuba), CV (Cabo Verde), CW (Curacao), CX (Christmas Island), CY (Cyprus), CZ (Czech Republic), DE (Germany), DJ (Djibouti), DK

Parameter	Type	Required	Example	Description
CountryFilter	RepeatList	No	["GB", "US"]	(Denmark), DM (Dominica), DO (Dominican Republic), DZ (Algeria), EC (Ecuador), EE (Estonia), EG (Egypt), EH (Sahrawi Arab Democratic Republic), ER (Eritrea), ES (Spain), ET (Ethiopia), FI (Finland), FJ (Fiji), FK (Falkland Islands), FM (Federated States of Micronesia), FO (Faroe Islands), FR (France), GA (Gabon), GB (United Kingdom), GD (Grenada), GE (Georgia), GF (French Guiana), GG (Guernsey), GH (Ghana), GI (Gibraltar), GL (Greenland), GM (Gambia), GN (Guinea), GP (Guadeloupe), GQ (Equatorial Guinea), GR (Greece), GS (South Georgia and The South Sandwich Islands), GT (Guatemala), GU (Guam), GW (Guinea-Bissau), GY (Guyana), HK (Hong Kong), HM (Heard Island and McDonald Islands), HN (Honduras), HR (Croatia), HT (Haiti), HU (Hungary), ID (Indonesia), IE (Ireland), IL (Israel), IM (Isle of Man), IN (India), IO (British Indian Ocean Territory), IQ (Iraq), IR (Iran), IS (Iceland), IT (Italy), JE (Jersey), JM (Jamaica), JO (Jordan), JP (Japan), KE (Kenya), KG (Kyrgyzstan), KH (Kampuchea), KI (Kiribati), KM (Comoros), KN (Saint Kitts and Nevis), KP (Democratic People's Republic of Korea), KR (Republic of Korea), KW (Kuwait), KY (Cayman Islands), KZ (Kazakhstan), LA (Laos), LB (Lebanon), LC (Saint Lucia), LI (Liechtenstein), LK (Sri Lanka), LR (Liberia), LS (Lesotho), LT (Lithuania), LU (Luxembourg), LV (Latvia), LY (Libya), MA (Morocco), MC (Monaco), MD (Moldova), ME (Montenegro), MF (Saint Martin), MG (Madagascar), MH (Marshall Islands), MK (Macedonia), ML (Mali), MM (Myanmar), MN (Mongolia), MP (Northern Mariana Islands), MQ (Martinique), MR (Mauritania), MS (Montserrat), MT (Malta), MU (Mauritius), MV (Maldives), MW (Malawi), MX (Mexico), MY (Malaysia), MZ (Mozambique), NA (Namibia), NC (New Caledonia), NE (Niger), NF (Norfolk Island), NG (Nigeria), NI (Nicaragua), NL (Netherlands), NO (Norway), NP (Nepal), NR (Nauru), NU (Niue), NZ (New Zealand), OM (Oman), PA (Panama), PE (Peru), PF (French Polynesia), PG (Papua New Guinea), PH (Philippines), PK

Parameter	Type	Required	Example	Description
				(Pakistan), PL (Poland), PM (Saint Pierre and Miquelon), PN (Pitcairn Islands), PR (Puerto Rico), PS (Palestine), PT (Portugal), PW (Palau), PY (Paraguay), QA (Qatar), RE (Reunion), RO (Romania), RS (Serbia), RU (Russia), RW (Rwanda), SA (Saudi Arabia), SB (Solomon Islands), SC (Seychelles), SD (Sudan), SE (Sweden), SG (Singapore), SH (Saint Helena), SI (Slovenia), SJ (Svalbard and Jan Mayen Islands), SK (Slovakia), SL (Sierra Leone), SM (San Marino), SN (Senegal), SO (Somalia), SR (Suriname), SS (South Sudan), ST (Sao Tome and Principe), SV (El Salvador), SX (Sint Maarten), SY (Syria), SZ (Eswatini), TC (Turks and Caicos Islands), TD (Chad), TF (French Southern and Antarctic Lands), TG (Togo), TH (Thailand), TJ (Tajikistan), TK (Tokelau), TL (East Timor), TM (Turkmenistan), TN (Tunisia), TO (Tonga), TR (Turkey), TT (Trinidad and Tobago), TV (Tuvalu), TZ (Tanzania), UA (Ukraine), UG (Uganda), UM (United States Minor Outlying Islands), US (United States), UY (Uruguay), UZ (Uzbekistan), VA (Vatican City), VC (Saint Vincent and the Grenadines), VE (Venezuela), VG (British Virgin Islands), VI (United States Virgin Islands), VN (Vietnam), VU (Vanuatu), WF (Wallis and Futuna Islands), WS (Samoa), YE (Yemen), YT (Mayotte), ZA (South Africa), ZM (Zambia), and ZW (Zimbabwe).
EventIdFilter	RepeatList	No	["2a0ca6e9-a33d-4164-8a8d-3b0e91130069"]	The event ID to filter logs. You can enter multiple IDs.
SourceIpFilter	RepeatList	No	["192.168.XX.XX"]	The source IP address to filter logs. You can enter multiple source IP addresses.
HostFilter	RepeatList	No	["www.aliyun.com"]	The attacked domain name to filter logs. You can enter multiple domain names.
UrlPathFilter	RepeatList	No	["/"]	The URL path to filter logs. You can enter multiple URL paths.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	<pre>{ "items": [{ "attack_type": "SQL injection", "risk_level": "High risk", "action": { "value": 1, "translation": "Block" }, "protocol": "http", "country": "United States", "province": "", "dest_port": 80, "src_ip": "1.2.XX.XX", "url_path": "/", "host": "www.baidu.com", "timestamp": 1594610215, "id": "976ada8c-7561-48be-8d63-2d668defcbad", "event_id": "7f7ae14bada0490bb257547f05901ec7", "rule_id": "m_sqli", "detector": "a36c01009.cloud.c01.amtest11", "proxy_name": "a36c01009.cloud.c01.amtest11", "src_port": 34109, "dest_ip": "43.17.XX.XX", "req_header_raw": "HEAD /?id=1 or b=2 HTTP/1.1\r\nUser-Agent: curl/7.29.0\r\nAccept: /\r\nHost: www.baidu.com\r\nX-Forwarded-For: 1.2.XX.XX\r\n\r\n", "req_body": "", "resp_header_raw": "", "resp_body": "", "payload": "1 or b=2", "session": "" }] }</pre>	

Parameter	Type	Example	Description
		<pre>"location": "/urlpath", "decode_path": "", "ali_uid": "1376988933618853", "aliyun_extra": {"resource_port_mapping": {}}, "real_dest_port": 80, "vpc_id": "", "vpc_name": "yd_vpc", "extra": {}, "module": "SQL injection detection module", "reason": "SQL injection detected", "website": "http://www.baidu.com/"}}, "total": "101"}</pre>	

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=QueryAttackDetectionLog  
&RegionId=cn-hangzhou  
&PageSize=20  
&PageNumber=1  
&TimestampRangeFilter.1=1594656000-1596729600  
&RiskLevelFilter.1=1  
&AttackTypeFilter.1=1  
&ActionFilter.1=1  
&ProtocolFilter.1=0  
&CountryFilter.1=["GB", "US"]  
&EventIdFilter.1=2a0ca6e9-a33d-4164-8a8d-3b0e91130069  
&SourceIpFilter.1=192.168.100.200  
&HostFilter.1=www.aliyun.com  
&UrlPathFilter.1=/  

```

Sample success responses

XML format

```
<QueryAttackDetectionLogResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"items": [{"attack_type": "SQL injection", "risk_level": "High risk", "action": {"value": 1, "translation": "Block"}, "protocol": "http", "country": "United States", "province": "", "dest_port": 80, "src_ip": "1.2.XX.XX", "url_path": "/", "host": "www.baidu.com", "timestamp": 1594610215, "id": "976ada8c-7561-48be-8d63-2d668defcbad", "event_id": "7f7ae14bada0490bb257547f05901ec7", "rule_id": "m_sqli", "detector": "a36c01009.cloud.c01.amtest11", "proxy_name": "a36c01009.cloud.c01.amtest11", "src_port": 34109, "dest_ip": "43.17.XX.XX", "req_header_raw": "\"\"HEAD /?id=1 or b=2 HTTP/1.1\\r\\nUser-Agent: curl/7.29.0\\r\\nAccept: */*\\r\\nHost: www.baidu.com\\r\\nX-Forwarded-For: 1.2.XX.XX\\r\\n\\r\\n\"", "req_body": "\"\"\", \"resp_header_raw\": \"\"\", \"resp_body\": \"\"\", \"payload\": \"1 or b=2\", \"session\": \"\", \"location\": \"urlpath\", \"decode_path\": \"\", \"ali_uid\": \"1376988933618853\", \"aliyun_extra\": \"{ \"resource_port_mapping\": {} }\", \"real_dest_port\": 80, \"vpc_id\": \"\", \"vpc_name\": \"yd_vpc\", \"extra\": \"{}\", \"module\": \"SQL injection detection module\", \"reason\": \"SQL injection detected\", \"website\": \"http://www.baidu.com/\"}], \"total\": \"101\"}</Result>
</QueryAttackDetectionLogResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "items": [
      {
        "attack_type": "SQL injection",
        "risk_level": "High risk",
        "action": {
          "value": 1,
          "translation": "Block"
        },
        "protocol": "http",
        "country": "United States",
        "province": "",
        "dest_port": 80,
        "src_ip": "1.2.XX.XX",
        "url_path": "/",
        "host": "www.baidu.com",
        "timestamp": 1594610215,
        "id": "976ada8c-7561-48be-8d63-2d668defcbad",
        "event_id": "7f7ae14bada0490bb257547f05901ec7",
        "rule_id": "m_sqli",
        "detector": "a36c01009.cloud.c01.amtest11",
        "proxy_name": "a36c01009.cloud.c01.amtest11",
        "src_port": 34109,
        "dest_ip": "43.17.XX.XX",
        "req_header_raw": "\"\"HEAD /?id=1 or b=2 HTTP/1.1\\r\\nUser-Agent: curl/7.29.0\\r\\nAccept: */*\\r\\nHost: www.baidu.com\\r\\nX-Forwarded-For: 1.2.XX.XX\\r\\n\\r\\n\"",
        "req_body": "\"\"\", \"resp_header_raw\": \"\"\", \"resp_body\": \"\"\", \"payload\": \"1 or b=2\", \"session\": \"\", \"location\": \"urlpath\", \"decode_path\": \"\", \"ali_uid\": \"1376988933618853\", \"aliyun_extra\": \"{ \"resource_port_mapping\": {} }\", \"real_dest_port\": 80, \"vpc_id\": \"\", \"vpc_name\": \"yd_vpc\", \"extra\": \"{}\", \"module\": \"SQL injection detection module\", \"reason\": \"SQL injection detected\", \"website\": \"http://www.baidu.com/\"}],
        "total": "101"
      }
    ]
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.5.3. QueryAttackDetectionDetailLog

Queries the details of a specific attack detection log.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryAttackDetectionDetailLog	The operation that you want to perform. Set the value to QueryAttackDetectionDetailLog.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
LogId	String	Yes	1e23f8d1-a9d2-4dd9-b7e2-424b9832183f	The ID of the attack detection log.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{ "items": [{ "attack_type": "SQL injection", "risk_level": "High risk", "action": { "value": 1, "translation": "Block" }, "protocol": "http", "country": "United States", "province": "", "dest_port": 80, "src_ip": "1.2.XX.XX", "url_path": "/", "host": "www.baidu.com", "timestamp": 1594610215, "id": "976ada8c-7561-48be-8d63-2d668defcbad", "event_id": "7f7ae14bada0490bb257547f05901ec7", "rule_id": "m_sqli", "detector": "a36c01009.cloud.c01.amtest11", "proxy_name": "a36c01009.cloud.c01.amtest11", "src_port": 34109, "dest_ip": "43.17.XX.XX", "req_header_raw": "HEAD /? id=1 or b=2 HTTP/1.1\r\nUser-Agent: curl/7.29.0\r\nAccept: /\r\nHost: www.baidu.com\r\nX-Forwarded-For: 1.2.XX.XX\r\n\r\n", "req_body": "", "resp_header_raw": "", "resp_body": "", "payload": "1 or b=2", "session": "", "location": "urlpath", "decode_path": "", "ali_uid": "1376988933618853", "aliyun_extra": { "resource_port_mapping": {} }, "real_dest_port": 80, "vpc_id": "", "vpc_name": "yd_vpc", "extra": {}, "module": "SQL injection detection module", "reason": "SQL injection detected", "website": "http://www.baidu.com/" }] }	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[ RegionId ].aliyuncs.com/?Action=QueryAttackDetectionDetailLog
&RegionId=cn-hangzhou
&LogId=1e23f8d1-a9d2-4dd9-b7e2-424b9832183f
```

Sample success responses

XML [format](#)

```
<QueryAttackDetectionDetailLogResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"items": [{"attack_type": "SQL injection", "risk_level": "High risk", "action": {"value": 1, "translation": "Block"}, "protocol": "http", "country": "United States", "province": "", "dest_port": 80, "src_ip": "1.2.XX.XX", "url_path": "/", "host": "www.baidu.com", "timestamp": 1594610215, "id": "976ada8c-7561-48be-8d63-2d668defcbad", "event_id": "7f7ae14bada0490bb257547f05901ec7", "rule_id": "m_sqli", "detector": "a36c01009.cloud.c01.amtestt11", "proxy_name": "a36c01009.cloud.c01.amtestt11", "src_port": 34109, "dest_ip": "43.17.XX.XX", "req_header_raw": "HEAD /? id=1 or b=2 HTTP/1.1\\r\\nUser-Agent: curl/7.29.0\\r\\nAccept: */*\\r\\nHost: www.baidu.com\\r\\nX-Forwarded-For: 1.2.XX.XX\\r\\n\\r\\n", "req_body": "", "resp_header_raw": "", "resp_body": "", "payload": "1 or b=2", "session": "", "location": "urlpath", "decode_path": "", "ali_uid": "1376988933618853", "aliyun_extra": {"resource_port_mapping": {}}, "real_dest_port": 80, "vpc_id": "", "vpc_name": "yd_vpc", "extra": "{}", "module": "SQL injection detection module", "reason": "SQL injection detected", "website": "http://www.baidu.com/"}]}</Result>
</QueryAttackDetectionDetailLogResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "items": [
      {
        "attack_type": "SQL injection",
        "risk_level": "High risk",
        "action": {
          "value": 1,
          "translation": "Block"
        },
        "protocol": "http",
        "country": "United States",
        "province": "",
        "dest_port": 80,
        "src_ip": "1.2.XX.XX",
        "url_path": "/",
        "host": "www.baidu.com",
        "timestamp": 1594610215,
        "id": "976ada8c-7561-48be-8d63-2d668defcbad",
        "event_id": "7f7ae14bada0490bb257547f05901ec7",
        "rule_id": "m_sqli",
        "detector": "a36c01009.cloud.c01.amtestt11",
        "proxy_name": "a36c01009.cloud.c01.amtestt11",
        "src_port": 34109,
        "dest_ip": "43.17.XX.XX",
        "req_header_raw": "HEAD /? id=1 or b=2 HTTP/1.1\\r\\n\\r\\nUser-Agent: curl/7.29.0\\r\\n\\r\\nAccept: */*\\r\\n\\r\\nHost: www.baidu.com\\r\\n\\r\\nX-Forwarded-For: 1.2.XX.XX\\r\\n\\r\\n\\r\\n\\r\\n",
        "req_body": "",
        "resp_header_raw": "",
        "resp_body": "",
        "payload": "1 or b=2",
        "session": "",
        "location": "urlpath",
        "decode_path": "",
        "ali_uid": "1376988933618853",
        "aliyun_extra": {
          "resource_port_mapping": {}
        },
        "real_dest_port": 80,
        "vpc_id": "",
        "vpc_name": "yd_vpc",
        "extra": {},
        "module": "SQL injection detection module",
        "reason": "SQL injection detected",
        "website": "http://www.baidu.com/"
      }
    ]
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.5.4. QueryAuditLog

Queries system operations logs.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryAuditLog	The operation that you want to perform. Set the value to QueryAuditLog.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.
PageSize	Integer	No	20	The number of entries to return on each page. Default value: 10.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"items": [{"content": "An access control whitelist is created. Data: {'comment': '', 'target_type': 'Session', 'target_list': ['1313'], 'target_group_list': []}", "username": "1376988933618853", "id": "756897bd-a178-445b-a193-5b46c14fa44c", "ip": "10.17.XX.XX", "user_agent": "Apache-HttpClient/4.5.2 (Java/1.8.0_152)", "log_type": "Access control and management", "create_time": "1594653501"}], "total": "36"}	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=QueryAuditLog
&RegionId=cn-hangzhou
&PageSize=20
&PageNumber=1
```

Sample success responses

XML format

```
<QueryAuditLogResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"items": [{"content": "An access control whitelist is created. Data: {'comment': '', 'target_type': 'Session', 'target_list': ['1313'], 'target_group_list': []}", "username": "1376988933618853", "id": "756897bd-a178-445b-a193-5b46c14fa44c", "ip": "10.17.XX.XX", "user_agent": "Apache-HttpClient/4.5.2 (Java/1.8.0_152)", "log_type": "Access control and management", "create_time": "1594653501"}], "total": "36"}</Result>
</QueryAuditLogResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "items": [
      {
        "content": "An access control whitelist is created. Data: {'comment': '', 'target_type': 'Session', 'target_list': ['1313'], 'target_group_list': []}",
        "username": "1376988933618853",
        "id": "756897bd-a178-445b-a193-5b46c14fa44c",
        "ip": "10.17.XX.XX",
        "user_agent": "Apache-HttpClient/4.5.2 (Java/1.8.0_152)",
        "log_type": "Access control and management",
        "create_time": "1594653501"
      }
    ],
    "total": "36"
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.5.5. QueryCCRuleExecutionLog

Queries the logs on the execution of HTTP flood protection rules.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryCCRuleExecutionLog	The operation that you want to perform. Set the value to QueryCCRuleExecutionLog.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.
PageSize	Integer	No	20	The number of entries to return on each page. Default value: 10.
TimestampRangeFilter	RepeatList	No	["1594656000-1596729600"]	The time range to filter logs. You can enter multiple ranges. Unit: seconds.
CCRuleTemplateIdList	RepeatList	No	[1, 2]	The rule ID to filter logs. You can enter multiple IDs. You can call the DescribeCCRuleTemplate operation to query the IDs of HTTP flood protection rules.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	<pre>{"items": [{"acl_rule_id": "29", "acl_rule_template_id": "38", "acl_rule_template_version": "39", "timestamp": "1594610400", "count": "100", "acl_rule_target": "1.2.XX.XX", "acl_rule_template": {"name": "123", "match_method": {"target_type": "CIDR", "period": 5, "limit": 1, "scope": "URL", "policy": "www.baidu.com", "scheme": "http"}, "action": {"action": "forbid"}, "template_type": "auto", "dry_run": false, "status": "ok"}}, {"total": 11}</pre>	

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=QueryCCRuleExecutionLog
&RegionId=cn-hangzhou
&PageSize=20
&PageNumber=1
&TimestampRangeFilter.1=1594656000-1596729600
&CCRuleTemplateIdList.1=1
```

Sample success responses

XML format

```
<QueryCCRuleExecutionLogResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"items": [{"acl_rule_id": "29", "acl_rule_template_id": "38", "acl_rule_template_version": "39", "timestamp": "1594610400", "count": "100", "acl_rule_target": "1.2.XX.XX", "acl_rule_template": {"name": "123", "match_method": {"target_type": "CIDR", "period": 5, "limit": 1, "scope": "URL", "policy": "www.baidu.com", "scheme": "http"}, "action": {"action": "forbid"}, "template_type": "auto", "dry_run": false, "status": "ok"}}, {"total": 11}]
</Result>
</QueryCCRuleExecutionLogResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"items": [{"acl_rule_id": "29", "acl_rule_template_id": "38", "acl_rule_template_version": "39", "timestamp": "1594610400", "count": "100", "acl_rule_target": "1.2.XX.XX", "acl_rule_template": {"name": "123", "match_method": {"target_type": "CIDR", "period": 5, "limit": 1, "scope": "URL", "policy": "www.baidu.com", "scheme": "http"}, "action": {"action": "forbid"}, "template_type": "auto", "dry_run": false, "status": "ok"}}, {"total": 11}]
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.5.6. QueryFullAccessLog

Queries full access logs.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryFullAccessLog	The operation that you want to perform. Set the value to QueryFullAccessLog.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: 10.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.
TimestampRangeFilter	RepeatList	No	["1594656000-1596729600"]	The time range to filter logs. You can enter multiple time ranges.
SourceIpFilter	RepeatList	No	["192.168.XX.XX"]	The source IP address to filter logs. You can enter multiple source IP addresses.
DestinationIp	RepeatList	No	["10.10.XX.XX"]	The destination IP address to filter logs. You can enter multiple destination IP addresses.
MethodFilter	RepeatList	No	["POST"]	The request method to filter logs. You can enter multiple methods.
SourcePortFilter	RepeatList	No	[11013, 55555]	The source port to filter logs. You can enter multiple source ports.
ResponseCode	RepeatList	No	[302, 404]	The response code to filter logs. You can enter multiple codes.
DestinationPortFilter	RepeatList	No	[80, 443]	The destination port to filter logs. You can enter multiple destination ports.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
		{"items": [{"id": "a03511f0-b325-	

Parameter	Type	Example	Description
Result	String	<pre> 4674-8f50-80feb5de2023", "ali_uid": "1376988933618853 ", "timestamp": 1594698077, "dest_ip": "43.17.XX.XX", "dest_port": 10003, "real_dest_port": 80, "src_ip": "10.17.XX.XX", "src_port": 37078, "req_header_raw": ""GET / HTTP/1.1\r\nUser- Agent: curl/7.29.0\r\nAcce pt: /\r\nhost: www.wafcloud.com \r\n\r\n", "method": "GET", "req_body": "", "resp_header_raw": ""HTTP/1.1 200 OK\r\nServer: nginx/1.10.2\r\nDat e: Tue, 14 Jul 2020 03:40:35 GMT\r\nContent- Type: text/html\r\nConte nt-Length: 3700\r\nLast- Modified: Tue, 28 Mar 2017 07:33:40 GMT\r\nConnection: keep-alive\r\nETag: "58da11d4- e74"\r\nAccept- Ranges: bytes\r\n\r\n", "resp_code": 200, "payload": "", "url": "/", "content_type": "text/html", "event_id": "", "session": "null", "proxy_name": "a36c01009.cloud.c0 1.amtest11", "website": "www.wafcloud.co m", "host": "www.wafcloud.co </pre>	The returned result of the request.

Parameter	Type	Example	Description
		m", "vpc": "vpc-9qb3r79gohas1khsr2x7e", "vpc_name": "-"}, {"total": "1"}]	

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=QueryFullAccessLog
&RegionId=cn-hangzhou
&PageSize=20
&PageNumber=1
&TimestampRangeFilter.1=1594656000-1596729600
&SourceIpFilter.1=192.168.XX.XX
&DestinationIp.1=10.10.XX.XX
&MethodFilter.1=POST
&ResponseCode.1=302
&SourcePortFilter.1=11013
&DestinationPortFilter.1=80
&HostFilter.1=192.168.XX.XX
&PathFilter.1=/index.html
```

Sample success responses

XML format

```
<QueryFullAccessLogResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"items": [{"id": "a03511f0-b325-4674-8f50-80feb5de2023", "ali_uid": "1376988933618853", "timestamp": 1594698077, "dest_ip": "43.17.XX.XX", "dest_port": 10003, "real_dest_port": 80, "src_ip": "10.17.XX.XX", "src_port": 37078, "req_header_raw": "GET / HTTP/1.1\r\nUser-Agent: curl/7.29.0\r\nAccept: */*\r\nhost: www.wafcloud.com\r\n\r\n", "method": "GET", "req_body": "", "resp_header_raw": "HTTP/1.1 200 OK\r\nServer: nginx/1.10.2\r\nDate: Tue, 14 Jul 2020 03:40:35 GMT\r\nContent-Type: text/html\r\nContent-Length: 3700\r\nLast-Modified: Tue, 28 Mar 2017 07:33:40 GMT\r\nConnection: keep-alive\r\nETag: \"58da11d4-e74\"\r\nAccept-Ranges: bytes\r\n\r\n", "resp_code": 200, "payload": "", "url": "/", "content_type": "text/html", "event_id": "", "session": "null", "proxy_name": "a36c01009.cloud.c01.amtest11", "website": "www.wafcloud.com", "host": "www.wafcloud.com", "vpc": "vpc-9qb3r79gohas1khsr2x7e", "vpc_name": "-"}], "total": "1"}</Result>
</QueryFullAccessLogResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "items": [
      {
        "id": "a03511f0-b325-4674-8f50-80feb5de2023",
        "ali_uid": "1376988933618853",
        "timestamp": 1594698077,
        "dest_ip": "43.17.XX.XX",
        "dest_port": 10003,
        "real_dest_port": 80,
        "src_ip": "10.17.XX.XX",
        "src_port": 37078,
        "req_header_raw": "GET / HTTP/1.1\r\nUser-Agent: curl/7.29.0\r\nAccept: */*\r\nhost: www.wafcloud.com\r\n\r\n",
        "method": "GET",
        "req_body": "",
        "resp_header_raw": "HTTP/1.1 200 OK\r\nServer: nginx/1.10.2\r\nDate: Tue, 14 Jul 2020 03:40:35 GMT\r\nContent-Type: text/html\r\nContent-Length: 3700\r\nLast-Modified: Tue, 28 Mar 2017 07:33:40 GMT\r\nConnection: keep-alive\r\nETag: \"58da11d4-e74\"\r\nAccept-Ranges: bytes\r\n\r\n",
        "resp_code": 200,
        "payload": "",
        "url": "/",
        "content_type": "text/html",
        "event_id": "",
        "session": "null",
        "proxy_name": "a36c01009.cloud.c01.amtest11",
        "website": "www.wafcloud.com",
        "host": "www.wafcloud.com",
        "vpc": "vpc-9qb3r79gohas1khsr2x7e",
        "vpc_name": "-",
        "total": 1
      }
    ]
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.5.7. QueryFullAccessDetailLog

Queries the details of a specific full access log.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryFullAccessDetailLog	The operation that you want to perform. Set the value to QueryFullAccessDetailLog.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
LogId	String	Yes	1e23f8d1-a9d2-4dd9-b7e2-424b9832183f	The ID of the log.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	{ "items": [{ "id": "a03511f0-b325-4674-8f50-80feb5de2023", "ali_uid": "1376988933618853", "timestamp": 1594698077, "dest_ip": "43.17.XX.XX", "dest_port": 10003, "real_dest_port": 80, "src_ip": "10.17.XX.XX", "src_port": 37078, "req_header_raw": "GET / HTTP/1.1\r\nUser-Agent: curl/7.29.0\r\nAccept: /\r\nhost: www.wafcloud.com\r\n\r\n", "method": "GET", "req_body": "", "resp_header_raw": "HTTP/1.1 200 OK\r\nServer: nginx/1.10.2\r\nDate: Tue, 14 Jul 2020 03:40:35 GMT\r\nContent-Type: text/html\r\nContent-Length: 3700\r\nLast-Modified: Tue, 28 Mar 2017 07:33:40 GMT\r\nConnection: keep-alive\r\nETag: \"58da11d4-e74\"\r\nAccept-Ranges: bytes\r\n\r\n", "resp_code": 200, "payload": "", "url": "/", "content_type": "text/html", "event_id": "", "session": "null", "proxy_name": "a36c01009.cloud.c01.amtest11", "website": "www.wafcloud.com", "host": "www.wafcloud.com", "vpc": "vpc-9qb3r79gohas1khsr2x7e", "vpc_name": "-" }]}	

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=QueryFullAccessDetailLog
&RegionId=cn-hangzhou
&LogId=1e23f8d1-a9d2-4dd9-b7e2-424b9832183f
```

Sample success responses

XML **format**

```
<QueryFullAccessDetailLogResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{
    "items": [{
      "id": "a03511f0-b325-4674-8f50-80feb5de2023",
      "ali_uid": "1376988933618853",
      "timestamp": 1594698077,
      "dest_ip": "43.17.XX.XX",
      "dest_port": 10003,
      "real_dest_port": 80,
      "src_ip": "10.17.XX.XX",
      "src_port": 37078,
      "req_header_raw": "GET / HTTP/1.1\r\nUser-Agent: curl/7.29.0\r\nAccept: */*\r\nhost: www.wafcloud.com\r\n\r\n",
      "method": "GET",
      "req_body": "",
      "resp_header_raw": "HTTP/1.1 200 OK\r\nServer: nginx/1.10.2\r\nDate: Tue, 14 Jul 2020 03:40:35 GMT\r\nContent-Type: text/html\r\nContent-Length: 3700\r\nLast-Modified: Tue, 28 Mar 2017 07:33:40 GMT\r\nConnection: keep-alive\r\nETag: \"58da11d4-e74\"\r\nAccept-Ranges: bytes\r\n\r\n",
      "resp_code": 200,
      "payload": "",
      "url": "/",
      "content_type": "text/html",
      "event_id": "",
      "session": "null",
      "proxy_name": "a36c01009.cloud.c01.amtest11",
      "website": "www.wafcloud.com",
      "host": "www.wafcloud.com",
      "vpc": "vpc-9qb3r79gohas1khsr2x7e",
      "vpc_name": "-"
    }]}
</QueryFullAccessDetailLogResponse>
```

JSON **format**


```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "items": [
      {
        "id": "a03511f0-b325-4674-8f50-80feb5de2023",
        "ali_uid": "1376988933618853",
        "timestamp": 1594698077,
        "dest_ip": "43.17.XX.XX",
        "dest_port": 10003,
        "real_dest_port": 80,
        "src_ip": "10.17.XX.XX",
        "src_port": 37078,
        "req_header_raw": "GET / HTTP/1.1\r\nUser-Agent: curl/7.29.0\r\nAccept: */*\r\nhost: www.wafcloud.com\r\n\r\n",
        "method": "GET",
        "req_body": "",
        "resp_header_raw": "HTTP/1.1 200 OK\r\nServer: nginx/1.10.2\r\nDate: Tue, 14 Jul 2020 03:40:35 GMT\r\nContent-Type: text/html\r\nContent-Length: 3700\r\nLast-Modified: Tue, 28 Mar 2017 07:33:40 GMT\r\nConnection: keep-alive\r\nETag: \"58da11d4-e74\"\\r\\nAccept-Ranges: bytes\\r\\n\\r\\n",
        "resp_code": 200,
        "payload": "",
        "url": "/",
        "content_type": "text/html",
        "event_id": "",
        "session": "null",
        "proxy_name": "a36c01009.cloud.c01.amtest11",
        "website": "www.wafcloud.com",
        "host": "www.wafcloud.com",
        "vpc": "vpc-9qb3r79gohas1khsr2x7e",
        "vpc_name": "-"}
    ]
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.5.8. QueryPerformanceStatistics

Queries the historical performance data of a specific node.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryPerformanceStatistics	The operation that you want to perform. Set the value to QueryPerformanceStatistics.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
NodeName	String	Yes	a36c01009.cloud.c01.amtest11	The name of the node.
TimestampRangeFilter	RepeatList		["1594656000-1596729600"]	The time range to filter historical performance data. You can enter multiple time ranges.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	<pre>{ "id": "2005654", "name": "c43b02111.cloud.b03.amtest21", "timestamp": "1594697170", "cpu_usage": 1.5670533277966774, "memory_usage": 8.946810185810278, "disk_usage": 5.475940507296313, "network_read": 26010.129032258064, "network_write": 25739.064516129034, "qps": 0.0, "cps": 10.6, "extra": {}}, { "id": "2005652", "name": "c43b02111.cloud.b03.amtest21", "timestamp": "1594697165", "cpu_usage": 1.3590924225742251, "memory_usage": 8.943323969418117, "disk_usage": 5.475936863788965, "network_read": 23102.645161290322, "network_write": 22265.774193548386, "qps": 0.0, "cps": 9.2, "extra": {}} }</pre>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[ RegionId].aliyuncs.com/?Action=QueryPerformanceStatistics
&RegionId=cn-hangzhou
&NodeName=a36c01009.cloud.c01.amtest11
&TimestampRangeFilter.1=1594656000-1596729600
```

Sample success responses

XML format

```
<QueryPerformanceStatisticsResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>[{
    "id": "2005654", "name": "c43b02111.cloud.b03.amtest21", "timestamp": "1594697170",
    "cpu_usage": 1.5670533277966774, "memory_usage": 8.946810185810278, "disk_usage": 5.475940507296313,
    "network_read": 26010.129032258064, "network_write": 25739.064516129034, "qps": 0.0, "cps": 10.6,
    "extra": {}}, {
      "id": "2005652", "name": "c43b02111.cloud.b03.amtest21", "timestamp": "1594697165",
      "cpu_usage": 1.3590924225742251, "memory_usage": 8.943323969418117, "disk_usage": 5.475936863788965,
      "network_read": 23102.645161290322, "network_write": 22265.774193548386, "qps": 0.0, "cps": 9.2,
      "extra": {}}
    ]</Result>
</QueryPerformanceStatisticsResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": [{
    "id": "2005654", "name": "c43b02111.cloud.b03.amtest21", "timestamp": "1594697170",
    "cpu_usage": 1.5670533277966774, "memory_usage": 8.946810185810278, "disk_usage": 5.475940507296313,
    "network_read": 26010.129032258064, "network_write": 25739.064516129034, "qps": 0.0, "cps": 10.6,
    "extra": {}}, {
      "id": "2005652", "name": "c43b02111.cloud.b03.amtest21", "timestamp": "1594697165",
      "cpu_usage": 1.3590924225742251, "memory_usage": 8.943323969418117, "disk_usage": 5.475936863788965,
      "network_read": 23102.645161290322, "network_write": 22265.774193548386, "qps": 0.0, "cps": 9.2,
      "extra": {}}
    ]
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.6. SSL certificate management

9.6.1. DescribeSSLCert

Queries the information about SSL certificates.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSSLCert	The operation that you want to perform. Set the value to DescribeSSLCert.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	No	1	The ID of the SSL certificate.
PageSize	Integer	No	10	The number of entries to return on each page. Default value: 10.
PageNumber	Integer	No	1	The number of the page to return. Default value: 1.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	<pre>{ "id": 1, "websites": [], "create_time": "1589445455", "name": "test_cert_1", "signature": "329b059f298419c002fc69f1ee9a3df1", "info": { "serial": "0xb79b1ba15f4fb061", "issuer": "Aliyun", "not_valid_before": 1567468800, "not_valid_after": 1882828800, "domains": [] } }</pre>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeSSLCert
&RegionId=cn-hangzhou
&Id=1
&PageSize=10
&PageNumber=1
```

Sample success responses

XML format

```
<DescribeSSLCertResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>[{ "id": 1, "websites": [], "create_time": "1589445455", "name": "test_cert_1",
"signature": "329b059f298419c002fc69f1ee9a3df1", "info": { "serial": "0xb79b1ba15f4fb061", "
issuer": "Aliyun", "not_valid_before": 1567468800, "not_valid_after": 1882828800, "domains"
: [] } } ]</Result>
</DescribeSSLCertResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": "[{ \"id\": 1, \"websites\": [], \"create_time\": \"1589445455\", \"name\": \"tes
t_cert_1\", \"signature\": \"329b059f298419c002fc69f1ee9a3df1\", \"info\": { \"serial\": \"0
xb79b1ba15f4fb061\", \"issuer\": \"Aliyun\", \"not_valid_before\": 1567468800, \"not_valid_
after\": 1882828800, \"domains\": [] } } ]"
```

Error codes

For a list of error codes, see [Error codes](#).

9.6.2. UploadSSLCert

Uploads an SSL certificate.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	UploadSSLCert	The operation that you want to perform. Set the value to UploadSSLCert.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
CertName	String	No	taobao_cert	The name of the SSL certificate.

Parameter	Type	Required	Example	Description
CertFile	Json	Yes	<pre>{"name": "", "content": "bEtrYmd rFVsb3pLY1dM a01BVmZrekhG dGxw****"}</pre>	The Base64-encoded certificate authority (CA) certificate file. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • name: Leave this field unspecified. • content: the Base64-encoded CA certificate file.
KeyFile	Json	No	<pre>{"name": "", "content": "eElzcEZE aElzaXlqVFBGU1 B0ZG9qdm1iSEV 1****"}</pre>	The Base64-encoded private key file. This parameter is a string consisting of JSON structs. A JSON struct includes the following fields: • name: Leave this field unspecified. • content: the Base64-encoded private key file.
CertPassword	String	No	jgXzOoigHGWCL xE	The password of the SSL certificate.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	<pre>{"id": 7, "websites": [], "create_time": "1589771325", "name": "test-cert- 1", "signature": "ec23ec040764d0cc 078879582a375c2c", "info": {"serial": "0xdd45e828dca4b8 c9", "issuer": null, "not_valid_before": 1560816000, "not_valid_after": 1592352000, "domains": []}}</pre>	

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=UploadSSLCert
&RegionId=cn-hangzhou
&CertName=taobao_cert
&CertFile={"name":"","content":"bEtrYmdrVFVSb3plY1dMa01BVmZrekhGdGxweVpl"}
&KeyFile={"name":"","content":"eElzcEZEaElzaXlqVFBGU1B0ZG9qdmliSEVlYW16"}
&CertPassword=jgXzOoigHGWCLxE
```

Sample success responses

XML format

```
<UploadSSLCertResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"id": 7, "websites": [], "create_time": "1589771325", "name": "test-cert-1", "signature": "ec23ec040764d0cc078879582a375c2c", "info": {"serial": "0xdd45e828dca4b8c9", "issuer": null, "not_valid_before": 1560816000, "not_valid_after": 1592352000, "domains": []}}
</Result>
</UploadSSLCertResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"id": 7, "websites": [], "create_time": "1589771325", "name": "test-cert-1", "signature": "ec23ec040764d0cc078879582a375c2c", "info": {"serial": "0xdd45e828dca4b8c9", "issuer": null, "not_valid_before": 1560816000, "not_valid_after": 1592352000, "domains": []}}
```

Error codes

For a list of error codes, see [Error codes](#).

9.6.3. EditSSLCert

Modifies the name of a specific SSL certificate.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	EditSSLCert	The operation that you want to perform. Set the value to EditSSLCert.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Id	Integer	No	1	The ID of the SSL certificate. You can call the DescribeSSLCert operation to query the ID of the SSL certificate.

Parameter	Type	Required	Example	Description
CertName	String	No	aliyun_cert	The name of the SSL certificate. You can call the DescribeSSLCert operation to query the name of the SSL certificate.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"id": 1, "websites": [], "create_time": "1589771325", "name": "test-cert-1", "signature": "ec23ec040764d0cc078879582a375c2c", "info": {"serial": "0xdd45e828dca4b8c9", "issuer": null, "not_valid_before": 1560816000, "not_valid_after": 1592352000, "domains": []}}	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=EditSSLCert
&RegionId=cn-hangzhou
&Id=1
&CertName=aliyun_cert
```

Sample success responses

XML format

```
<EditSSLCertResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"id": 7, "websites": [], "create_time": "1589771325", "name": "test-cert-1", "signature": "ec23ec040764d0cc078879582a375c2c", "info": {"serial": "0xdd45e828dca4b8c9", "issuer": null, "not_valid_before": 1560816000, "not_valid_after": 1592352000, "domains": []}}
</Result>
</EditSSLCertResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "id": 7,
    "websites": [],
    "create_time": "1589771325",
    "name": "test-cert-1",
    "signature": "ec23ec040764d0cc078879582a375c2c",
    "info": {
      "serial": "0xdd45e828dca4b8c9",
      "issuer": null,
      "not_valid_before": 1560816000,
      "not_valid_after": 1592352000,
      "domains": []
    }
  }
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.6.4. DeleteSSLCert

Deletes a specific SSL certificate.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DeleteSSLCert	The operation that you want to perform. Set the value to DeleteSSLCert.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
IdList	RepeatList	Yes	[1, 2]	The ID of the SSL certificate. You can enter multiple IDs. You can call the DescribeSSLCert operation to query the IDs of SSL certificates.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String		The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DeleteSSLCert
&RegionId=cn-hangzhou
&IdList.1=1
```


Sample success responses

XML format

```
<DeleteSSLCertResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result></Result>
</DeleteSSLCertResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": ""
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.7. System information

9.7.1. DescribeMetrics

Queries the monitoring metrics of physical WAF nodes.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeMetrics	The operation that you want to perform. Set the value to DescribeMetrics.
RegionId	String	Yes	cn-hangzhou	The ID of the region.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.

Parameter	Type	Example	Description
Result	String	<pre>{"nodes": [{"id": "a36c01009.cloud.c01.amtest11", "qps": 0, "disk_watermark": 0.05619211156645502, "throughput_read": 368475, "throughput_write": 368434, "connections": 1, "delta_connections": 0}], "website_count": 0, "domain_count": 0, "is_healthy": true}</pre>	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeMetrics
&RegionId=cn-hangzhou
```

Sample success responses

XML format

```
<DescribeMetricsResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"nodes": [{"id": "a36c01009.cloud.c01.amtest11", "qps": 0, "disk_watermark": 0.05619211156645502, "throughput_read": 368475, "throughput_write": 368434, "connections": 1, "delta_connections": 0}], "website_count": 0, "domain_count": 0, "is_healthy": true}</Result>
</DescribeMetricsResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"nodes": [{"id": "a36c01009.cloud.c01.amtest11", "qps": 0, "disk_watermark": 0.05619211156645502, "throughput_read": 368475, "throughput_write": 368434, "connections": 1, "delta_connections": 0}], "website_count": 0, "domain_count": 0, "is_healthy": true}
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.7.2. DescribeNodeStatus

Queries the status information about physical WAF nodes.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeNodeStatus	The operation that you want to perform. Set the value to DescribeNodeStatus.
RegionId	String	Yes	cn-hangzhou	The ID of the region.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
		<pre>[{"ha": {"services": [{"estate": "master", "healthy": true, "mstate": "idle", "name": "redis", "url": ""}], "id": "c43b02111.cloud.b03.amtest21", "node": {"cpu": 0.015010513044737767, "detector": {"conn_client": 14, "conn_client_close": 0, "conn_client_estab": 0, "conn_server": 0, "conn_server_close": 0, "conn_server_estab": 0, "cpu": 7.2e-05, "detector_version": "4.1.4-5b5eb8e3", "fusion_stat": {"req": {"average_length": 0, "average_time": 0, "count": 0, "max_length": 0, "max_time": 0, "min_length": 0, "min_time": 0, "sd_length": 0, "sd_time": 0, "top10_length": 0, "top10_time": 0, "top50_length": 0, "top50_time": 0, "top90_length": 0, "top90_time": 0, "top99_length": 0, "top99_time": 0}, "rsp": {"average_length": 0, "average_time": 0, "count": 0, "max_length": 0, "max_time": 0, "min_length": 0, "min_time": 0, "sd_length": 0, "sd_time": 0, "top10_length": 0, "top10_time": 0, "top50_length": 0, "top50_time": 0, "top90_length": 0, "top90_time": 0, "top99_length": 0, "top99_time": 0}}, "ioread": 12782, "iowrite": 3416, "mem": 0.004292, "node": "c43b02111.cloud.b03.amtest21", "policy_version": {"cc_config_version": "2827", "config_version": "4", "current_version": "1", "detector_config_version": "1890", "extra_config_version": "1890", "ip_group_config_version": "7", "policy_config_version": "1890", "site_config_version": "1890"}, "req_average_time": 0, "req_detect_count": 0, "req_detect_time": 0, "req_detect_time_distribution": [{"latency": 0, "percent": 99}, {"latency": 0, "percent": 90}, {"latency": 0, "percent": 75}, {"latency": 0, "percent": 50}], "req_ngx_count": 0, "req_ngx_time": 0, "req_ngx_time_distribution": {}, "req_num_accepted": 0, "req_num_access_log": 0, "req_num_attack": 0, "req_num_attack_acl": 0, "req_num_attack_web": 0, "req_num_blocked": 0, "req_num_blocked_acl": 0, "req_num_blocked_web": 0, "req_num_dropped": 0,</pre>	

Parameter	Type	Example	Description
Result	String	<pre> "req_num_handled": 0, "req_num_total": 0, "rsp_average_time": 0, "rsp_detect_count": 0, "rsp_detect_time": 0, "rsp_detect_time_distribution": [{"latency": 0, "percent": 99}, {"latency": 0, "percent": 90}, {"latency": 0, "percent": 75}, {"latency": 0, "percent": 50}], "rsp_ngx_count": 0, "rsp_ngx_time": 0, "rsp_ngx_time_distribution": {}, "rsp_num_accepted": 0, "rsp_num_access_log": 0, "rsp_num_attack": 0, "rsp_num_attack_acl": 0, "rsp_num_attack_web": 0, "rsp_num_blocked": 0, "rsp_num_blocked_acl": 0, "rsp_num_blocked_web": 0, "rsp_num_dropped": 0, "rsp_num_handled": 0, "rsp_num_total": 0, "time_from": "1594696127.271", "time_to": "1594696132.271", "uptime": "6 23:33:25.880", "workers": [{"conn_client": 1, "conn_client_close": 0, "conn_client_estab": 0, "conn_server": 0, "conn_server_close": 0, "conn_server_estab": 0, "cpu": 0, "index": 0, "ioread": 913, "iowrite": 244}, {"conn_client": 1, "conn_client_close": 0, "conn_client_estab": 0, "conn_server": 0, "conn_server_close": 0, "conn_server_estab": 0, "cpu": 0, "index": 1, "ioread": 913, "iowrite": 244}], "disk_info": {"raids_status": [], "read": 0, "time_from": "1594696127", "time_to": "1594696132", "total": "1124191502336", "usage": "61553455104", "write": 229376}, {"last_timestamp": "1594696127", "mario": {"access_log_stat": {"num_pending": 0, "num_processed": 3, "num_processed_last_10s": 0}, "detect_log_stat": {"num_pending": 0, "num_processed": 3, "num_processed_last_10s": 0}, "num_goroutine": 8903, "policy_version": {"acl_data_config": "11", "acl_template": "58", "acl_whitelist": "18", "detect_log_forward_config": "10", "log_aggregate_config": "18", "plugin": "17", "summary_config": "14"}, "router_message_stat": {"num_receive": 0, "num_receive_error": 0, "num_receive_error_last_10s": 0, "num_receive_last_10s": 0, "num_receive_pending": 0, "num_send": 0, "num_send_error": 0, "num_send_error_last_10s": 0, "num_send_last_10s": 0}}, "mem": 0.08940248252983965, "network_io": [{"interface": "eth0", "read": 417525, "time_from": "1594696127", "time_to": "1594696132", "write": 467457}, {"interface": "eth1", "read": 403066, "time_from": "1594696127", "time_to": "1594696132", "write": 322033}, {"interface": "ens1f0", "read": 0, "time_from": "1594696127", "time_to": "1594696132", "write": 0}, {"interface": "ens1f1", "read": 0, "time_from": "1594696127", "time_to": "1594696132", "write": 0}, {"interface": "ens2f0", "read": 0, "time_from": "1594696127", "time_to": "1594696132", "write": 0}, {"interface": "ens2f1", "read": 0, "time_from": "1594696127", "time_to": "1594696132", "write": 0}], "received_timestamp": 1594696132, "engine": {"config_version": 1868, "stats": {"accepts": 45, "connections": 1, "handled": 45, "requests": 2, "time_from": 1594696127, "time_to": 1594696132, "avg_time": 0}, "hostname": "c43b02111.cloud.b03.amtest21"}, "timestamp": "1594696132", "uptime": 5188576, "status": "HEALTHY"}, {"services": [{"cpu": 2.413311965811966e-05, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.007124904089239252, "name": "engine", "status": "HEALTHY", "uptime": 603206, "version": "v3.12.0_r5"}, {"cpu": 2.523696581196581e-05, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.004504908368650695, "name": "detector-srv", "status": "HEALTHY", "uptime": 603206, "version": "v3.12.0_r5"}, {"cpu": 0.0011938266737891738, "extra": null, "hostname": "3ed9747c2003", "mem": 0.007155565200169913, </pre>	The returned result of the request.

Parameter	Type	Description
Example		<pre> "name": "mario", "status": "HEALTHY", "uptime": 603207, "version": "v3.12.0_r5", {"cpu": 0.0036347603276353276, "extra": null, "hostname": "598a767919bc", "mem": 0.0373652018262435, "name": "mgt-api", "status": "HEALTHY", "uptime": 321446, "version": "v3.12.0_r5", {"cpu": 0.0002562163105413105, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.043149085452621895, "name": "mgt-redis", "status": "HEALTHY", "uptime": 603208, "version": "5.0", {"cpu": 1.5907836879432624e-05, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.008885680945231749, "name": "agent", "status": "HEALTHY", "uptime": 603205, "version": "v3.12.0_r5", {"cpu": 0.037529611403212516, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.0002865208871662617, "name": "minion", "status": "HEALTHY", "uptime": 603209, "version": "v3.12.0_r5"}, {"sites": [{"name": "1749", "servers": {"10.10.XX.XX:15044": "HEALTHY"}}, "_version_details": {"service_name": "engine", "versions": {"config_version": {"heartbeat_version": 1868, "database_version": 1868, "version_status": "sync"}, "service_status": "HEALTHY"}, {"service_name": "detector-srv", "versions": {"cc_config_version": {"heartbeat_version": 2827, "database_version": 2837, "version_history": [], "version_status": "fall_behind"}, "detector_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "extra_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "ip_group_config_version": {"heartbeat_version": 7, "database_version": 7, "version_status": "sync"}, "policy_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "site_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "service_status": "HEALTHY"}, {"service_name": "mario", "versions": {"acl_data_config": {"heartbeat_version": 11, "database_version": 12, "version_history": [], "version_status": "fall_behind"}, "acl_template": {"heartbeat_version": 58, "database_version": 62, "version_history": [], "version_status": "fall_behind"}, "acl_whitelist": {"heartbeat_version": 18, "database_version": 18, "version_status": "sync"}, "detect_log_forward_config": {"heartbeat_version": 10, "database_version": 11, "version_history": [], "version_status": "fall_behind"}, "log_aggregate_config": {"heartbeat_version": 18, "database_version": 20, "version_history": [], "version_status": "fall_behind"}, "plugin": {"heartbeat_version": 17, "database_version": 20, "version_history": [], "version_status": "fall_behind"}, "summary_config": {"heartbeat_version": 14, "database_version": 14, "version_status": "sync"}, "service_status": "HEALTHY"}]] </pre>

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeNodeStatus
&RegionId=cn-hangzhou
```

Sample success responses

XML [format](#)

```
<DescribeNodeStatusResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>[{ "ha": { "services": [{ "estate": "master", "healthy": true, "mstate": "idle", "name": "redis", "url": "" } ] }, "id": "c43b02111.cloud.b03.amtest21", "node": { "cpu": 0.015010513044737767, "detector": { "conn_client": 14, "conn_client_close": 0, "conn_client_estab": 0, "conn_server": 0, "conn_server_close": 0, "conn_server_estab": 0, "cpu": 7.2e-05, "detector_version": "4.1.4-5b5eb8e3", "fusion_stat": { "req": { "average_length": 0, "average_time": 0, "count": 0, "max_length": 0, "max_time": 0, "min_length": 0, "min_time": 0, "sd_length": 0, "sd_time": 0, "top10_length": 0, "top10_time": 0, "top50_length": 0, "top50_time": 0, "top90_length": 0, "top90_time": 0, "top99_length": 0, "top99_time": 0 }, "rsp": { "average_length": 0, "average_time": 0, "count": 0, "max_length": 0, "max_time": 0, "min_length": 0, "min_time": 0, "sd_length": 0, "sd_time": 0, "top10_length": 0, "top10_time": 0, "top50_length": 0, "top50_time": 0, "top90_length": 0, "top90_time": 0, "top99_length": 0, "top99_time": 0 }, "ioread": 12782, "iowrite": 3416, "mem": 0.004292, "node": "c43b02111.cloud.b03.amtest21", "policy_version": { "cc_config_version": "2827", "config_version": "4", "current_version": "1", "detector_config_version": "1890", "extra_config_version": "1890", "ip_group_config_version": "7", "policy_config_version": "1890", "site_config_version": "1890" }, "req_average_time": 0, "req_detect_count": 0, "req_detect_time": 0, "req_detect_time_distribution": [{ "latency": 0, "percent": 99 }, { "latency": 0, "percent": 90 }, { "latency": 0, "percent": 75 }, { "latency": 0, "percent": 50 } ], "req_ngx_count": 0, "req_ngx_time": 0, "req_ngx_time_distribution": {}, "req_num_accepted": 0, "req_num_access_log": 0, "req_num_attack": 0, "req_num_attack_acl": 0, "req_num_attack_web": 0, "req_num_blocked": 0, "req_num_blocked_acl": 0, "req_num_blocked_web": 0, "req_num_dropped": 0, "req_num_handled": 0, "req_num_total": 0, "rsp_average_time": 0, "rsp_detect_count": 0, "rsp_detect_time": 0, "rsp_detect_time_distribution": [{ "latency": 0, "percent": 99 }, { "latency": 0, "percent": 90 }, { "latency": 0, "percent": 75 }, { "latency": 0, "percent": 50 } ], "rsp_ngx_count": 0, "rsp_ngx_time": 0, "rsp_ngx_time_distribution": {}, "rsp_num_accepted": 0, "rsp_num_access_log": 0, "rsp_num_attack": 0, "rsp_num_attack_acl": 0, "rsp_num_attack_web": 0, "rsp_num_blocked": 0, "rsp_num_blocked_acl": 0, "rsp_num_blocked_web": 0, "rsp_num_dropped": 0, "rsp_num_handled": 0, "rsp_num_total": 0, "time_from": "1594696127.271", "time_to": "1594696132.271", "uptime": "6 23:33:25.880", "workers": [{ "conn_client": 1, "conn_client_close": 0, "conn_client_estab": 0, "conn_server": 0, "conn_server_close": 0, "conn_server_estab": 0, "cpu": 0, "index": 0, "ioread": 913, "iowrite": 244 }, { "conn_client": 1, "conn_client_close": 0, "conn_client_estab": 0, "conn_server": 0, "conn_server_close": 0, "conn_server_estab": 0, "cpu": 0, "index": 1, "ioread": 913, "iowrite": 244 } ], "disk_info": { "raids_status": [], "read": 0, "time_from": "1594696127", "time_to": "1594696132", "total": "1124191502336", "usage": "61553455104", "write": 229376 }, "last_timestamp": "1594696127", "mario": { "access_log_stat": { "num_pending": 0, "num_processed": 3, "num_processed_last_10s": 0 }, "detect_log_stat": { "num_pending": 0, "num_processed": 3, "num_processed_last_10s": 0 }, "num_goroutine": 8903, "policy_version": { "acl_data_config": "11", "acl_template": "58", "acl_whitelist": "18", "detect_log_forward_config": "10", "log_aggregate_config": "18", "plugin": "17", "summary_config": "14" }, "router_message_stat": { "num_receive": 0, "num_receive_error": 0, "num_receive_error_last_10s": 0, "num_receive_last_10s": 0, "num_receive_pending": 0, "num_send": 0, "num_send_error": 0, "num_send_error_last_10s": 0, "num_send_last_10s": 0 }, "mem": 0.08940248252983965, "network_io": [{ "interface": "eth0", "read": 417525, "time_from": "1594696127", "time_to": "1594696132", "write": 467457 }, { "interface": "eth1", "read": 403066, "time_from": "1594696127", "time_to": "1594696132", "write": 322033 }, { "interface": "ens1f0", "read": 0, "time_from": "1594696127", "time_to": "1594696132", "write": 0 }, { "interface": "ens1f1", "read": 0, "time_from": "1594696127", "time_to": "1594696132", "write": 0 }, { "interface": "ens2f0", "read": 0, "time_from": "1594696127", "time_to": "1594696132", "write": 0 }, { "interface": "ens2f1", "read": 0, "time_from": "1594696127", "time_to": "1594696132", "write": 0 } ], "received_timestamp": 1594696132, "tengine": { "config_version": 1868, "stats": { "accepts": 45, "connections": 1, "handled": 45, "requests": 2, "time_from": 1594696127, "time_to": 1594696132, "avg_time": 0 }, "hostname": "c43b02111.cloud.b03.amtest21", "timestamp": "1594696132", "up
```

```
time": 5188576, "status": "HEALTHY"}, "services": [{"cpu": 2.413311965811966e-05, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.007124904089239252, "name": "tengine", "status": "HEALTHY", "uptime": 603206, "version": "v3.12.0_r5"}, {"cpu": 2.523696581196581e-05, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.004504908368650695, "name": "detector-srv", "status": "HEALTHY", "uptime": 603206, "version": "v3.12.0_r5"}, {"cpu": 0.0011938266737891738, "extra": null, "hostname": "3ed9747c2003", "mem": 0.007155565200169913, "name": "mario", "status": "HEALTHY", "uptime": 603207, "version": "v3.12.0_r5"}, {"cpu": 0.0036347603276353276, "extra": null, "hostname": "598a767919bc", "mem": 0.0373652018262435, "name": "mgt-api", "status": "HEALTHY", "uptime": 321446, "version": "v3.12.0_r5"}, {"cpu": 0.0002562163105413105, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.043149085452621895, "name": "mgt-redis", "status": "HEALTHY", "uptime": 603208, "version": "5.0"}, {"cpu": 1.5907836879432624e-05, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.008885680945231749, "name": "agent", "status": "HEALTHY", "uptime": 603205, "version": "v3.12.0_r5"}, {"cpu": 0.037529611403212516, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.0002865208871662617, "name": "minion", "status": "HEALTHY", "uptime": 603209, "version": "v3.12.0_r5"}], "sites": [{"name": "1749", "servers": {"10.10.XX.XX:15044": "HEALTHY"}}, {"_version_details": [{"service_name": "tengine", "versions": {"config_version": {"heartbeat_version": 1868, "database_version": 1868, "version_status": "sync"}, "service_status": "HEALTHY"}, {"service_name": "detector-srv", "versions": {"cc_config_version": {"heartbeat_version": 2827, "database_version": 2837, "version_history": [], "version_status": "fall_behind"}, "detector_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "extra_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "ip_group_config_version": {"heartbeat_version": 7, "database_version": 7, "version_status": "sync"}, "policy_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "site_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, {"service_name": "mario", "versions": {"acl_data_config": {"heartbeat_version": 11, "database_version": 12, "version_history": [], "version_status": "fall_behind"}, "acl_template": {"heartbeat_version": 58, "database_version": 62, "version_history": [], "version_status": "fall_behind"}, "acl_whitelist": {"heartbeat_version": 18, "database_version": 18, "version_status": "sync"}, "detect_log_forward_config": {"heartbeat_version": 10, "database_version": 11, "version_history": [], "version_status": "fall_behind"}, "log_aggregate_config": {"heartbeat_version": 18, "database_version": 20, "version_history": [], "version_status": "fall_behind"}, "plugin": {"heartbeat_version": 17, "database_version": 20, "version_history": [], "version_status": "fall_behind"}, "summary_config": {"heartbeat_version": 14, "database_version": 14, "version_status": "sync"}, "service_status": "HEALTHY"}]}]}</Result></DescribeNodeStatusResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {
    "ha": {
      "services": [
        {
          "estate": "master",
          "healthy": true,
          "mstate": "idle",
          "name": "redis",
          "url": ""
        }
      ],
      "id": "c43b02111.cloud.b03.amtest21",
      "node": {
        "cpu": 0.015010513044737767,
        "detector": {
          "conn_client": 14,
          "conn_client_close": 0,
          "conn_client_estab": 0,
          "conn_server": 0,
          "conn_server_close": 0,
          "conn_server_estab": 0,
          "cpu": 7.2e-05,
          "detector_version": "4.1.4-5b5eb8e3",
          "fusion_stat": {
            "req": {
              "average_length": 0,
              "average_time": 0,
              "count": 0,
              "max_length": 0,
              "max_time": 0,
              "min_length": 0,
              "min_time": 0,
              "sd_length": 0,
              "sd_time": 0,
              "top10_length": 0,
              "top10_time": 0,
              "top50_length": 0,
              "top50_time": 0,
              "top90_length": 0,
              "top90_time": 0,
              "top99_length": 0,
              "top99_time": 0
            },
            "rsp": {
              "average_length": 0,
              "average_time": 0,
              "count": 0,
              "max_length": 0,
              "max_time": 0,
              "min_length": 0,
              "min_time": 0,
              "sd_length": 0,
              "sd_time": 0,
              "top10_length": 0,
              "top10_time": 0,
              "top50_length": 0,
              "top50_time": 0,
              "top90_length": 0,
              "top90_time": 0,
              "top99_length": 0,
              "top99_time": 0
            }
          }
        }
      }
    }
  }
}
```

```
length\": 0, \"min_time\": 0, \"sd_length\": 0, \"sd_time\": 0, \"top10_length\": 0, \"top10_time\": 0, \"top50_length\": 0, \"top50_time\": 0, \"top90_length\": 0, \"top90_time\": 0, \"top99_length\": 0, \"top99_time\": 0}}, \"ioread\": 12782, \"iowrite\": 3416, \"mem\": 0.004292, \"node\": \"c43b02111.cloud.b03.amtest21\", \"policy_version\": {\"cc_config_version\": \"2827\", \"config_version\": \"4\", \"current_version\": \"1\", \"detector_config_version\": \"1890\", \"extra_config_version\": \"1890\", \"ip_group_config_version\": \"7\", \"policy_config_version\": \"1890\", \"site_config_version\": \"1890\"}, \"req_average_time\": 0, \"req_detect_count\": 0, \"req_detect_time\": 0, \"req_detect_time_distribution\": [{\"latency\": 0, \"percent\": 99}, {\"latency\": 0, \"percent\": 90}, {\"latency\": 0, \"percent\": 75}, {\"latency\": 0, \"percent\": 50}], \"req_ngx_count\": 0, \"req_ngx_time\": 0, \"req_ngx_time_distribution\": {}, \"req_num_accepted\": 0, \"req_num_access_log\": 0, \"req_num_attack\": 0, \"req_num_attack_acl\": 0, \"req_num_attack_web\": 0, \"req_num_blocked\": 0, \"req_num_blocked_acl\": 0, \"req_num_blocked_web\": 0, \"req_num_dropped\": 0, \"req_num_handled\": 0, \"req_num_total\": 0, \"rsp_average_time\": 0, \"rsp_detect_count\": 0, \"rsp_detect_time\": 0, \"rsp_detect_time_distribution\": [{\"latency\": 0, \"percent\": 99}, {\"latency\": 0, \"percent\": 90}, {\"latency\": 0, \"percent\": 75}, {\"latency\": 0, \"percent\": 50}], \"rsp_ngx_count\": 0, \"rsp_ngx_time\": 0, \"rsp_ngx_time_distribution\": {}, \"rsp_num_accepted\": 0, \"rsp_num_access_log\": 0, \"rsp_num_attack\": 0, \"rsp_num_attack_acl\": 0, \"rsp_num_attack_web\": 0, \"rsp_num_blocked\": 0, \"rsp_num_blocked_acl\": 0, \"rsp_num_blocked_web\": 0, \"rsp_num_dropped\": 0, \"rsp_num_handled\": 0, \"rsp_num_total\": 0, \"time_from\": \"1594696127.271\", \"time_to\": \"1594696132.271\", \"uptime\": \"6 23:33:25.880\", \"workers\": [{\"conn_client\": 1, \"conn_client_close\": 0, \"conn_client_estab\": 0, \"conn_server\": 0, \"conn_server_close\": 0, \"conn_server_estab\": 0, \"cpu\": 0, \"index\": 0, \"ioread\": 913, \"iowrite\": 244}, {\"conn_client\": 1, \"conn_client_close\": 0, \"conn_client_estab\": 0, \"conn_server\": 0, \"conn_server_close\": 0, \"conn_server_estab\": 0, \"cpu\": 0, \"index\": 1, \"ioread\": 913, \"iowrite\": 244}]}, \"disk_info\": {\"raids_status\": [], \"read\": 0, \"time_from\": \"1594696127\", \"time_to\": \"1594696132\", \"total\": \"1124191502336\", \"usage\": \"61553455104\", \"write\": 229376}, \"last_timestamp\": \"1594696127\", \"mario\": {\"access_log_stat\": {\"num_pending\": 0, \"num_processed\": 3, \"num_processed_last_10s\": 0}, \"detect_log_stat\": {\"num_pending\": 0, \"num_processed\": 3, \"num_processed_last_10s\": 0}, \"num_goroutine\": 8903, \"policy_version\": {\"acl_data_config\": \"11\", \"acl_template\": \"58\", \"acl_whitelist\": \"18\", \"detect_log_forward_config\": \"10\", \"log_aggregate_config\": \"18\", \"plugin\": \"17\", \"summary_config\": \"14\"}, \"router_message_stat\": {\"num_receive\": 0, \"num_receive_error\": 0, \"num_receive_error_last_10s\": 0, \"num_receive_last_10s\": 0, \"num_receive_pending\": 0, \"num_send\": 0, \"num_send_error\": 0, \"num_send_error_last_10s\": 0, \"num_send_last_10s\": 0}}, \"mem\": 0.08940248252983965, \"network_io\": [{\"interface\": \"eth0\", \"read\": 417525, \"time_from\": \"1594696127\", \"time_to\": \"1594696132\", \"write\": 467457}, {\"interface\": \"eth1\", \"read\": 403066, \"time_from\": \"1594696127\", \"time_to\": \"1594696132\", \"write\": 322033}, {\"interface\": \"ens1f0\", \"read\": 0, \"time_from\": \"1594696127\", \"time_to\": \"1594696132\", \"write\": 0}, {\"interface\": \"ens1f1\", \"read\": 0, \"time_from\": \"1594696127\", \"time_to\": \"1594696132\", \"write\": 0}, {\"interface\": \"ens2f0\", \"read\": 0, \"time_from\": \"1594696127\", \"time_to\": \"1594696132\", \"write\": 0}, {\"interface\": \"ens2f1\", \"read\": 0, \"time_from\": \"1594696127\", \"time_to\": \"1594696132\", \"write\": 0}], \"received_timestamp\": 1594696132, \"tengine\": {\"config_version\": 1868, \"stats\": {\"accepts\": 45, \"connections\": 1, \"handled\": 45, \"requests\": 2, \"time_from\": 1594696127, \"time_to\": 1594696132, \"avg_time\": 0}, \"hostname\": \"c43b02111.cloud.b03.amtest21\", \"timestamp\": \"1594696132\", \"uptime\": 5188576, \"status\": \"HEALTHY\", \"services\": [{\"cpu\": 2.413311965811966e-05, \"extra\": null, \"hostname\": \"c43b02111.cloud.b03.amtest21\", \"mem\": 0.007124904089239252, \"name\": \"tengine\", \"status\": \"HEALTHY\", \"uptime\": 603206, \"version\": \"v3.12.0_r5\"}, {\"cpu\": 2.523696581196581e-05, \"extra\": null, \"hostname\": \"c43b02111.cloud.b03.amtest21\", \"mem\": 0.004504908368650695, \"name\": \"detector-srv\", \"status\": \"HEALTHY\", \"uptime\": 603206, \"version\": \"v3.12.0_r5\"}, {\"cpu\": 0.0011938266737891738, \"extra\": null, \"hostname\": \"3ed9747c2003\", \"mem\": 0.007155565200169913,
```



```

    "name": "mario", "status": "HEALTHY", "uptime": 603207, "version": "v3.12.0_r5"}, {"cpu": 0.0036347603276353276, "extra": null, "hostname": "598a767919bc", "mem": 0.0373652018262435, "name": "mgt-api", "status": "HEALTHY", "uptime": 321446, "version": "v3.12.0_r5"}, {"cpu": 0.0002562163105413105, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.043149085452621895, "name": "mgt-redis", "status": "HEALTHY", "uptime": 603208, "version": "5.0"}, {"cpu": 1.5907836879432624e-05, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.008885680945231749, "name": "agent", "status": "HEALTHY", "uptime": 603205, "version": "v3.12.0_r5"}, {"cpu": 0.037529611403212516, "extra": null, "hostname": "c43b02111.cloud.b03.amtest21", "mem": 0.0002865208871662617, "name": "minion", "status": "HEALTHY", "uptime": 603209, "version": "v3.12.0_r5"}], "sites": [{"name": "1749", "servers": [{"10.10.XX.XX:15044": "HEALTHY"}]}, {"_version_details": [{"service_name": "tengine", "versions": {"config_version": {"heartbeat_version": 1868, "database_version": 1868, "version_status": "sync"}}, "service_status": "HEALTHY"}, {"service_name": "detector-srv", "versions": {"cc_config_version": {"heartbeat_version": 2827, "database_version": 2837, "version_history": [], "version_status": "fall_behind"}, "detector_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "extra_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "ip_group_config_version": {"heartbeat_version": 7, "database_version": 7, "version_status": "sync"}, "policy_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}, "site_config_version": {"heartbeat_version": 1890, "database_version": 1890, "version_status": "sync"}}, "service_status": "HEALTHY"}, {"service_name": "mario", "versions": {"acl_data_config": {"heartbeat_version": 11, "database_version": 12, "version_history": [], "version_status": "fall_behind"}, "acl_template": {"heartbeat_version": 58, "database_version": 62, "version_history": [], "version_status": "fall_behind"}, "acl_whitelist": {"heartbeat_version": 18, "database_version": 18, "version_status": "sync"}, "detect_log_forward_config": {"heartbeat_version": 10, "database_version": 11, "version_history": [], "version_status": "fall_behind"}, "log_aggregate_config": {"heartbeat_version": 18, "database_version": 20, "version_history": [], "version_status": "fall_behind"}, "plugin": {"heartbeat_version": 17, "database_version": 20, "version_history": [], "version_status": "fall_behind"}, "summary_config": {"heartbeat_version": 14, "database_version": 14, "version_status": "sync"}}, "service_status": "HEALTHY"}]}]
}

```

Error codes

For a list of error codes, see [Error codes](#).

9.7.3. DescribeRealTimeAccess

Queries the monitoring information about access status.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeRealTimeAccess	The operation that you want to perform. Set the value to DescribeRealTimeAccess.

Parameter	Type	Required	Example	Description
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Type	String	Yes	ip	The type to filter monitoring information. Valid values: • ip • session • website • url • If you leave this parameter unspecified, all monitoring information is returned. These types can be combined to filter monitoring information. Example: ipwebsite.
OrderBy	String	Yes	count	The method to sort monitoring information. Valid values: • count: the number of requests • time: the average time of responses
Limit	Integer	No	100	The upper limit of returned entries. Default value: 100.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"data": [{"ip": "10.10.XX.XX", "count": 2}], "type": "top_ip", "order_by": "count"}	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeRealTimeAccess
&RegionId=cn-hangzhou
&Type=ip
&OrderBy=count
&Limit=100
```

Sample success responses

XML format

```
<DescribeRealTimeAccessResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"data": [{"ip": "10.10.XX.XX", "count": 2}], "type": "top_ip", "order_by": "count"}</Result>
</DescribeRealTimeAccessResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": "{\"data\": [{\"ip\": \"10.10.XX.XX\", \"count\": 2}], \"type\": \"top_ip\", \"order_by\": \"count\"}"
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.7.4.

DescribeAttackDetectionAggregationConfig

Queries the configurations of attack detection aggregation.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeAttackDetectionAggregationConfig	The operation that you want to perform. Set the value to DescribeAttackDetectionAggregationConfig.
RegionId	String	Yes	cn-hangzhou	The ID of the region.

Response parameters

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"is_enabled": true}	

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=DescribeAttackDetectionAggregationConfig
&RegionId=cn-hangzhou
```

Sample success responses

XML format

```
<DescribeAttackDetectionAggregationConfigResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result>{"is_enabled": true}</Result>
</DescribeAttackDetectionAggregationConfigResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": {"is_enabled": true}
}
```

Error codes

For a list of error codes, see [Error codes](#).

9.7.5. ToggleAttackDetectionAggregation

Enables or disables the attack detection aggregation feature.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	ToggleAttackDetectionAggregation	The operation that you want to perform. Set the value to ToggleAttackDetectionAggregation.
RegionId	String	Yes	cn-hangzhou	The ID of the region.
Enable	Boolean	No	true	Specifies whether to enable the attack detection aggregation feature. Valid values: - true - false Default value: true.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
RequestId	String	53e59af3-3209-452a-853c-ac10ad815929	The ID of the request.
Result	String	{"is_enabled": true}	The returned result of the request.

Examples

Sample requests

```
https://semawaf.[RegionId].aliyuncs.com/?Action=ToggleAttackDetectionAggregation
&RegionId=cn-hangzhou
&Enable=true
```

Sample success responses

XML format

```
<ToggleAttackDetectionAggregationResponse>
  <RequestId>53e59af3-3209-452a-853c-ac10ad815929</RequestId>
  <Result></Result>
</ToggleAttackDetectionAggregationResponse>
```

JSON format

```
{
  "RequestId": "53e59af3-3209-452a-853c-ac10ad815929",
  "Result": ""
}
```

Error codes

For a list of error codes, see [Error codes](#).

10. Security Operations Center

10.1. Operations

10.1.1. DescribeAttacks

You can call this operation to query attacks on users or on the platform based on specified conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeAttacks</i> .
DataScope	Integer	Yes	Specifies whether the attacks on users or on the platform are queried. Valid values: 0: platform 1: users
SourceFrom	Integer	No	The source of attack data.
UserId	Long	No	The ID of the department to query.
PageSize	Integer	Yes	The number of attacks to return on each page.
PageNo	Integer	Yes	The number of the page to return.
AttackType	String	No	The type of the attacks to query.
ProcessState	Integer	No	The processing status of the attacks to query. 0: An alert has been generated on the attack. 1: The attack has been blocked. 3: The attack traffic is being scrubbed. 4: The attack traffic has been scrubbed.
StartTime	Long	No	The beginning of the time range to query. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.

Parameter	Type	Required	Description
EndTime	Long	No	The end of the time range to query. This value is a UNIX timestamp representing the number of milliseconds that have elapsed since the epoch time January 1, 1970, 00:00:00 UTC.
KeyWord	String	No	The keyword of the attack name or asset name.

Response parameters

Parameter	Type	Description
PageNo	Integer	The page number of the returned page.
PageSize	Integer	The number of attacks returned per page.
Total	Integer	The total number of records.
RequestId	String	The ID of the request.
AttackName	String	The name of the attack.
AttackId	Long	The ID of the attack.
AssetType	Integer	The type of the asset.
Asset	String	The ID of the asset.
UserName	String	The name of the department.
RaisedTime	Long	The time of the attack.
ProcessState	Integer	The processing status of the attack.
UserId	Long	The ID of the user or department.
AttackType	String	The type of the attack.
SourceFrom	Integer	The data source of the attack.
AttackerIp	String	The IP address of the attacker.
AssetName	String	The name of the asset.
AssetPublicIps	String	The public IP address of the affected asset.
AssetPrivateIps	String	The internal IP address of the affected asset.

Examples

Sample requests

```
http(s)://yundunnewsoc-pop.[ RegionId].example.com/? Action=DescribeAttacks
&DataScope=1
&PageSize=20
&PageNo=1
&<Common request parameters>
```

Sample success responses in JSON format

```
{
  "code":200,
  "data":{
    "Data":{
      "PageSize":20,
      "Total":222,
      "Items":[
        {
          "UserName":"yundun****",
          "SourceFrom":46,
          "AttackType":"Brute-force",
          "AttackerIp":"172. *. *.105",
          "AssetName":"monodb****",
          "SourceFromIp":"172. *. *.105",
          "AssetPrivateIps":"172. *. *.92",
          "AssetType":"ECS",
          "UserId":163957166417****,
          "AssetPublicIps": "",
          "Asset":"0fbc7e34-b1f6-4eeb-b100-130c15eb1c3b",
          "RaisedTime":1572921381000
        }
      ],
      "PageNo":1
    }
  },
  "requestId":"69C66589-F448-4A47-BFEA-EC12F55DCB53",
  "success":true
}
```

Error codes

For a list of error codes, visit the [Error codes](#).

10.1.2. DescribeAlarms

You can call this operation to query security alerts on users or on the platform based on specified conditions.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeAlarms</i> .

Parameter	Type	Required	Description
DataScope	Integer	Yes	Specifies whether the alerts on users or the platform are queried. Valid values: 0: platform 1: users
SourceFrom	Integer	No	The data source of security alerts.
UserId	Long	No	The ID of the department to query.
PageSize	Integer	Yes	The number of alerts to return on each page.
PageNo	Integer	Yes	The number of the page to return.
AlarmType	String	No	The type of the alerts to query.
ProcessState	Integer	No	The processing status of the alerts to query.
KeyWord	String	No	The keywords of the alerts or keywords in the ID or names of assets related to the alerts.
RiskLevels	List<Integer>	No	The risk levels of the alerts to query.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
AlarmId	Long	The ID of the alert.
RiskLevel	Integer	The risk level of the alert.
AlarmName	String	The name of the alert.
AssetType	String	The type of the asset.
Asset	String	The ID of the asset.
UserName	String	The user name.
UserId	Long	The ID of the user or platform.
RaisedTime	Long	The time when the alert was generated.
ProcessState	Integer	The processing status of the alert.

Parameter	Type	Description
AlarmType	String	The type of the alert.
SourceFrom	Integer	The data source of the alert.
AttackerIp	String	The IP address of the attacker.
AssetName	String	The name of the asset.
AssetPublicIps	String	The public IP address of the affected asset.
AssetPrivateIps	String	The internal IP address of the affected asset.
AlarmUniqueInfo	String	The unique key of the alert.
LastTime	String	The last time when the alert was generated.
Total	Integer	The total number of entries returned.

Examples

Sample requests

```
http(s)://yundunnewsoc-pop.[RegionId].example.com/? Action=DescribeAlarms
&RiskLevels=[0,1,2]
&DataScope=1
&PageSize=20
&PageNo=1
&<Common request parameters>
```

Sample success responses in JSON format

```
{
  "code":200,
  "data":{
    "Data":{
      "PageSize":20,
      "Total":177,
      "Items":[
        {
          "AlarmId":30307,
          "UserName":"yundun****",
          "AlarmType":"Malicious Process",
          "SourceFrom":20,
          "AssetName":"yun****",
          "AssetPrivateIps":"192. *. *.1",
          "ProcessState":1,
          "AssetType":"ECS",
          "AlarmName":"Mining process",
          "UserId":1****,
          "AlarmUniqueInfo":"34dsal",
          "AssetPublicIps":"10. *. *.1",
          "Asset":"2f43eb69-****",
          "RaisedTime":1571826361000,
          "RiskLevel":2,
          "LastTime":1573021501000
        }
      ],
      "PageNo":1
    }
  },
  "requestId":"B2C5D1EB-202F-4132-A763-2D16538B****",
  "success":true
}
```

Error codes

For a list of error codes, visit the [Error codes](#).

10.1.3. DescribeVulFrangs

You can call this operation to query vulnerabilities.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeVulFrangs</i> .
UserId	Long	No	The ID of the department to query.
RiskLevels	Integer	No	The severity of the vulnerabilities to query.

Parameter	Type	Required	Description
ProcessState	Integer	No	The processing status of the vulnerabilities to query.
Page	Integer	Yes	The number of the page to return.
PageSize	Integer	Yes	The number of entries to return on each page.
VulType	String	No	The type of the vulnerabilities to query.
KeyWord	String	No	The name of the vulnerability or asset to query.
DataScope	Integer	Yes	Specifies whether the data of users or the platform is queried. Valid values: • 0: platform • 1: users
NeedFix	String	No	Specifies whether the vulnerabilities to query require fixes.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
PageSize	Integer	The number of entries returned per page.
PageNo	Integer	The page number of the returned page.
Total	Integer	The number of entries returned.
Items	Array	The list of vulnerabilities.
└LastTime	Long	The last time when the vulnerability was detected.
└RiskLevel	Integer	The severity of the vulnerability.
└ProcessState	Integer	The processing status of the vulnerability.
└AssetType	String	The type of the affected asset.
└NeedFix	String	Indicates whether the vulnerability requires a fix.
└VulRelated	String	The ID of the vulnerability details.
└Asset	String	The ID of the asset affected by the vulnerability.
└SourceFrom	Integer	The data source.

Parameter	Type	Description
Id	Long	The ID of the vulnerability.
RaisedTime	Long	The first time when the vulnerability was detected.
VulName	String	The name of the vulnerability.
VulType	String	The type of the vulnerability.
AssetPublicIps	String	The public IP address of the affected asset.
AssetPrivateIps	String	The internal IP address of the affected asset.
AssetName	String	The name of the affected asset.

Examples

Sample requests

```
http(s)://yundunnewsoc-pop.[RegionId].example.com/? Action=DescribeVulFrangs
&DataScope=1
&PageSize=20
&Page=1
&<Common request parameters>
```

Sample success responses in JSON format

```
{
  "code":200,
  "data":{
    "Data":{
      "PageSize":20,
      "Total":445,
      "Items":[
        {
          "ProcessState":1,
          "AssetType":"ECS",
          "NeedFix":"later",
          "VulRelated":"CVE-2016-5195",
          "Asset":"eb9ea4b0-****",
          "SourceFrom":1,
          "Id":6370,
          "RaisedTime":2019,
          "RiskLevel":1,
          "VulName":"RHSA-2017:0372: kernel-aarch64 security and bug fix update",
          "LastTime":"2019-11-05 17:12:12",
          "VulType":"cve"
        }
      ],
      "PageNo":1
    }
  },
  "requestId":"32B57B56-958C-49C5-BB49-0BABE2060305",
  "success":true
}
```

Error codes

For a list of error codes, visit the [Error codes](#).

10.1.4. DescribeHcFrangs

You can call this operation to query the risks in the server configurations set by the user.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeHcFrangs</i> .
ProcessState	Integer	No	The processing status of the risks to query.
HcType	String	No	The type of server configuration risks to query.
Page	Integer	Yes	The number of the page to return.

Parameter	Type	Required	Description
PageSize	Integer	Yes	The number of entries to return on each page.
KeyWord	String	No	The server baseline name or asset name.
DataScope	Integer	Yes	Specifies whether the data of users or the platform is queried. Valid values: 0: platform 1: users
UserId	Long	No	The ID of the department to query.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
PageSize	Integer	The number of entries returned per page.
PageNo	Integer	The page number of the returned page.
Total	Integer	The total number of the returned entries.
Items	Array	The list of servers that SOC is authorized to scan.
└LastFoundTime	Long	The last time when risks were detected.
└RiskLevel	Integer	The level of the risk. Valid values: 0: low 1: medium 3: high
└ProcessState	Integer	The processing status of the risk. 1: handled 2: unhandled
└HcName	String	The name of the server configuration risk.
└HcType	String	The type of the server configuration risk.
└UserName	String	The name of the department to which the affected asset belongs.
└UserId	Long	The ID of the department to which the affected asset belongs.
└SourceFrom	Integer	The data source.

Parameter	Type	Description
Id	Long	The ID of the entry.
Asset	String	The ID of the affected asset.
AssetType	String	The type of the affected asset.
AssetName	String	The name of the affected asset.
AssetPublicIps	String	The public IP address of the affected asset.
AssetPrivateIps	String	The internal IP address of the affected asset.

Examples

Sample requests

```
http(s)://yundunnewsoc-pop.[RegionId].example.com/? Action=DescribeHcFrangs
&DataScope=1
&PageSize=20
&Page=1
&<Common request parameters>
```

Sample success responses in JSON format


```
{
  "code":200,
  "data":{
    "Data":{
      "PageSize":20,
      "Total":47,
      "Items":[
        {
          "UserName":"yun****",
          "SourceFrom":2,
          "HcType":"Alibaba Cloud",
          "AssetName":"yun3 ",
          "LastFoundTime":"2019-11-06 01:03:55",
          "AssetPrivateIps":"192. *. *.1",
          "ProcessState":1,
          "HcName":"Alibaba Cloud Standard",
          "AssetType":"ECS",
          "UserId":11424,
          "AssetPublicIps":"10. *. *.1",
          "Asset":"71513dfc ",
          "Id":111,
          "RiskLevel":2
        }
      ],
      "PageNo":1
    }
  },
  "requestId":"FE7137B7-84D8-4AF7-969B-C0DF5118****",
  "success":true
}
```

Error codes

For a list of error codes, visit the [Error codes](#).

10.2. SOAR

10.2.1. Playbooks

10.2.1.1. ModifyPlaybook

Modifies a playbook.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	ModifyPlaybook	The operation that you want to perform. Set the value to ModifyPlaybook .
DisplayName	String	Yes	Test 1	The display name of the playbook.
PlaybookId	Integer	Yes	582	The ID of the playbook.
Taskflow	String	No	XXX	The configuration file of the playbook.
Description	String	No	Demo playbook	The description of the playbook.
InputType	String	No	event	The input type. Set the value to event .
OperateType	String	No	general	The operation type of the playbook. Set the value to general .
OwnType	String	No	user	The ownership type of the playbook. Valid values: user: custom sys: built-in
ExecuteMode	String	No	one	The execution method of the playbook in the production environment. Valid values: one: The playbook is manually run. mul: The playbook is run based on scheduling configurations. stream: The playbook is run based on streaming data.
Cron	String	No	0 0 9 * * ?	The scheduling configurations for the playbook.

Response parameters

Parameter	Type	Example	Description

Parameter	Type	Example	Description
RequestId	String	8277EDCA-9E03-4102-867E-E346E280865C	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=ModifyPlaybook
&DisplayName=Test 1
&PlaybookId=582
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>8277EDCA-9E03-4102-867E-E346E280865C</RequestId>
```

JSON format

```
{
  "RequestId": "8277EDCA-9E03-4102-867E-E346E280865C"
}
```

10.2.1.2. TriggerPlaybook

Runs a playbook.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	TriggerPlaybook	The operation that you want to perform. Set the value to TriggerPlaybook .
InputParam	String	Yes	{"name":"test","ip":"10.123.10.10"}	The parameters that are used to run the playbook. Specify the custom input parameters of the playbook.
PlaybookName	String	Yes	test_rtap	The name of the playbook that you want to run.

Parameter	Type	Required	Example	Description
PlaybookId	Integer	No	531	The ID of the playbook that you want to run.
TriggerType	String	No	manual	The method for running the playbook.

Response parameters

Parameter	Type	Example	Description
RequestId	String	0E402C78-34DC-4B2B-BB15-73BB914172C1	The ID of the request.
TriggerUuid	String	a5a60946-3ad4-4e0d-92db-500da9619793	The UUID of the task that is generated when the playbook is run. You can stop the task or query the result of the task by using the UUID.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=TriggerPlaybook
&InputParam={"name":"test","ip":"10.123.10.10"}
&PlaybookName=test_rtap
&<Common request parameters>
```

Sample success responses

XML format

```
<TriggerUuid>a5a60946-3ad4-4e0d-92db-500da9619793</TriggerUuid>
<RequestId>0E402C78-34DC-4B2B-BB15-73BB914172C1</RequestId>
```

JSON format

```
{
  "TriggerUuid": "a5a60946-3ad4-4e0d-92db-500da9619793",
  "RequestId": "0E402C78-34DC-4B2B-BB15-73BB914172C1"
}
```

10.2.1.3. PublishPlaybook

Publishes a playbook.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	PublishPlaybook	The operation that you want to perform. Set the value to PublishPlaybook .
PlaybookId	Integer	Yes	531	The ID of the playbook. An ID is generated for each playbook that you create. You can manage playbooks by ID.
Restart	Boolean	Yes	true	Specifies whether to restart the playbook. Valid values: • true: restarts and publishes the playbook after the playbook is stopped. • false: directly publishes the playbook.
State	Boolean	Yes	true	The status of the playbook. Valid values: • true: The playbook is published. • false: The playbook is disabled.
PicUrl	String	No	http://sophon-gen//2018-12-03/-4a86-aa76-8705e4fc6988.jpg	The URL of the image for the playbook.

Response parameters

Parameter	Type	Example	Description
RequestId	String	913BE26B-F9CC-4A84-8CEC-190E4BADD246	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=PublishPlaybook
&PlaybookId=531
&Restart=true
&State=true
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>913BE26B-F9CC-4A84-8CEC-190E4BADD246</RequestId>
```

JSON format

```
{
  "RequestId": "913BE26B-F9CC-4A84-8CEC-190E4BADD246"
}
```

10.2.1.4. StopOneAction

Stops the task that is generated when a playbook is run.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	StopOneAction	The operation that you want to perform. Set the value to StopOneAction .
RequestId	String	Yes	73b14357-e011-4993-a769-bfb779ab3638	The UUID of the task that you want to stop. You can obtain the UUID from TriggerUuid by calling the TriggerPlaybook operation.

Response parameters

Parameter	Type	Example	Description
RequestId	String	C8242F6C-F6E9-491C-AA00-D619224268ED	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=StopOneAction
&RequestId=73b14357-e011-4993-a769-bfb779ab3638
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>C8242F6C-F6E9-491C-AA00-D619224268ED</RequestId>
```

JSON format

```
{
  "RequestId": "C8242F6C-F6E9-491C-AA00-D619224268ED"
}
```

10.2.1.5. DescribePlaybook

Queries the details of a playbook.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribePlaybook	The operation that you want to perform. Set the value to DescribePlaybook .
PlaybookId	Integer	No	597	The ID of the playbook.
PlaybookName	String	No	Portrait_of_victim	The name of the playbook.

Response parameters

Parameter	Type	Example	Description
Playbook	Struct		The details of the playbook.
Active	Boolean	false	The status of the playbook. Valid values: true: The playbook is enabled. false: The playbook is disabled.
Compiledresult	String	""	The compilation result of the playbook.
Creator	String	sys	The user who created the playbook.
Cron	String	0 0 9 * * ?	The scheduling configurations for the playbook.
Description	String	""	The description of the playbook.
DisplayName	String	Test 1	The display name of the playbook.

Parameter	Type	Example	Description
DomainId	String	ids-group	The tenant information of the playbook.
ExecuteMode	String	one	The execution method of the playbook. Valid values: • one: The playbook is manually run. • mul: The playbook is run based on scheduling configurations. • stream: The playbook is run based on streaming data.
GmtCreate	Long	1642066923992	The time at which the playbook was created. The value is a 13-byte timestamp. Unit: milliseconds.
GmtModified	Long	1642066923992	The time at which the playbook was last modified. The value is a 13-byte timestamp. Unit: milliseconds.
Id	Long	582	The ID of the playbook.
InputParams	String	[{"name": "component_name", "dataType": "String", "description": "Component name", "required": false, "stanchDefaultV alue": ""}, {"name": "version", "dataType": "String", "description": "Component version", "required": false, "stanchDefault Value": ""}]	The input parameters of the playbook.
Inputtype	String	event	The input type.
Modifier	String	yundunluck	The user who last modified the playbook.
Name	String	Test 1	The name of the playbook.

Parameter	Type	Example	Description
OnlineActive	Boolean	false	The status of the playbook. Valid values: true: The playbook is enabled. false: The playbook is disabled.
OnlineCompiled result	String	""	The compilation result of the playbook in the production environment.
OnlineExecuteMode	String	one	The execution method of the playbook in the production environment. Valid values: one: The playbook is manually run. mul: The playbook is run based on scheduling configurations. stream: The playbook is run based on streaming data.
OnlineOss	String	sophon-gen/23cf45b4-ab29-4e36-accb-ba81cd3cc999-1641814492160-beaver_linkage_attack_ban_v62_test.jar	The Object Storage Service (OSS) storage path that is used for the compilation result of the playbook in the production environment.
OperateType	String	general	The operation type of the playbook.
Oss	String	sophon-gen/23cf45b4-ab29-4e36-accb-ba81cd3cc999-1641814492160-beaver_linkage_attack_ban_v62_test.jar	The OSS storage path that is used for the compilation result of the playbook.
Owner	String	sys	The owner of the playbook.
Taskconfig	String	{ "apps": [{ "actions": [{ "customInput": true, "description": "Call an API operation", "id": 0, "name": "executeAPI" }] }] }	The configuration file of the playbook.

Parameter	Type	Example	Description
Taskflow	String	<?xml version=\"1.0\" encoding=\"UTF-8\"?> <bpmn:definitions xmlns:xsi=\"http:// www.w3.org/2001/ XMLSchema- instance\"	The information about the component on which the playbook depends.
TenantId	String	baba	The tenant information.
TriggerInfo	String	{\"Query start time\":\"2022-01-05 10:10:10\",\"Query end time\":\"2022-01- 05 10:10:10\"}	The information that is used to manually run the playbook.
ownType	String	user	The ownership type of the playbook. Valid values: • user: custom • sys: built-in
RequestId	String	65C02B7B-C23D- 4929-A378- 11EB59813141	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribePlaybook  
&<Common request parameters>
```

Sample success responses

XML format

```
<Playbook>
  <Owner>sys</Owner>
  <Description>""</Description>
  <GmtModified>1642066923992</GmtModified>
  <Creator>sys</Creator>
  <OnlineExecuteMode>one</OnlineExecuteMode>
  <Cron>0 0 9 * * ?</Cron>
  <Taskconfig>{"apps":[{"actions":[{"customInput":true,"description":"Call an AP
I operation","id":0,"name":"executeAPI"}]}</Taskconfig>
  <Name>Test 1</Name>
  <Compiledresult>""</Compiledresult>
  <InputParams>[{"name":"component_name","dataType":"String","description":"Component nam
e","required":false,"stanchDefaultValue":""}, {"name":"version","dataType":"String","descrip
tion":"Component version","required":false,"stanchDefaultValue":""}]</InputParams>
  <OnlineActive>>false</OnlineActive>
  <DisplayName>Test 1</DisplayName>
  <Inputtype>event</Inputtype>
  <ExecuteMode>one</ExecuteMode>
  <Modifier>yundunluck</Modifier>
  <OperateType>general</OperateType>
  <Taskflow>&lt;?xml version="1.0" encoding="UTF-8"?&gt;&lt;bpmn:definitions xmlns:xs
i="http://www.w3.org/2001/XMLSchema-instance"></Taskflow>
  <TriggerInfo>{"Query start time":"2022-01-05 10:10:10","Query end time":"2022-01-05 10:
10:10"}</TriggerInfo>
  <Oss>sophon-gen/23cf45b4-ab29-4e36-accb-ba81cd3cc999-1641814492160-beaver_linkage_attac
k_ban_v62_test.jar</Oss>
  <TenantId>baba</TenantId>
  <GmtCreate>1642066923992</GmtCreate>
  <Active>>false</Active>
  <DomainId>ids-group</DomainId>
  <OnlineOss>sophon-gen/23cf45b4-ab29-4e36-accb-ba81cd3cc999-1641814492160-beaver_linkage
_attack_ban_v62_test.jar</OnlineOss>
  <ownType>user</ownType>
  <OnlineCompiledresult>""</OnlineCompiledresult>
  <Id>582</Id>
</Playbook>
<RequestId>65C02B7B-C23D-4929-A378-11EB59813141</RequestId>
```

JSON format

```
{
  "Playbook": {
    "Owner": "sys",
    "Description": "\\\"\\\",
    "GmtModified": 1642066923992,
    "Creator": "sys",
    "OnlineExecuteMode": "one",
    "Cron": "0 0 9 * * ?",
    "Taskconfig": "{\\\"apps\\\":[{\\\"actions\\\":[{\\\"customInput\\\":true,\\\"description\\\":\\\"Call an API operation\\\",\\\"id\\\":0,\\\"name\\\":\\\"executeAPI\\\",
    "Name": "Test 1",
    "Compiledresult": "\\\"\\\",
    "InputParams": "[{\\\"name\\\":\\\"component_name\\\",\\\"dataType\\\":\\\"String\\\",\\\"description\\\":\\\"Component name\\\",\\\"required\\\":false,\\\"stanchDefaultValue\\\":\\\"\\\",{\\\"name\\\":\\\"version\\\",\\\"dataType\\\":\\\"String\\\",\\\"description\\\":\\\"Component version\\\",\\\"required\\\":false,\\\"stanchDefaultValue\\\":\\\"\\\"}]",
    "OnlineActive": false,
    "DisplayName": "Test 1",
    "Inputtype": "event",
    "ExecuteMode": "one",
    "Modifier": "yundunluck",
    "OperateType": "general",
    "Taskflow": "<?xml version=\\\"1.0\\\" encoding=\\\"UTF-8\\\"?><bpmn:definitions xmlns:xsi=\\\"http://www.w3.org/2001/XMLSchema-instance\\\",
    "TriggerInfo": "{\\\"Query start time\\\":\\\"2022-01-05 10:10:10\\\",\\\"Query end time\\\":\\\"2022-01-05 10:10:10\\\"}",
    "Oss": "sophon-gen/23cf45b4-ab29-4e36-accb-ba81cd3cc999-1641814492160-beaver_linkage_attack_ban_v62_test.jar",
    "TenantId": "baba",
    "GmtCreate": 1642066923992,
    "Active": false,
    "DomainId": "ids-group",
    "OnlineOss": "sophon-gen/23cf45b4-ab29-4e36-accb-ba81cd3cc999-1641814492160-beaver_linkage_attack_ban_v62_test.jar",
    "ownType": "user",
    "OnlineCompiledresult": "\\\"\\\",
    "Id": 582
  },
  "RequestId": "65C02B7B-C23D-4929-A378-11EB59813141"
}
```

10.2.1.6. DescribeSoarRecords

Queries the execution history of a playbook.

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeSoarRecords	The operation that you want to perform. Set the value to DescribeSoarRecords .
PageNumber	Integer	Yes	1	The number of the page to return.
PageSize	Integer	Yes	20	The number of entries to return on each page.
QueryCondition	String	Yes	<pre>{\"type\": \"complex\", \"condition\": {\"condition\": {\"AND\": {\"rules\": [{\"field\": \"taskName\", \"match\": \"is\", \"type\": \"string\", \"value\": \"test_rtap\"}]}}}</pre>	The query conditions. The value of this parameter includes the following fields: • field: the field to match. • value: the value to match. • type: the type of match that you want to perform. Valid values: ◦ match: EQUALS TO. ◦ contains: CONTAINS. ◦ complex: a nested query. You must specify a nested query based on the description for QueryCondition.
TaskUuid	String	No	73b14357-e011-4993-a769-bfb779ab3638	The UUID of the task that is generated when the playbook is run. You can obtain the UUID from TriggerUuid by calling the TriggerPlaybook operation. If you specify TriggerUuid , the value of QueryCondition does not take effect.

Response parameters

Parameter	Type	Example	Description
PageNumber	Integer	1	The page number of the returned page.
PageSize	Integer	20	The number of entries returned per page.
RequestId	String	B57576EA-1F92-4810-8CC7-B27FEE6CD9DE	The ID of the request.

Parameter	Type	Example	Description
SoarExecuteRecords	Array of SoarExecuteRecord		An array that consists of details of the execution history.
All	Integer	1	The number of times that the playbook is run.
DataSourceName	String	4357	The name of the data source that triggers the playbook.
EndTime	Long	1641460993364	The time at which the playbook stops running. The value is a 13-byte timestamp. Unit: milliseconds.
EventId	String	1641460993340	The ID of the event that triggers the playbook.
RawEventReq	String	{\"ac\": \"c60dcd29f8b0acc18028d0dc82d73d3b\", \"dataSourceName\": \"4357\", \"domainId\": \"ids-group\", \"eventId\": \"1641460993340\", \"eventStr\": {}, \"taskList\": [\"test_rtap\"], \"taskTriggerList\": [], \"tenantId\": \"baba\", \"triggerType\": \"manual\", \"triggerUser\": \"sys\", \"ts\": \"1641460993340\"}	The detailed raw data about how the playbook is triggered.
RequestUuid	String	a5a60946-3ad4-4e0d-92db-500da9619793	The UUID of the task that is generated when the playbook is run.
ResultLevel	String	DEBUG	The log level of the execution result for the playbook. Valid values: - DEBUG - INFO - ERROR

Parameter	Type	Example	Description
ResultMessage	String	""	The message of the execution result for the playbook.
Sao	String	test_rtap	The name of the playbook.
Saold	Long	531	The ID of the playbook.
SrcIp	String	10.10.XX.XX	The IP address of the server on which the playbook is run.
StartTime	Long	1641460993348	The time at which the playbook starts to run. The value is a 13-byte timestamp. Unit: milliseconds.
Status	String	success	The execution result. Valid values: • success • failed • inprogresss
Success	Integer	1	The number of successful tasks.
TaskName	String	test_rtap	The name of the task.
TaskUuid	String	cfa5cc68-9279-45fa-88a0-c79cca020efe	The UUID of the task.
TriggerDataId	String	1641460993340	The ID of the data source that triggers the playbook.
TriggerType	String	manual	The method for running the playbook.
TriggerUser	String	12385**452	The user who triggers the playbook. The value is the ID of the account that is used for logon and API calls.
resultMessage	String	""	The information about the execution result for the playbook. This parameter is deprecated.

Parameter	Type	Example	Description
TotalCount	Integer	23	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeSoarRecords
&PageNumber=1
&PageSize=20
&QueryCondition={"type":"complex","condition":{"condition":{"AND":"","rules":{"field":"taskName","match":{"is":"","type":"","string":"","value":["test_rtap"]}}}}}
```

&<Common request parameters>

Sample success responses

XML format

```
<TotalCount>23</TotalCount>
<PageSize>20</PageSize>
<RequestId>B57576EA-1F92-4810-8CC7-B27FEE6CD9DE</RequestId>
<PageNumber>1</PageNumber>
<SoarExecuteRecords>
  <Status>success</Status>
  <Sao>test_rtap</Sao>
  <All>1</All>
  <TriggerType>manual</TriggerType>
  <SaoId>531</SaoId>
  <EndTime>1641460993364</EndTime>
  <TaskUuid>cfa5cc68-9279-45fa-88a0-c79cca020efe</TaskUuid>
  <StartTime>1641460993348</StartTime>
  <resultMessage>"</resultMessage>
  <ResultMessage>"</ResultMessage>
  <SrcIp>10.10.XX.XX</SrcIp>
  <Success>1</Success>
  <TriggerUser>12385**452</TriggerUser>
  <TriggerDataId>1641460993340</TriggerDataId>
  <ResultLevel>DEBUG</ResultLevel>
  <TaskName>test_rtap</TaskName>
  <DataSourceName>4357</DataSourceName>
  <EventId>1641460993340</EventId>
  <RequestUuid>a5a60946-3ad4-4e0d-92db-500da9619793</RequestUuid>
  <RawEventReq>{"ac":"c60dcd29f8b0acc18028d0dc82d73d3b","dataSourceName":"4357","domainId":"ids-group","eventId":"1641460993340","eventStr":{"taskList":["test_rtap"],"taskTriggerList":[]},"tenantId":"baba","triggerType":"manual","triggerUser":"sys","ts":"1641460993340"}</RawEventReq>
</SoarExecuteRecords>
```

JSON format


```
{
  "TotalCount": 23,
  "PageSize": 20,
  "RequestId": "B57576EA-1F92-4810-8CC7-B27FEE6CD9DE",
  "PageNumber": 1,
  "SoarExecuteRecords": {
    "Status": "success",
    "Sao": "test_rtap",
    "All": 1,
    "TriggerType": "manual",
    "SaoId": 531,
    "EndTime": 1641460993364,
    "TaskUuid": "cfa5cc68-9279-45fa-88a0-c79cca020efe",
    "StartTime": 1641460993348,
    "resultMessage": "\\\"\\\"\\\"\\\",
    "ResultMessage": "\\\"\\\"\\\"\\\",
    "SrcIp": "10.10.XX.XX",
    "Success": 1,
    "TriggerUser": "12385**452",
    "TriggerDataId": 1641460993340,
    "ResultLevel": "DEBUG",
    "TaskName": "test_rtap",
    "DataSourceName": 4357,
    "EventId": 1641460993340,
    "RequestUuid": "a5a60946-3ad4-4e0d-92db-500da9619793",
    "RawEventReq": "{\\\"ac\\\":\\\"c60dcd29f8b0acc18028d0dc82d73d3b\\\",\\\"dataSourceName\\\":\\\"4357\\\",\\\"domainId\\\":\\\"ids-group\\\",\\\"eventId\\\":\\\"1641460993340\\\",\\\"eventStr\\\":{\\\",\\\"taskList\\\":[\\\"test_rtap\\\"],\\\"taskTriggerList\\\":[],\\\"tenantId\\\":\\\"baba\\\",\\\"triggerType\\\":\\\"manual\\\",\\\"triggerUser\\\":\\\"sys\\\",\\\"ts\\\":\\\"1641460993340\\\"}\\\"\\\""}
  }
}
```

10.2.2. Intelligence

10.2.2.1. SyncBanRecord

Synchronizes blocking records.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	SyncBanRecord	The operation that you want to perform. Set the value to SyncBanRecord .

Parameter	Type	Required	Example	Description
BanType	String	Yes	ban-whole	The type of the blocking operation. You can specify this parameter based on your business requirements. The type of the blocking operation is returned when you unblock a threat indicator.
EndTime	Long	Yes	-1	The end of the time range during which a threat indicator is blocked. The value is a 13-byte timestamp. Unit: milliseconds. If a threat indicator is permanently blocked, set the value to -1.
Entity	String	Yes	12.12.XX.XX	The value of the blocked threat indicator.
EntityType	String	Yes	IP	The type of the blocked threat indicator. Valid values include IP and file_hash .
PolicyId	String	Yes	23	The ID of the blocking rule that triggers the blocking operation. The ID is specified in the system that performs the blocking operation.
RuleConfig	String	Yes	{}	The custom configurations of the blocking rule.
StartTime	Long	Yes	1640169543000	The beginning of the time range during which a threat indicator is blocked. The value is a 13-byte timestamp. Unit: milliseconds.
TaskName	String	No	Test blocking record	The name of the task.
EventUuid	String	No	3BB85AD2-E1D2-45C5-B22B-949CBC9BD98B	The UUID of the case.

Response parameters

Parameter	Type	Example	Description
Id	Long	10	The ID of the blocking result.
RequestId	String	3BB85AD2-E1D2-45C5-B22B-949CBC9BD98B	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=SyncBanRecord
&BanType=ban-whole
&EndTime=-1
&Entity=12.12.XX.XX
&EntityType=IP
&PolicyId=23
&RuleConfig={}
&StartTime=1640169543000
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>3BB85AD2-E1D2-45C5-B22B-949CBC9BD98B</RequestId>
<Id>10</Id>
```

JSON format

```
{
  "RequestId": "3BB85AD2-E1D2-45C5-B22B-949CBC9BD98B",
  "Id": 10
}
```

10.2.3. Cases

10.2.3.1. CreateEventByAlert

Creates a case based on a threat event that is reported by Security Operations Center (SOC).

Request parameters

Parameter	Type	Required	Example	Description

Parameter	Type	Required	Example	Description
Action	String	Yes	CreateEventByAlert	The operation that you want to perform. Set the value to CreateEventByAlert .
DocId	String	No	1234567	The docId of the threat event data in an Elasticsearch index.
BatchCode	String	No	20212045	The batch code of the threat event data. You can use the code to associate the threat event with raw error logs.
EsIndex	String	No	soc-alarms____2021.12.2	The name of the Elasticsearch index to which the threat event belongs.
Name	String	No	SOAR-Webshell event	The name of the case.
Severity	String	No	information	The severity of the threat event. Valid values: 1. information 2. suspicious 3. general 4. serious 5. urgent
Type	String	No	networkScanning	The type of the threat event. Valid values: 1. networkScanning 2. exploitVulnerability 3. maliciousSoftware 4. networkAttack 5. riskConnection 6. abnormalBehavior 7. illegalAccount
SourceIps	String	No	[{"ip": "12.12.XX.XX", "port": 123, "location": "China"}]	The list of source IP addresses.

Parameter	Type	Required	Example	Description
DestIps	String	No	[{"ip":"12.12.XX.XX","port":123,"location":"China"}]	The list of destination IP addresses.
StartTime	Long	No	1641540484251	The start time of the case. The value is a 13-byte timestamp. Unit: milliseconds.
ThreatTime	Long	No	1641540484251	The beginning of the time range for the threat event. The value is a 13-byte timestamp. Unit: milliseconds.
EndTime	Long	No	1641540484251	The end time of the case. The value is a 13-byte timestamp. Unit: milliseconds.
AttCks	String	No	attack	The name of the Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) stage.
Suggestions	String	No	Handling suggestion	The suggestions to handle the threat event.
Description	String	No	Threat description	The description of the threat event.

Response parameters

Parameter	Type	Example	Description
Id	Long	12	The ID of the case.
RequestId	String	3BB85AD2-E1D2-45C5-B22B-949CBC9BD98B	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=CreateEventByAlert
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>3BB85AD2-E1D2-45C5-B22B-949CBC9BD98B</RequestId>
<Id>12</Id>
```

JSON format

```
{
  "RequestId": "3BB85AD2-E1D2-45C5-B22B-949CBC9BD98B",
  "Id": 12
}
```

10.2.4. Tasks

10.2.4.1. DescribeManualTaskInfo

Queries the execution results.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	DescribeManualTaskInfo	The operation that you want to perform. Set the value to DescribeManualTaskInfo .
NeedDataInfo	Boolean	Yes	true	Specifies whether to return details. Valid values: true: yes false: no
PageNumber	Integer	Yes	10	The number of the page to return.
PageSize	Integer	Yes	1	The number of entries to return on each page.
Id	Long	No	1	The ID of the task.
NodeName	String	No	test	The name of the node.
TaskUuid	String	No	13123233	The UUID of the task.

Response parameters

Parameter	Type	Example	Description
ManualTaskRecords	Array of SaoManualTaskInfoDO		An array that consists of details about the task.
ActionUuid	String	AF2B656D-C2C1-4E47-85FD-1596C83C6B86	The UUID of the action.
ActualDealedTime	Long	1641803299000	The time at which the task is handled.
ActualDealerId	String	1	The ID of the user who handled the task.
AkkaActorInfo	String	test	The actor information in Akka.
AssignedUserGroup	String	test	The name of the user group.
AssignedUserId	String	test	The ID of the user.
Content	String	Data information	The content.
DataInfo	String	{"k":"value"}	The data information.
DataUrl	String	http://xxxxxx	The data URL.
DeadlineTime	Long	1641803299000	The deadline for handling the task.
DisplayActionUuid	String	AF2B656D-C2C1-4E47-85FD-1596C83C6B86	The display UUID of the action.
DownloadUrl	String	http://xxxxxx	The download URL.
GmtCreate	Long	1641803299000	The creation time.
GmtModified	Long	1641803299000	The modification time.
Id	Long	1231	The ID of the node.

Parameter	Type	Example	Description
NeedDataInfo	Boolean	true	Indicates whether data information is required.
NodeName	String	test	The name of the node.
PageConfigId	Long	1	The ID of the page configuration.
PlaybookId	Long	1	The ID of the playbook.
PlaybookName	String	test	The name of the playbook.
Status	Integer	0	The status of the task. If this parameter is not specified, all tasks are queried. Valid values: • -1: handling not required • 0: unhandled • 1: handled • 2: unhandled after the deadline
TaskType	Integer	1	The type of the task. Valid values: • 0: manual handling • 1: notification
TaskUuid	String	AF2B656D-C2C1-4E47-85FD-1596C83C6B86	The UUID of the task.
TenantId	String	yundun	The ID of the tenant.
Url	String	http://	The data URL.
PageNumber	Long	1	The page number of the returned page.
PageSize	Long	10	The number of entries returned per page.
RequestId	String	AF2B656D-C2C1-4E47-85FD-1596C83C6B86	The ID of the request.

Parameter	Type	Example	Description
TotalCount	Long	100	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=DescribeManualTaskInfo
&NeedDataInfo=true
&PageNumber=10
&PageSize=1
&<Common request parameters>
```

Sample success responses

XML format

```
<TotalCount>100</TotalCount>
<PageSize>10</PageSize>
<RequestId>AF2B656D-C2C1-4E47-85FD-1596C83C6B86</RequestId>
<PageNumber>1</PageNumber>
<ManualTaskRecords>
  <DataInfo>{"k":"value"}</DataInfo>
  <Status>0</Status>
  <ActualDealedTime>1641803299000</ActualDealedTime>
  <ActionUuid>AF2B656D-C2C1-4E47-85FD-1596C83C6B86</ActionUuid>
  <AssignedUserId>test</AssignedUserId>
  <NodeName>test</NodeName>
  <AssignedUserGroup>test</AssignedUserGroup>
  <NeedDataInfo>true</NeedDataInfo>
  <TaskUuid>AF2B656D-C2C1-4E47-85FD-1596C83C6B86</TaskUuid>
  <GmtModified>1641803299000</GmtModified>
  <AkkaActorInfo>test</AkkaActorInfo>
  <PlaybookName>test</PlaybookName>
  <Url>http://</Url>
  <PageConfigId>1</PageConfigId>
  <TenantId>yundun</TenantId>
  <GmtCreate>1641803299000</GmtCreate>
  <Content>Data information</Content>
  <DeadlineTime>1641803299000</DeadlineTime>
  <TaskType>1</TaskType>
  <DataUrl>http://xxxxxx</DataUrl>
  <PlaybookId>1</PlaybookId>
  <Id>1231</Id>
  <DisplayActionUuid>AF2B656D-C2C1-4E47-85FD-1596C83C6B86</DisplayActionUuid>
  <ActualDealerId>1</ActualDealerId>
  <DownloadUrl>http://xxxxxx</DownloadUrl>
</ManualTaskRecords>
```

JSON format

```
{
  "TotalCount": 100,
  "PageSize": 10,
  "RequestId": "AF2B656D-C2C1-4E47-85FD-1596C83C6B86",
  "PageNumber": 1,
  "ManualTaskRecords": {
    "DataInfo": "{\"k\":\"value\"}",
    "Status": 0,
    "ActualDealedTime": 1641803299000,
    "ActionUuid": "AF2B656D-C2C1-4E47-85FD-1596C83C6B86",
    "AssignedUserId": "test",
    "NodeName": "test",
    "AssignedUserGroup": "test",
    "NeedDataInfo": true,
    "TaskUuid": "AF2B656D-C2C1-4E47-85FD-1596C83C6B86",
    "GmtModified": 1641803299000,
    "AkkaActorInfo": "test",
    "PlaybookName": "test",
    "Url": "http://",
    "PageConfigId": 1,
    "TenantId": "yundun",
    "GmtCreate": 1641803299000,
    "Content": "Data information",
    "DeadlineTime": 1641803299000,
    "TaskType": 1,
    "DataUrl": "http://xxxxxx",
    "PlaybookId": 1,
    "Id": 1231,
    "DisplayActionUuid": "AF2B656D-C2C1-4E47-85FD-1596C83C6B86",
    "ActualDealerId": 1,
    "DownloadUrl": "http://xxxxxx"
  }
}
```

10.3. Operations Center

10.3.1. QueryThreats

Queries attack data in the Operations Center dashboard.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryThreats	The operation that you want to perform. Set the value to QueryThreats .

Parameter	Type	Required	Example	Description
FromTime	Long	No	1640944798076	The beginning of the time range to query. Unit: milliseconds.
ToTime	Long	No	1641549603697	The end of the time range to query. Unit: milliseconds.
CurrentPage	Integer	No	1	The number of the page to return.
PageSize	Integer	No	10	The number of entries to return on each page.
Index	String	No	threat	The data index. Set the value to threat .
UserIds	String	No	- 1,295614088888* ***	The ID of the department. You can specify -1 or the ID of a tenant organization. The value -1 specifies that data on the platform side is queried. Separate multiple values with commas (,).
Aliuid	Long	No	1	This parameter is deprecated.
Query	String	No	192.168.XX.XX	The keyword to match. You can specify the IP address of an alerting asset or the IP address in an attack.
ProcessStatus	String	No	1	The handling status. Valid values: • 1: unhandled • 2: handled
ThreatLevel	String	No	1	The risk level of the attack. Valid values: • 1: low • 2: medium • 3: high

Parameter	Type	Required	Example	Description
SrcFrom	String	No	20,40	The source of data. Separate multiple values with commas (,). Valid values: • 20: Server Guard • 40: Web Application Firewall (WAF) • 41: Cloud Firewall • 44: Network Detection and Response (NDR)
ThreatType	String	No	Suspicious process	The type of the alert that is generated for the attack. Valid values include Non-web attack , Precise defense , Web attack , Other , and Suspicious process .
ThreatName	String	No	Suspicious encoded command	The name of the attack.
ProcessWay	String	No	1	The handling method. Valid values: • 0: allow • 1: intercept • 2: ignore • 3: manually handle • 4: batch block • 5: automatically handle • 6: alert • 7: discard • 8: block
ThreatInoutside	String	No	1	The source of the attack. Valid values: • 1: internal attack • 2: external attack
ThreatResult	String	No	Success	The result of the attack. Valid values include Attempt , Success , and Failure .
Lang	String	No	zh_CN	The language of the content within the request and response. Valid values: • zh_CN: Simplified Chinese • zh_TW: Traditional Chinese • en_US: English

Parameter	Type	Required	Example	Description
Tag	String	No	121	The tag.
DestinationIp	String	No	192.168.XX.XX	The attacked IP address.
ThreatSourceIp	String	No	172.12.XX.XX	The source IP address of the attack.
UrlHost	String	No	www.ecs****.com	The website.

Response parameters

Parameter	Type	Example	Description
CurrentPage	Integer	1	The page number of the returned page.
Datas	List	<pre>{"lastTime":1641549724000,"__logTime":1641549724287,"process_way":""}</pre>	The list of data records that are queried from Elasticsearch. Each array in the list represents a data record.
FromTime	Long	1641484800000	The start time of the attack. Unit: milliseconds.
HistogramInterval	Long	0	The interval of the histogram.
PageSize	Integer	10	The number of entries returned per page.
RequestId	String	8010791A-3154-4154-ACB2-866E56A6****	The ID of the request.
ToTime	Long	1641550177290	The end time of the attack. Unit: milliseconds.
Total	Integer	200	The total number of entries returned.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=QueryThreats
&CurrentPage=1
&PageSize=10
&FromTime=1641484800000
&ToTime=1641550177290
&<Common request parameters>
```

Sample success responses

XML format

```
<ToTime>1641550177290</ToTime>
<PageSize>10</PageSize>
<RequestId>8010791A-3154-4154-ACB2-866E56A6****</RequestId>
<HistogramInterval>0</HistogramInterval>
<CurrentPage>1</CurrentPage>
<Datas>{"lastTime":1641549724000,"__logTime":1641549724287,"process_way":""}</Datas>
<Total>200</Total>
<FromTime>1641484800000</FromTime>
```

JSON format

```
{"ToTime":"1641550177290","PageSize":"10","RequestId":"8010791A-3154-4154-ACB2-866E56A6****",
"HistogramInterval":"0","CurrentPage":"1","Datas":{"lastTime":1641549724000,"__logTime":1641549724287,
"process_way":"","Total":200,"FromTime":"1641484800000"}}
```

10.3.2. QueryThreatChartData

Queries the data in a chart of the Operations Center dashboard.

Request parameters

Parameter	Type	Required	Example	Description
Action	String	Yes	QueryThreatChartData	The operation that you want to perform. Set the value to QueryThreatChartData .
FromTime	Long	No	1640944798076	The beginning of the time range to query. Unit: milliseconds.
ToTime	Long	No	1641549603697	The end of the time range to query. Unit: milliseconds.
CurrentPage	Integer	No	1	The number of the page to return.

Parameter	Type	Required	Example	Description
PageSize	Integer	No	10	The number of entries to return on each page.
Index	String	No	threat	The data index. Set the value to threat .
Aliuid	Long	No	1	This parameter is deprecated.
UserIds	String	No	- 1,295614088888* ***	The ID of the department. You can specify -1 or the ID of a tenant organization. The value -1 specifies that data on the platform side is queried. Separate multiple values with commas (,).
Query	String	No	192.168.XX.XX	The keyword to match. You can specify the IP address of an alerting asset or the IP address in an attack.
ProcessStatus	String	No	1	The handling status. Valid values: • 1: unhandled • 2: handled
ThreatLevel	String	No	1	The risk level of the attack. Valid values: • 1: low • 2: medium • 3: high
SrcFrom	String	No	20,40	The source of data. Separate multiple values with commas (,). Valid values: • 20: Server Guard • 40: Web Application Firewall (WAF) • 41: Cloud Firewall • 44: Network Detection and Response (NDR)

Parameter	Type	Required	Example	Description
ThreatType	String	No	Suspicious process	The type of the alert that is generated for the attack. Valid values include Non-web attack , Precise defense , Web attack , Other , and Suspicious process .
ThreatName	String	No	Suspicious encoded command	The name of the attack.
ProcessWay	String	No	1	The handling method. Valid values: • 0: allow • 1: intercept • 2: ignore • 3: manually handle • 4: batch block • 5: automatically handle • 6: alert • 7: discard • 8: block
ThreatInoutside	String	No	1	The source of the attack. Valid values: • 1: internal attack • 2: external attack
ThreatResult	String	No	Success	The result of the attack. Valid values include Attempt , Success , and Failure .
Properties	String	No	<code>{"x_type": "term", "y_config_1": "src_from, count"}</code>	The settings that are used to query the chart. Specify the value in the following JSON format: <code>{"x_type": "term"(X-axis), "y_config_1": "src_from(Y-axis), count(Count)"}</code> .
ChartType	String	No	pie	The type of the chart. Valid values include histogram , bar , line , pie , table , and value .

Parameter	Type	Required	Example	Description
Lang	String	No	zh_CN	The language of the content within the request and response. Valid values: • zh_CN: Simplified Chinese • zh_TW: Traditional Chinese • en_US: English
Tag	String	No	tem	The tag.
Size	String	No	10	The number of entries to return on each page.

Response parameters

Parameter	Type	Example	Description
Data	List	{"20": {"src_from,count":"23507"}}	The list of data records that are queried from Elasticsearch. Each array in the list represents a data record.
RequestId	String	8010791A-3154-4154-ACB2-866E56A6****	The ID of the request.

Examples

Sample requests

```
http(s)://[Endpoint]/?Action=QueryThreatChartData
&CurrentPage=1
&PageSize=10
&FromTime=1641484800000
&ToTime=1641550177290
&<Common request parameters>
```

Sample success responses

XML format

```
<RequestId>8010791A-3154-4154-ACB2-866E56A6****</RequestId>
<Data>{"20":{"src_from,count":"23507"}}</Data>
```

JSON format

```
{"RequestId":"8010791A-3154-4154-ACB2-866E56A6****","Data":{"20":{"src_from,count":"23507"}}
```

11.Security Audit

11.1. APIs

11.1.1. CreateEventType

Description

You can call this operation to create an audit event type.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>CreateEventType</i> .
SourceId	String	Yes	The ID of the log source.
LogType	String	Yes	The log type code.
Name	String	Yes	The name of the audit event type.
Mark	String	Yes	The description of the audit event type.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
EventType	Struct	Information about the created audit event type. For more information, see the following parameter descriptions.
CreateTime	Long	The time when the audit event type was created.
Id	Integer	The ID of the audit event type.
LogType	Integer	The log type code.
Name	String	The audit event type name.
Mark	String	The description of the audit event type.
Reserved	Boolean	Indicates whether this is a system-reserved event type.
SourceId	Integer	The ID of the log source.

Name	Type	Description
SourceName	String	The name of the log source.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=CreateEventType
&LogType=5
&Name=High-risk database query
&Remark=High-risk database query operation
&SourceId=10000
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "4E5FB761-4927-443A-9606-79F22D516BE8",
  "EventType": {
    "CreateTime": 1519810541531,
    "SourceId": 10000,
    "LogType": 5,
    "SourceName": "DRDS Rtools audit log",
    "Id": 10235,
    "Name": "High-risk database query",
    "Reserved": false,
    "Remark": "High-risk database query operation"
  }
}
```

11.1.2. DescribeEventType

Description

You can call this operation to query information about audit event types.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeEventType</i>
PageSize	String	No	The maximum number of records displayed on a page.
CurrentPage	String	No	The current page number.

Name	Type	Required	Description
SourceId	String	No	The ID of the log source. Default value: <i>null</i> . If you do not specify this parameter, the log source ID is null.
LogType	String	No	The code of the log 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.
EventTypeList	Array	The list of audit event types. For more information, see the following parameter descriptions.
CreateTime	Long	The creation time.
Code	String	The code of the audit event type.
Id	Integer	The ID of the audit event type.
LogType	Integer	The code of the log type.
Name	String	The name of the audit event type.
Remark	String	The description of the audit event type.
Reserved	Boolean	Indicates whether this is a reserved event type in the system.
SourceId	Integer	The ID of the log source.
SourceName	String	The name of the log data source.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId ].example.com/?Action=DescribeEventType
&CurrentPage=1
&LogType=1
&PageSize=100
&SourceId=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "1D494150-8CFC-4A53-9AD4-4E7EA5C2C245",
  "TotalCount": 6,
  "PageSize": 20,
  "CurrentPage": 1,
  "EventTypeList": [
    {
      "CreateTime": 1519810541531,
      "SourceId": 10000,
      "LogType": 5,
      "SourceName": "DRDS Rtools Audit Log",
      "Id": 10235,
      "Name": "High-risk query",
      "Reserved": false,
      "Remark": "High-risk database query operation"
    }
  ]
}
```

11.1.3. DeleteEventType

Description

You can call this operation to delete an audit event type.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DeleteEventType</i> .
Id	Integer	Yes	The ID of the audit event type.

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://auditprivate.[ RegionId].example.com/?Action=DeleteEventType
&Id=10001
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "4E5FB761-4927-443A-9606-79F22D516BE8"
}
```

11.1.4. CreateLogFilter

Description

You can call this operation to create a match criterion for audit log query.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>CreateLogFilter</i> .
SourceId	String	Yes	The ID of the log source.
LogType	String	Yes	The type of the log.
Name	String	Yes	The name of the match criterion.
Type	Integer	Yes	The type of the match criterion. Valid values: 1: filters by log. 2: filters by audit event.
Alertable	String	No	Indicates whether alerting is enabled. Valid values: <i>True</i>: indicates that alerting is enabled. <i>False</i>: indicates that alerting is disabled.

Name	Type	Required	Description
Defaultable	String	No	Indicates whether the match criterion is a default match criterion. Valid values: • <i>True</i>: indicates that it is a default match criterion. • <i>False</i>: indicates that it is not a default match criterion.
EndTime	String	No	The end time of the time frame specified for query, in timestamp format.
EventRiskLevel	String	No	The risk level code.
EventType	String	No	The audit event type.
LogAction	String	No	The action to be performed when the criterion is matched.
LogInitiator	String	No	The user that initiates the security audit.
LogOutcome	String	No	The result.
LogReason	String	No	The reason.
LogTarget	String	No	The target.
Query	String	No	The keywords specified for query.
StartTime	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.
LogFilter	Struct	The created match criterion. For more information, see the following parameter descriptions.
CreateTime	Long	The time when the match criterion was created.
EventType	Integer	The audit event type.
Defaultable	Boolean	Indicates whether the match criterion is a default match criterion.
Id	Integer	The ID of the match criterion.
LogType	Integer	The type of the log.

Name	Type	Description
Name	String	The name of the match criterion.
SourceId	Integer	The ID of the log source.
Type	Integer	The match criterion type code.
UserId	String	The ID of the creator.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId].example.com/?Action=CreateLogFilter
&LogType=5
&Name=test
&SourceId=10000
&Type=1
&Alertable=null
&Defaultable=null
&EndTime=null
&EventRiskLevel=null
&EventType=info
&LogAction=null
&LogInitiator=null
&LogOutcome=null
&LogReason=null
&LogTarget=null
&Query=null
&StartTime=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "4320E3EC-AAC0-46BB-9814-4E1DBE550F76",
  "LogFilter": {
    "Type": 1,
    "UserId": 1519714049632764,
    "CreateTime": 1519813584985,
    "SourceId": 10000,
    "LogType": 5,
    "Id": 10109,
    "Name": "test2",
    "Defaultable": false
  }
}
```


11.1.5. DescribeLogFilter

Description

You can call this operation to query audit log filter criteria.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeLogFilter</i> .
SourceId	String	No	The ID of the log source. Default value: <i>null</i> . If you use the default setting, the log source with ID null is used.
LogType	String	No	The type of the log.
Type	Integer	Yes	The type of the filter criteria. Valid values: 1: indicates filtering by log. 2: indicates filtering by audit event.
Count	Integer	No	The number of returned records.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
LogFilterList	Array	A list of filter criteria. For more information, see the following parameter descriptions.
Alertable	Boolean	Indicates whether alerting is enabled.
CreateTime	Long	The time when the criterion was created.
Defaultable	Boolean	Indicates whether the criterion is a default filter criterion.
EndTime	Long	The time when the query was complete.
EventRiskLevel	Integer	The ID of the event risk level.
EventType	Integer	The ID of the event type.

Name	Type	Description
Id	Integer	The ID of the filter criterion.
LogType	Integer	The type of the log.
Name	String	The name of the filter criterion.
LogAction	String	The action to be performed.
LogInitiator	String	The user that sent the log query.
LogOutcome	String	The result.
LogReason	String	The reason.
LogTarget	String	The target.
Query	String	The keywords for query.
StartTime	Long	The start time of the time frame specified for query.
SourceId	Integer	The ID of the log source.
Type	Integer	The code of the filter criterion type.
UserId	String	The ID of the creator.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId].example.com/?Action=DescribeLogFilter
&Count=10
&LogType=1
&SourceId=1
&Type=null
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "6893FB2A-4D4D-4F3B-9963-59D9B9435FDD",
  "LogFilterList": [
    {
      "query": "",
      "EndTime": 0,
      "EventType": 1,
      "SourceId": 10000,
      "CreateTime": 1522315869000,
      "LogType": 5,
      "Starttime": 0,
      "EventRiskLevel": 0,
      "LogTarget": "",
      "Name": "test2",
      "Type": 1,
      "LogAction": "",
      "LogInitiator": "",
      "UserId": "1519714049632764",
      "LogReason": "",
      "LogOutcome": "",
      "Alertable": true,
      "Id": 10130,
      "Defaultable": true
    }
  ]
}
```

11.1.6. DeleteLogFilter

Description

You can call this operation to delete audit log search conditions.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DeleteLogFilter</i> .
Id	Integer	No	The ID of the search condition.

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://auditprivate.[RegionId].example.com/?Action=DeleteLogFilter
&Id=10001
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "4320E3EC-AAC0-46BB-9814-4E1DBE550F76"
}
```

11.1.7. CreateReceiver

Description

Creates an alert recipient for audit events.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>CreateReceiver</i>
Contact	String	Yes	The contact information about the alert recipient.
LogType	String	Yes	The type of log.
Name	String	Yes	The name of the alert recipient.
Type	Integer	Yes	The code of the alert receiving method. Set the value to <i>7</i> . In this case, alerts are sent through emails.
EventRiskLevel	String	Yes	The code of the risk level.
SourceId	String	Yes	The ID of the log source.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.

Parameter	Type	Description
Receiver	Struct	The created alert recipient. For more information, see the following parameter descriptions.
Contact	String	The contact information about the alert recipient.
CreateTime	Long	The time when the alert recipient was created.
EventRiskLevel	Integer	The code of the risk level.
Id	Integer	The ID of the alert recipient.
LogType	Integer	The type of log.
Name	String	The name of the alert recipient.
SourceId	Integer	The ID of the log source.
SourceName	String	The name of the log source.
Type	Integer	The code of the alert receiving method.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=CreateReceiver
&Contact=test@example.com
&EventRiskLevel=1
&LogType=5
&Name=test
&SourceId=100000
&Type=1
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "452C6406-D60E-4E20-A2D3-2AF1BACD24FC",
  "Receiver": {
    "Type": 1,
    "CreateTime": 1519817388511,
    "SourceId": 10000,
    "LogType": 5,
    "SourceName": "DRDS Rtools audit logs",
    "Id": 10010,
    "EventRiskLevel": 1,
    "Name": "test",
    "Contact": "test@example.com"
  }
}
```

11.1.8. DescribeReceiver

Description

Queries information about alert recipients.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeReceiver</i> .
PageSize	String	No	The number of entries to return on each page.
CurrentPage	String	No	The number of the page to return.
Contact	String	No	The contact information about the alert recipient.
LogType	String	No	The type of log.
Name	String	No	The name of the alert recipient.
EventRiskLevel	String	No	The code of the risk level.
SourceId	String	No	The ID of the log source. Default value: <i>null</i> . If you do not specify this parameter, the log source ID is null.
SourceName	String	No	The name of the log source.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
TotalCount	Integer	The number of entries returned.
ReceiverList	Array	The list of alert recipients. For more information, see the following parameter descriptions.
Contact	String	The contact information about the alert recipient.
CreateTime	Long	The time when the alert recipient was created.
EventRiskLevel	Integer	The code of the risk level.
Id	Integer	The ID of the alert recipient.
LogType	Integer	The type of log.
Name	String	The name of the alert recipient.
SourceId	Integer	The ID of the log source.
SourceName	String	The name of the log source.
Type	Integer	The code of the alert receiving method.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=DescribeReceiver
&Contact=null
&CurrentPage=1
&EventRiskLevel=1
&LogType=1
&Name=null
&PageSize=100
&SourceId=1
&SourceName=null
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "AF012FF0-3851-4132-A7A8-3F77DE40BF91",
  "TotalCount": 2,
  "PageSize": 20,
  "CurrentPage": 1,
  "ReceiverList": [
    {
      "Type": 1,
      "CreateTime": 1519817388511,
      "SourceId": 10000,
      "LogType": 5,
      "SourceName": "DRDS Rtools audit logs",
      "Id": 10010,
      "EventRiskLevel": 1,
      "Name": "test",
      "Contact": "test@example.com"
    }
  ]
}
```

11.1.9. DeleteReceiver

Description

You can call this operation to delete an audit event alert recipient.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DeleteReceiver</i> .
Id	Integer	Yes	The ID 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://auditprivate.[ RegionId].example.com/?Action=DeleteReceiver
&Id=10000
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "452C6406-D60E-4E20-A2D3-2AF1BACD24FC"
}
```

11.1.10. CreateRule

Description

You can call this operation to create an audit rule.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>CreateRule</i> .
Alertable	Boolean	Yes	Indicates whether alerting is enabled.
EventTypeId	Integer	Yes	The audit event type code.
LogType	Integer	Yes	The log type code.
RuleName	String	Yes	The name of the audit rule.
AlertActionList	String	No	The alert recipient. Separate multiple alert recipients with commas (,).
EndTime	String	No	The end time in timestamp format.
Expression	String	No	The audit rule expression.
LogAction	String	No	The audit target.
LogInitiator	String	No	The user that initiates the security audit.
LogOutcome	String	No	The auditing result.
LogReason	String	No	The reason.
LogTarget	String	No	The target.
Mark	String	No	Remarks.
StartTime	String	No	The time when the security audit starts, in timestamp format.

Name	Type	Required	Description
EventRiskLevel	String	Yes	The risk level code.
SourceId	String	Yes	The ID of the log source.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Rule	Struct	The created audit rule. For more information, see the following parameter descriptions.
AlertActions	String	The alert recipient.
CreateTime	Long	The time at which the audit rule was created.
EventRiskLevel	Integer	The risk level code.
Enabled	Boolean	Indicates whether the rule is enabled.
Alertable	Boolean	Indicates whether alerting is enabled.
EventTypeId	Integer	The audit event type ID.
EventTypeName	String	The type of the audit event.
Id	Integer	The ID of the audit rule.
LogType	Integer	The type of the log.
Name	String	The name of the audit rule.
Reserved	Boolean	Indicates whether the rule is reserved.
SourceId	Integer	The ID of the log source.
SourceName	String	The name of the log source.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=CreateRule
&Alertable=false
&EventRiskLevel=1
&EventTypeId=10003
&LogType=5
&RuleName=test
&SourceId=10000
&AlertActionList=null
&EndTime=null
&Expression=null
&LogAction=null
&LogInitiator=null
&LogOutcome=null
&LogReason=null
&LogTarget=null
&Remark=null
&StartTime=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "A9B34E07-02E2-4DC7-8A30-27D59E940279",
  "Rule ": [
    {
      "SourceId": 10000,
      "CreateTime": 1519816442199,
      "LogType": 5,
      "Enable": true,
      "EventTypeId": 10003,
      "SourceName": "DRDS Rtools audit log",
      "AlertActions": "",
      "Name": "test2",
      "EventTypeName": "Create",
      "Alertable": false,
      "Id": 25765,
      "EventRiskLevel": 1,
      "Reserved": false
    }
  ]
}
```

11.1.11. DescribeRule

Description

You can call this operation to query audit rules.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeRule</i> .

Name	Type	Required	Description
PageSize	String	No	The maximum number of records displayed on a page.
CurrentPage	String	No	The current page number.
Alertable	Boolean	No	Indicates whether alarming is enabled
Enabled	Boolean	No	Indicates whether the rule is enabled.
EventTypeId	Integer	No	The audit event type code.
LogType	Integer	No	The log type code
Expression	String	No	The expression of the audit rule.
EventRiskLevel	String	No	The risk level code.
SourceId	String	No	The ID of the log source. Default value: <i>null</i> . If you use the default setting, the log source with ID null is used.

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 number of returned records.
RuleList	Struct	A list of audit rules. For more information, see the following parameter descriptions.
AlertActions	String	The alarm recipient.
CreateTime	Long	The time when the audit rule was created.
EventRiskLevel	Integer	The risk level code.
Enabled	Boolean	Indicates whether the rule is enabled.

Name	Type	Description
Alertable	Boolean	Indicates whether alerting is enabled.
EventTypeId	Integer	The ID of the event type.
EventTypeName	String	The name of the event type.
Expression	String	The expression of the audit rule.
SourceName	String	The name of the log source.
Id	Integer	The ID of the audit rule.
LogType	Integer	The type of the log.
Name	String	The name of the audit rule.
Reserved	Boolean	Indicates whether the audit rule is reserved.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId ].example.com/?Action=DescribeRule
&Alertable=true
&CurrentPage=1
&Enabled=true
&EventRiskLevel=1
&EventTypeId=1000
&Expression=null
&LogType=5
&PageSize=100
&SourceId=100000
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "A6204082-0FD3-4F9A-AFAD-1E2E3F56748A",
  "TotalCount": 16,
  "PageSize": 20,
  "CurrentPage": 1,
  "RuleList": [
    {
      "Expression": "( initiator= \"1\" OR initiator= \"2\" OR initiator= \"3\" ) AND ( target INCLUDE \"4\" OR target INCLUDE \"5\" OR target INCLUDE \"6\" ) AND ( action REGEX \"7\" OR action REGEX \"8\" OR action REGEX \"9\" ) AND ( outcome = \"aa\" ) AND ( reason = \"bb\" )",
      "CreateTime": 1513156159000,
      "Type": 1,
      "Enable": true,
      "EventTypeName": "1982",
      "EventTypeId": 10208,
      "Alertable": true,
      "Id": 25740,
      "AlertActions": "",
      "EventRiskLevel": 1,
      "Name": "test2",
      "Reserved": false
    }
  ]
}
```

11.1.12. EnableRule

Description

You can call this operation to enable an audit rule.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>EnableRule</i> .
Id	Integer	Yes	The ID of the audit rule.

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://auditprivate.[ RegionId ].example.com/?Action=EnableRule
&Id=10001
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "A9B34E07-02E2-4DC7-8A30-27D59E940279"
}
```

11.1.13. DisableRule

Description

You can call this operation to disable an audit rule.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DisableRule</i> .
Id	Integer	Yes	The ID of the audit rule.

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://auditprivate.[ RegionId ].example.com/?Action=DisableRule
&Id=10001
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "A9B34E07-02E2-4DC7-8A30-27D59E940279"
}
```

11.1.14. DeleteRule

Description

You can call this operation to delete an audit rule.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DeleteRule</i> .
Id	Integer	Yes	The ID of the audit rule.

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://auditprivate.[RegionId].example.com/?Action=DeleteRule
&Id=10000
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "A9B34E07-02E2-4DC7-8A30-27D59E940279"
}
```

11.1.15. CreateTask

Description

You can call this operation to create an export task.

Request parameters

Name	Type	Required	Description

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>CreateTask</i> .
Type	Integer	Yes	The type of the export task.
Param	String	Yes	The query parameters in JSON format. For information about the parameter format, see the following sample request.

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
Task	Struct	The created export task. For more information, see the following parameter descriptions.
CreateTime	Long	The time when the export task was created.
Id	Integer	The ID of the export task.
Param	String	The query parameters.
Status	Integer	The status of the export task. Valid values: 1: indicates that the task is in preparation. 2: indicates that the task is being executed. 3: indicates that the task is complete. 4: indicates that the task has failed.
Result	String	The task execution result.
Type	Integer	The type 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://auditprivate.[RegionId].example.com/?Action=CreateTask
&Param={"logType":4,"sourceId":"","q":"","name":"Query all","from":1526987580000,"to":1527073980000}
&Type=1
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "5529324A-7E32-414F-8ADD-B7C3FF32EB6E",
  "Task": [
    {
      "Status": 1,
      "Type": 1,
      "CreateTime": 1519814652404,
      "Param": "{}",
      "Id": 10033,
      "Result": ""
    }
  ]
}
```

11.1.16. DescribeTask

Description

Queries information about export tasks.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeTask</i> .
PageSize	String	No	The number of entries to return on each page.
CurrentPage	String	No	The number of the page to return.
Status	Integer	No	The status of the export task.
Type	Integer	No	The type of the export task.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
TotalCount	Integer	The number of entries returned.
TaskList	Array	The list of export tasks. For more information, see the following parameter descriptions.
CreateTime	Long	The time when the export task was created.

Parameter	Type	Description
StartTime	Long	The time when the export task started.
EndTime	Long	The time when the export task ended.
Id	Integer	The ID of the export task.
Param	String	The query parameters.
Status	Integer	The status of the export task. Valid values: • 1: indicates that the task is in preparation. • 2: indicates that the task is running. • 3: indicates that the task is complete. • 4: indicates that the task failed.
Result	String	The result of the export task.
Type	Integer	The type of the export task.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=DescribeTask
&CurrentPage=1
&PageSize=100
&Status=2
&Type=1
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "2CF939E5-A0EF-4C0F-A761-CBC7DF4DE1BD",
  "TotalCount": 18,
  "PageSize": 20,
  "CurrentPage": 1,
  "TaskList": [
    {
      "Status": 1,
      "Type": 1,
      "CreateTime": 1519814652404,
      "StartTime": 1519814652000,
      "EndTime": 1519814653000,
      "Param": "{}",
      "Id": 10033,
      "Result": "{\"url\":\"http://security-auditlog-archive-dev1.oss-cn-hangzhou.example.com/download/20180228184412_243797.log?Expires=1519901052&OSSAccessKeyId=<yourAccessKeyId>&Signature=xxxx%xxxx%3D\"}"
    }
  ]
}
```

11.1.17. DeleteTask

Description

You can call this operation to delete an export task.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DeleteTask</i> .
Id	Integer	Yes	The ID of the export 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://auditprivate.[ RegionId].example.com/?Action=DeleteTask
&Id=10000
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "5529324A-7E32-414F-8ADD-B7C3FF32EB6E"
}
```

11.1.18. DescribeSetting

Description

You can call this operation to query the system parameter settings of security audit.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeSetting</i> .

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
SettingList	Array	The list of system parameters. For more information, see the following parameter descriptions.
Id	Integer	The system parameter ID.
Name	String	The system parameter name.
Remark	String	The system parameter description.
Type	Integer	The data type.
UpdateTime	Long	The last modification time.
Value	String	The system parameter value.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId].example.com/?Action=DescribeSetting
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "0C4EF12F-9736-429F-9A7A-7C0807BFBA91",
  "SettingList": [
    {
      "Type": 2,
      "Value": "2000",
      "UpdateTime": 1517566573000,
      "Id": 10004,
      "Name": "max_day_alert_number",
      "Remark": "The maximum number of alerts reported every day."
    }
  ]
}
```

11.1.19. ModifySetting

Description

You can call this operation to modify the system parameter settings of Security Audit.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>ModifySetting</i> .
Name	String	Yes	The name of the system parameter.
Value	String	Yes	The value of the system parameter.

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://auditprivate.[ RegionId].example.com/?Action=ModifySetting
&Name=max_day_alert_number
&Value=2000
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "0C4EF12F-9736-429F-9A7A-7C0807BFBA91"
}
```

11.1.20. DescribeLogType

Description

You can call this operation to obtain a list of log types.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeLogType</i> .

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
LogTypeList	Array	The list of log types. For more information, see the following parameter descriptions.
Type	Integer	The code of the log type.
Remark	String	The name of the log type.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId].example.com/?Action=DescribeLogType
&CurrentPage=1
&Enabled=true
&LogType=1
&PageSize=100
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "DD601BAA-4B2A-4CB3-954A-4A09A8771233",
  "LogTypeList": [
    {
      "Type": 1,
      "Remark": "Database"
    }
  ]
}
```

11.1.21. DescribeLogSource

Description

You can call this operation to query log source information.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeLogSource</i> .
PageSize	String	No	The maximum number of records displayed on a page.
CurrentPage	String	No	The current page number.
Enabled	Boolean	No	Indicates whether the log source is enabled.
LogType	Integer	No	The log type code.

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 number of returned records.
LogSourceList	Array	A list of log sources. For more information, see the following parameter descriptions.

Name	Type	Description
Alertable	Boolean	Indicates whether alerting is enabled.
Code	String	The log source code.
CreateTime	Long	The time when the log source was created.
Enabled	Boolean	Indicates whether the log source is enabled.
Id	Integer	The ID of the log source.
LogType	Integer	The log type code.
Name	String	The name of the log source.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=DescribeLogSource
&CurrentPage=1
&Enabled=true
&LogType=1
&PageSize=100
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "CEF1CFC8-53E9-45B7-B3FF-730636A5B430",
  "CurrentPage": 1,
  "TotalCount": 13,
  "PageSize": 1000,
  "LogSourceList": [
    {
      "CreateTime": 1497686376000,
      "LogType": 5,
      "Enable": true,
      "Alertable": false,
      "Id": "10000",
      "Code": "drds-rtools",
      "Name": "DRDS Rtools audit log"
    }
  ]
}
```

11.1.22. DescribeLogCountStat

Description

Description

You can call this operation to query raw log statistics.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeLogCountStat</i> .
EndTime	String	No	The end time of the time frame specified for query, in timestamp format.
LogTypeList	String	No	The log type code. Separate multiple log types with commas (,).
StartTime	String	No	The start 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.
StatList	Array	A list of raw log statistics. For more information, see the following parameter descriptions.
LogType	Integer	The log type code.
StatItemList	Array	The raw log statistics. For more information, see the following parameter descriptions.
Capacity	Float	The storage space usage.
Count	Integer	The number of raw log entries.
Time	Long	The time when the statistics were collected, in timestamp format.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId].example.com/?Action=DescribeLogCountStat
&EndTime=1517630399000
&LogTypeList=1,2,3
&StartTime=1517414400000
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "A633CC4C-914E-49D5-8AC2-1A0B82796E66",
  "StatList": [
    {
      "StatItemList": [
        {
          "Time": 1517414400000,
          "Count": 215239,
          "capacity": 356106.0
        }
      ],
      "LogType": 1
    }
  ]
}
```

11.1.23. DescribeLog

Description

Queries the details about raw logs.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeLog</i> .
PageSize	String	No	The number of entries to return on each page.
CurrentPage	String	No	The number of the page to return.
EndTime	String	No	The end of the time range to query. This value is a timestamp.
Query	String	No	The keywords for query.
SourceId	String	No	The ID of the log source. Default value: <i>null</i> . If you do not specify this parameter, the log source ID is null.

Parameter	Type	Required	Description
StartTime	String	No	The start of the time range to query. This value is a timestamp.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
TotalCount	Integer	The number of entries returned.
LogList	Array	The list of raw logs. For more information, see the following parameter descriptions.
LogTime	Long	The time when the log was generated.
Source	String	The name of the log source.
ColumnList	Array	The list of log details. For more information, see the following parameter descriptions.
Key	String	The name of the column.
Value	String	The value of the column.
TokenList	Array	The list of tokens. For more information, see the following descriptions.
Delimit	Boolean	Indicates whether the token is limited.
Work	String	The fixed value of the token.
HistogramList	Array	The information that indicates the number of raw logs. For more information, see the following descriptions.
Completed	Boolean	Indicates whether all of the raw logs that are generated within the specified time range have been collected. If not, the Count parameter shows an estimated value.
Count	Integer	The number of audit events.
EndTime	Long	The end time.
StartTime	Long	The start time.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=DescribeLog
&CurrentPage=1
&EndTime=1517630399000
&PageSize=100
&Query=null
&SourceId=2
&StartTime=1517414400000
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "DD601BAA-4B2A-4CB3-954A-4A09A8771233",
  "TotalCount": 0,
  "PageSize": 20,
  "CurrentPage": 1,
  "HistogramList": [
    {
      "StartTime": 1517414400000,
      "EndTime": 1517630399000,
      "Count": 1,
      "Completed": true
    }
  ],
  "LogList": [
    {
      "ColumnList": [
        {
          "TokenList": [
            {
              "Delimit": true,
              "Word": "a"
            }
          ],
          "Value": "delete",
          "Key": "action"
        }
      ],
      "Source": 1,
      "LogTime": 1517630399000
    }
  ]
}
```

11.1.24. DescribeEventRisk

Description

You can call this operation to query the risk level information of an audit event.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeEventRisk</i> .

Response parameters

Name	Type	Description
RequestId	String	The GUID generated by Alibaba Cloud for the request.
EventRiskList	Array	The list of event risk levels. For more information, see the following parameter descriptions.
Level	Integer	The code of the risk level.
Name	String	The name of the risk level.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=DescribeEventRisk
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "802DD13D-AEDE-4BD0-86B3-2F44D6D867A0",
  "RiskList": [
    {
      "Level": 0,
      "Name": "Global risk"
    }
  ]
}
```

11.1.25. DescribeEventRiskStat

Description

Queries audit event statistics by risk level.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeEventRiskStat</i> .
EndTime	String	No	The end of the time range to query. This value is a timestamp.
LogTypeList	String	No	The code of the log type. Separate multiple codes of log types with commas (,).
StartTime	String	No	The start of the time range to query. This value is a timestamp.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
StatList	Array	The list of audit event statistics. For more information, see the following parameter descriptions.
LogType	Integer	The code of the log type.
StatItemList	Array	The statistical data. For more information, see the following parameter descriptions.
Count	Integer	The number of audit events.
Capacity	Float	The storage space usage.
EventRiskLevel	Integer	The code of the risk level.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=DescribeEventRiskStat
&EndTime=1517630399000
&LogTypeList=1,2,3
&StartTime=1517414400000
&<Common request parameters>
```

- Sample success responses in JSON format

```
{
  "RequestId": "63DDF633-1394-4AEB-A8E3-6467BC23D78D",
  "StatList": [
    {
      "LogType": 1,
      "StatDataList": [
        {
          "EventRiskLevel": 3,
          "Count": 100
        }
      ]
    }
  ]
}
```

11.1.26. DescribeEventTypeStat

Description

You can call this operation to query audit event statistics by event type.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeEventTypeStat</i> .
EndTime	String	No	The end time of the time frame specified for query, in timestamp format.
LogTypeList	String	No	The log type code. Separate multiple log types with commas (,).
StartTime	String	No	The start 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.
StatList	Array	A list of audit event statistics. For more information, see the following parameter descriptions.
Capacity	Float	The storage space usage.
Reserved	Boolean	Indicates whether the audit event type is a default audit event type.
Count	Integer	The number of audit events.
Id	Integer	The audit event type ID.
Name	String	The audit event type name.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId].example.com/?Action=DescribeEventTypeStat
&EndTime=1517630399000
&LogTypeList=1,2,3
&StartTime=1517414400000
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "75F7A5A7-E9E4-476C-8D09-93B00D7EB120",
  "StatList": [
    {
      "Count": 634,
      "Id": 10208,
      "Name": "1982"
    }
  ]
}
```

11.1.27. DescribeEventCountStat

Description

You can call this operation to query audit event statistics.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeEventCountStat</i> .
EndTime	String	No	The end time of the time frame specified for query, in timestamp format.
LogTypeList	String	No	The log type code. Separate multiple log types with commas (.).
StartTime	String	No	The start 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.
StatList	Array	A list of audit event statistics. For more information, see the following parameter descriptions.
LogType	Integer	The log type code.
StatItemList	Array	The audit event information. For more information, see the following parameter descriptions.
Capacity	Float	The storage space usage.
Count	Integer	The number of audit events.
Time	Long	The time when the statistics were collected, in timestamp format.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId ].example.com/?Action=DescribeEventCountStat
&EndTime=1517630399000
&LogTypeList=1,2,3
&StartTime=1517414400000
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId": "63DDF633-1394-4AEB-A8E3-6467BC23D78D",
  "StatList": [
    {
      "Type": 1,
      "StatDataList": [
        {
          "Capacity": 55881.0,
          "Time": 1519228800000,
          "Count": 100
        }
      ]
    }
  ]
}
```

11.1.28. DescribeEvent

Description

Queries audit event details.

Request parameters

Parameter	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeEvent</i> .
PageSize	String	No	The number of entries to return on each page.
CurrentPage	String	No	The number of the page to return.
Alertable	Boolean	No	Specifies whether an alert is triggered.
EndTime	String	No	The end of the time range to query. This value is a timestamp.
EventRiskLevel	Integer	No	The code of the risk level.
EventTypeId	Long	No	The ID of the audit event type.
Keyword	String	No	The keywords for query.
LogAction	String	No	The operation.
LogInitiator	String	No	The initiator.
LogOutcome	String	No	The result.
LogReason	String	No	The reason.

Parameter	Type	Required	Description
LogTarget	String	No	The physical machine on which the operation is performed.
LogType	Integer	No	The code of the log type.
RuleId	Long	No	The ID of the audit rule.
SourceId	String	No	The ID of the log source. Default value: <i>null</i> . If you do not specify this parameter, the log source ID is null.
StartTime	String	No	The start of the time range to query. This value is a timestamp.

Response parameters

Parameter	Type	Description
RequestId	String	The ID of the request.
CurrentPage	Integer	The page number of the returned page.
PageSize	Integer	The number of entries returned per page.
TotalCount	Integer	The number of entries returned.
EventList	Array	The list of audit events. For more information, see the following parameter descriptions.
CreateTime	Long	The time when the audit event was created.
EventRiskLevel	Integer	The code of the risk level.
EventTypeId	Integer	The ID of the audit event type.
EventTypeName	String	The name of the audit event type.
EventTypeReserved	Boolean	Indicates whether the audit event type is the default audit event type.
Id	Integer	The ID of the audit event.
LogAction	String	The operation.
LogContent	String	The log content.
LogInitiator	String	The initiator.
LogMd5	String	The MD5 value of the log file.

Parameter	Type	Description
LogOutcome	String	The result.
LogReason	String	The reason.
LogSha256	String	The SHA-256 value of the log file.
LogTarget	String	The physical machine on which the operation is performed.
LogTime	Long	The time when the log was generated.
LogType	Integer	The code of the log type.
Receivers	String	The alert recipient.
RuleId	Integer	The ID of the audit rule.
SourceId	Integer	The ID of the log source.
SourceName	String	The name of the log source.
HistogramList	Array	The information that indicates the number of audit events. For more information, see the following descriptions.
Completed	Boolean	Indicates whether all of the audit events that occurred within the specified time range have been collected. If not, the Count parameter shows an estimated value.
Count	Integer	The number of audit events.
EndTime	Long	The end time.
StartTime	Long	The start time.

Error codes

For a list of error codes, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=DescribeEvent
&Alertable=yes
&CurrentPage=100
&EndTime=1517414400000
&EventRiskLevel=null
&EventTypeId=1
&Keyword=null
&LogAction=null
&LogInitiator=null
&LogOutcome=null
&LogReason=null
&LogTarget=null
&LogType=2
&PageSize=1
&RuleId=null
&SourceId=1
&SourceIp=x.x.x.x
&StartTime=1517630399000
&<Common request parameters>
```

- Sample success responses in JSON format

```

{
  "RequestId": "DD601BAA-4B2A-4CB3-954A-4A09A8771233",
  "TotalCount": 0,
  "PageSize": 20,
  "CurrentPage": 1,
  "HistogramList": [
    {
      "StartTime": 1517414400000,
      "EndTime": 1517630399000,
      "Count": 1,
      "Completed": true
    }
  ],
  "EventList": [
    {
      "LogInitiator": "histie",
      "LogAction": "insert betorcinol into(unnervous,dreadingly) value('rashti','interscapular');",
      "LogMd5": "",
      "SourceId": 11140,
      "CreateTime": 1519803668679,
      "RuleId": 25728,
      "LogTime": 1519803664000,
      "Receivers": "2:<test01@example.com>;xxx:<test02@example.com>",
      "LogType": 1,
      "EventTypeId": 10208,
      "SourceName": "1585",
      "LogReason": "",
      "LogTarget": "abdominales",
      "LogOutcome": "0",
      "LogSha256": "",
      "LogContent": "{\"_action\":\"insert betorcinol into(unnervous,dreadingly) value('rashti','interscapular');\", \"db\":\" abdominales\", \"origin_time\":\"3189556\", \"hash\":\"1906992916\", \"_initiator\":\"histie\", \"return_rows\":\"14\", \"ip\":\"x.x.x.x\", \"isbind\":\"1\", \"time\":1519803664000, \"latency\":\"533\", \"sql\":\"insert betorcinol into(unnervous,dreadingly) value('rashti','interscapular');\", \"fail\":\"0\", \"_outcome\":\"0\", \"check_rows\":\"561\", \"update_rows\":\"13860\", \"tid\":\"20794\", \"_target\":\" abdominales\", \"user\":\"histie\", \"_access_time\":1519803664000}\",
      "EventTypeName": "1982",
      "Id": 151980366867940****,
      "EventRiskLevel": 1
    }
  ]
}

```

11.1.29. DescribeArchiveCountStat

Description

You can call this operation to query log and event archiving statistics.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeArchiveCountStat</i> .
EndTime	String	No	The end time of the time frame specified for query, in timestamp format.
LogTypeList	String	No	The log type code. Separate multiple log types with commas (,).
StartTime	String	No	The start 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.
StatList	Array	A list of archiving statistics. For more information, see the following parameter descriptions.
LogType	Integer	The log type code.
StatItemList	Array	The archiving information. For more information, see the following parameter descriptions.
Capacity	Float	The storage space used for archiving.
Count	Integer	The number of archives.
Time	Long	The time when the statistics were collected, in timestamp format.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[ RegionId].example.com/?Action=DescribeArchiveCountStat
&EndTime=1517630399000
&LogTypeList=1,2,3
&StartTime=1497516900000
&<Common request parameters>
```


- Sample responses (JSON format)

```
{
  "RequestId": "63DDF633-1394-4AEB-A8E3-6467BC23D78D",
  "StatList": [
    {
      "Type": 1,
      "StatDataList": [
        {
          "Time": 1519228800000,
          "count": 10,
          "capacity": 356106.0
        }
      ]
    }
  ]
}
```

11.1.30. DescribeArchive

Description

You can call this operation to query log and event archive details.

Request parameters

Name	Type	Required	Description
Action	String	Yes	The operation that you want to perform. Set the value to <i>DescribeArchive</i> .
PageSize	String	No	The maximum number of records displayed on a page.
CurrentPage	String	No	The current page number.
EndTime	String	No	The end time, in timestamp format.
LogType	String	No	The log type code.
StartTime	String	No	The start time, in timestamp format.
Type	String	No	The archive type.

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.
ArchiveList	Array	The list of archived data. For more information, see the following parameter descriptions.
CompactAlg	Integer	The type of the compression algorithm.
Count	Integer	The number of records.
CreateTime	Long	The time when the archive was created.
Id	Integer	The ID of the archive.
LogType	Integer	The log type code.
Md5	String	The MD5 value of the archive file.
Name	String	The name of the archive file.
Sha256	String	The SHA256 value of the archive file.
Type	Integer	The archive type.

Error codes

For more information about the error codes that this operation can return, see [Error codes](#).

Examples

- Sample requests

```
https://auditprivate.[RegionId].example.com/?Action=DescribeArchive
&CurrentPage=1
&EndTime=1517630399000
&LogType=1
&PageSize=100
&StartTime=1517414400000
&Type=null
&<Common request parameters>
```

- Sample responses (JSON format)

```
{
  "RequestId":"D33241CB-8E4F-4803-A4D1-59E5B5C8849C",
  "TotalCount":1664162,
  "PageSize":20,
  "CurrentPage":1,
  "ArchiveList":[
    {
      "Type":1,
      "CompactAlg":2,
      "CreateTime":1519818135000,
      "LogType":5,
      "Count":2,
      "Id":3719841,
      "Name":"OPS/2018-02-28/OPS-20180228194215.gz",
      "Md5":"2637db033ab1d3501c1e9eeff8553fbe",
      "Sha256":"06bbc4e58c8e938a9a1acd3edba3cbf6255cbf6e1302bbc8db0ad5c4dfc50a30"
    }
  ]
}
```

12. Error codes

This topic describes the error codes returned for operations in Apsara Stack Security.

Common errors

Error code	Error message	Description
yd.error.all.10001	Authorization required.	The error message returned because you are not authorized to perform the operation. Check the account permissions.
yd.error.all.10002	A system error occurred. Try again later.	The error message returned because a system error occurred. Try again later.
yd.error.all.10003	The parameter is invalid.	The error message returned because the specified parameter is invalid. Check the request parameter and try again.
yd.error.all.other	A system exception occurred.	The error message returned because a system error occurred. Try again later.
yd.error.all.ConsoleSystemError_1001	An unknown error occurred.	The error message returned because an unknown error occurred. Try again later.
yd.error.all.ConsoleSystemError_1007	The specified API operation is unpublished.	The error message returned because the specified API operation is unpublished. Contact Alibaba Cloud technical support.
yd.error.all.ConsoleSystemError_1008	An error occurred while verifying postOnly.	The error message returned because the verification failed. Check the common request parameters and try again.
yd.error.all.ConsoleSystemError_1009	The csrfToken field is not specified.	The error message returned because the csrfToken field is empty. Check the common request parameters and try again.
yd.error.all.ConsoleSystemError_1010	An error occurred while verifying csrfToken.	The error message returned because the verification failed. Check the common request parameters and try again.

Error code	Error message	Description
yd.error.all.ConsoleSystemError_1011	The regionId parameter is not specified.	The error message returned because the RegionId parameter is not specified. Check the parameter.
yd.error.all.ConsoleSystemError_1012	The format of the specified regionId parameter is invalid.	The error message returned because the format of the specified RegionId parameter is invalid. Check the parameter.
yd.error.all.ConsoleSystemError_1013	The parameter is not specified.	The error message returned because the parameter is not specified. Check the parameter and try again.
yd.error.all.ConsoleSystemError_1014	The format of the specified parameter is invalid.	The error message returned because the format of the specified parameter is invalid. Check the parameter and try again.
yd.error.all.ConsoleNeedLogin	You are not logged on.	The error message returned because you are not authorized to perform the operation. Check the account permissions.
yd.error.all.InvalidApi	An operation exception occurred.	The error message returned because an operation exception occurred. Try again later.
yd.error.all.InvalidParameter	The parameter is invalid.	The error message returned because the specified parameter is invalid. Check the request parameter and try again.
yd.error.all.InvalidResult	The return value is invalid.	The error message returned because the return value is invalid. Try again later.
yd.error.all.PropertyConvertFailed	An error occurred during conversion.	The error message returned because property conversion failed. Try again later.
yd.error.all.NoPermission	Authorization required.	The error message returned because you are not authorized to perform the operation. Check the account permissions.
yd.error.all.ServerError	A server error occurred.	The error message returned because a server error occurred. Try again later or contact Alibaba Cloud technical support.

Error code	Error message	Description
yd.error.all.UnkownError	An unknown error occurred.	The error message returned because an unknown error occurred. Try again later or contact Alibaba Cloud technical support.

Error codes specific to Threat Detection Service

Error code	Error message	Description
yd.error.sas.1	The specified field does not exist in the metadata.	The error message returned because the field you queried does not exist in the metadata. Check the request and try again.
yd.error.sas.2	An error occurred while invoking the task engine. Try again.	The error message returned because the system failed to invoke the task engine. Try again later.
yd.error.sas.3	An error occurred while starting the task. Try again.	The error message returned because the system failed to start the task. Try again later.
yd.error.sas.4	An error occurred while stopping the task. Try again.	The error message returned because the system failed to stop the task. Try again later.
yd.error.sas.5	An error occurred while restarting the task. Try again.	The error message returned because the system failed to restart the task. Try again later.
yd.error.sas.6	An error occurred while obtaining the task status. Try again.	The error message returned because the system failed to obtain the task status. Try again later.
yd.error.sas.7	An error occurred while deleting the task. Try again.	The error message returned because the system failed to delete the task. Try again later.
yd.error.sas.8	The specified table does not contain metadata.	The error message returned because the table you queried does not contain metadata. Check the request and try again.
yd.error.sas.100	Request failed. Refresh the page and try again.	The error message returned because the request failed. Try again later.

Error code	Error message	Description
yd.error.sas.101	The parameter is invalid.	The error message returned because the parameter is invalid. Check the parameter and try again.
yd.error.sas.103	Request failed.	The error message returned because the request failed. Check the request and try again later.
yd.error.sas.400	The asset is under protection. Uninstall the Server Guard agent and try again.	The error message returned because the asset that you want to delete is protected by the Server Guard agent. Uninstall the Server Guard agent from the server and try again.
yd.error.sas.500	A system error occurred.	The error message returned because a system error occurred. Contact Alibaba Cloud technical support.
yd.error.sas.501	The feature is not available in the current version.	The error message returned because the version you used does not support this feature.
yd.error.sas.502	You are not authorized to access the server.	The error message returned because you are not authorized to manage the server.

Error codes specific to Anti-DDoS Service

Error code	Error message	Description
yd.error.ddos.400	An error occurred while accessing the server. Try again.	The error message returned because the system failed to access the server. Try again later.
yd.error.ddos.500	An error occurred on the server. Contact technical support.	The error message returned because an error occurred on the server. Contact Alibaba Cloud technical support.
yd.error.ddos.UNKNOWN_EXCEPTION	An unknown error occurred.	The error message returned because an unknown error occurred. Contact Alibaba Cloud technical support.
yd.error.ddos.REQUEST_TIMEOUT	The request timed out.	The error message returned because the request timed out. Try again later.

Error code	Error message	Description
yd.error.ddos.SERVER_FAILED	The operation failed.	The error message returned because the operation failed. Contact Alibaba Cloud technical support.
yd.error.ddos.NOT_AUTHORIZED	Authorization required.	The error message returned because you are not authorized to perform the operation. Check the account permissions.
yd.error.ddos.PARAMETER_INVALID	The parameter is invalid or is not specified.	The error message returned because the specified request parameter is invalid. Check the parameter and try again.
yd.error.ddos.IP_SEGMENT_INVALID	The specified CIDR block is invalid. Check the parameter and enter another value.	The error message returned because the specified CIDR block is invalid. Check the CIDR block specified in the request parameter.
yd.error.ddos.IP_SEGMENT_REPEAT	One CIDR block cannot be used in different regions. Enter another CIDR block.	The error message returned because the specified CIDR block is invalid. Check the CIDR block specified in the request parameter.
yd.error.ddos.IP_SEGMENT_ALREADY	The specified CIDR block already exists.	The error message returned because the specified CIDR block is in use. Check the CIDR block specified in the request parameter.
yd.error.ddos.IP_SEGMENT_MASK_LENGTH_ERR	The mask can contain a maximum of 24 bits.	The error message returned because the mask contains more than 24 bits. Check the mask of the CIDR block specified in the request parameter.
yd.error.ddos.QUERY_REGION_LIST_ERR	An error occurred while obtaining the region list.	The error message returned because the system failed to obtain the region list. Try again later.
yd.error.ddos.IP_SEGMENT_OPERATION_ERR	An error occurred while processing the CIDR block.	The error message returned because the system failed to process the CIDR block. Try again later.
yd.error.ddos.QUERY_IP_SEGMENT_ERR	An error occurred while obtaining the CIDR block.	The error message returned because the system failed to obtain the CIDR block. Try again later.

Error code	Error message	Description
yd.error.ddos.MODIFY_IP_SEGMENT_ERR	An error occurred while modifying the CIDR block.	The error message returned because the system failed to modify the CIDR block. Try again later.
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.
yd.error.ddos.CANCEL_FLOW_CLEAN_ERR	An error occurred while canceling traffic scrubbing. Check whether the network connection to Network Detection and Response is normal.	The error message returned because the system failed to cancel traffic scrubbing. Check the network connection to Network Detection and Response and try again.
yd.error.ddos.QUERY_FLOW_ANALYSIS_ERR	An error occurred while obtaining the traffic analysis result. Check whether the network connection to Network Detection and Response is normal.	The error message returned because the system failed to obtain the traffic analysis result. Check the network connection to Network Detection and Response and try again.
yd.error.ddos.QUERY_BEAVER_URL_ERR	An error occurred while obtaining the URL of Network Detection and Response.	The error message returned because the system failed to obtain the URL of Network Detection and Response. Check the network connection to Network Detection and Response and try again.
yd.error.ddos.SET_VALVE_INVALID	The threshold validation failed. Check the thresholds and enter correct values.	The error message returned because the threshold verification failed. Check the thresholds and try again.
yd.error.ddos.VALVE_DEFAULT_ALREADY	The specified request is invalid. You cannot add the default threshold.	The error message returned because the system failed to add the default threshold. The default threshold can only be modified.
yd.error.ddos.NOT_BELONG_BEAVER_IP_SEGMENT	Check whether the specified CIDR block belongs to the internal network of Network Detection and Response.	The error message returned because the CIDR block you entered does not belong to the internal network of Network Detection and Response. Check the CIDR block.

Error code	Error message	Description
yd.error.ddos.VALVE_DELETE_ERR	The default threshold or the threshold configured for 128.0.XX.XX/XX cannot be deleted.	The error message returned because the system failed to delete the default threshold or the threshold configured for 128.0.XX.XX/XX.
yd.error.ddos.QUERY_CODE_ERR	An error occurred while obtaining the product configuration.	The error message returned because the system failed to obtain the product configuration. Try again later.
yd.error.ddos.IS_OPENED	Enabled.	The error message returned because the specified switch has been turned on.
yd.error.ddos.IS_CLOSED	Disabled.	The error message returned because the specified switch has been turned off.

Error codes specific to Server Guard

Error code	Error message	Description
yd.error.aqs.REQUEST_FAILED	Request failed. Try again later.	The error message returned because the request failed. Try again later.

Error codes specific to Security Auditing

Error codes specific to Sync Center

Error codes specific to Cloud Firewall

Error code	Error message
yd.error.code.200	The request is successful.
yd.error.code.-360100	The request method is invalid.
yd.error.code.-360101	Authentication failed.
yd.error.code.-360102	Invocation failed.
yd.error.code.-360103	The parameter is invalid. Try again.
yd.error.code.-360104	The specified application is invalid. Try again.
yd.error.code.-360105	An error occurred while obtaining the logs.
yd.error.code.-360106	An error occurred while obtaining the logs.

Error code	Error message
yd.error.code.-360107	The specified UID is invalid. Try again.
yd.error.code.-360108	An error occurred while paging.
yd.error.code.-360109	The service is not supported.
yd.error.code.-360110	The format of the specified IP address is invalid. Enter another value.
yd.error.code.-360111	The specified time is invalid. Enter another value.
yd.error.code.-360112	A parsing error occurred.
yd.error.code.-360113	The name of the firewall is invalid. Enter another value.
yd.error.code.-360114	The specified network instance is invalid. Enter another value.
yd.error.code.-360115	The specified VPC is invalid. Enter another value.
yd.error.code.-360116	The specified region is invalid. Enter another value.
yd.error.code.-360117	The specified destination CIDR block is invalid. Enter another value.
yd.error.code.-360118	The specified VPC firewall does not exist. Enter another value.
yd.error.code.-360119	The firewall is configured and cannot be repeatedly created.
yd.error.code.-360120	Authorized required. You must grant permissions to the firewall.
yd.error.code.-360121	The specified security group is invalid.
yd.error.code.-360122	The specified security group is invalid.
yd.error.code.-360123	An error occurred while calling the ECS operation.
yd.error.code.-360124	An error occurred while calling the VPC operation.
yd.error.code.-360125	The format of the specified CIDR block is invalid. Enter another value.
yd.error.code.-360126	An error occurred while creating a vSwitch.
yd.error.code.-360127	An error occurred while creating an endpoint.
yd.error.code.-360128	An error occurred while deleting an endpoint.

Error code	Error message
yd.error.code.-360129	Authorization required. Try again.
yd.error.code.-360130	The specified ECS instance is unavailable.
yd.error.code.-360131	An unknown error occurred.
yd.error.code.-360132	An error occurred while searching the route table.
yd.error.code.-360133	The ID of the firewall is invalid.
yd.error.code.-360134	The status of the firewall is invalid. Try again later.
yd.error.code.-360135	The specified switch of the firewall is invalid. Enter another value.
yd.error.code.-360136	The specified status of the firewall is invalid. Enter another value.
yd.error.code.-360137	Unknown user. Try again.
yd.error.code.-360138	The specified VPC for the firewall is invalid. Enter another value.
yd.error.code.-360139	The specified VPC for the firewall is invalid. Enter another value.
yd.error.code.-360140	The specified firewall does not exist. Enter another value.
yd.error.code.-360141	The firewall is not configured. Configure the firewall.
yd.error.code.-360142	The firewall is enabled.
yd.error.code.-360143	The firewall is disabled.
yd.error.code.-360144	The firewall cannot be enabled because the status of the firewall is invalid. Try again later.
yd.error.code.-360145	The firewall cannot be disabled because the status of the firewall is invalid. Try again later.
yd.error.code.-360146	The NIC of the firewall is invalid. Check the parameter.
yd.error.code.-360147	The destination CIDR block is invalid. Specify another value.
yd.error.code.-360148	The same CIDR block cannot be repeatedly configured. Specify another CIDR block.

Error code	Error message
yd.error.code.-360149	The number of destination CIDR blocks exceeds the upper limit. Reduce the number of CIDR blocks.
yd.error.code.-360150	The ID of the firewall is invalid.
yd.error.code.-360151	The status of the endpoint is invalid.
yd.error.code.-360152	The endpoint is invalid.
yd.error.code.-360153	The endpoint is invalid.
yd.error.code.-360154	A timeout error occurred while creating the endpoint.
yd.error.code.-360155	A timeout error occurred while deleting the endpoint.
yd.error.code.-360156	Permissions required. Try again.
yd.error.code.-360157	The specified route table does not exist.
yd.error.code.-360158	The route entry is invalid.
yd.error.code.-360159	An error occurred while creating the route.
yd.error.code.-360160	An error occurred while deleting the route.
yd.error.code.-360161	A timeout error occurred while creating a route.
yd.error.code.-360162	A timeout error occurred while deleting a route.
yd.error.code.-360163	The route is invalid.
yd.error.code.-360164	The task status is invalid.
yd.error.code.-360165	An error occurred while enabling the firewall. Try again.
yd.error.code.-360166	An error occurred while disabling the firewall. Try again.
yd.error.code.-360167	The parameter is invalid. Try again.
yd.error.code.-360168	The parameter is invalid. Try again.
yd.error.code.-360169	The parameter is invalid. Try again.
yd.error.code.-360170	The parameter is invalid. Try again.
yd.error.code.-360171	The value of the Region parameter is invalid.
yd.error.code.-360172	The system is busy.

Error code	Error message
yd.error.code.-360173	The number of configured VPC firewalls reaches the upper limit. Increase the VPC firewall quota.
yd.error.code.-360174	The number of configured VPC firewalls reaches the upper limit. Increase the VPC firewall quota.
yd.error.code.-360175	The parameter is invalid. Try again.
yd.error.code.-360176	The parameter is invalid. Try again.
yd.error.code.-360177	The parameter is invalid. Try again.
yd.error.code.-360178	An unknown error occurred.
yd.error.code.-360179	An error occurred while calling the operation.
yd.error.code.-360180	The number of VPCs that are attached to the CEN instance is insufficient.
yd.error.code.-360181	The firewall of the CEN instance is overwritten. You do not need to create a firewall.
yd.error.code.-360182	The security group does not exist.
yd.error.code.-360183	The security group cannot be deleted.
yd.error.code.-360184	An unknown error occurred.
yd.error.code.-360185	An error occurred while updating the firewall route.
yd.error.code.-360186	You cannot configure the firewall because the status of the firewall is invalid.
yd.error.code.-360187	The number of VPCs in the region is insufficient. The VPC firewall cannot be enabled.
yd.error.code.-360188	The quota is insufficient. You cannot configure the VPC firewall. Increase the quota.
yd.error.code.-360189	The ECS instance does not exist.
yd.error.code.-360190	An error occurred while calling the operation.
yd.error.code.-360191	The parameter is invalid. Try again.
yd.error.code.-360192	The account is invalid. Enter another value.
yd.error.code.-360193	The account does not have the required permissions, and Cloud Firewall is not purchased.
yd.error.code.-360194	An error occurred while configuring IPS.

Error code	Error message
yd.error.code.-360195	The number of VPCs that are attached to the CEN instance is insufficient. The VPC firewall cannot be enabled.
yd.error.code.-360196	VPC firewalls can be created only in the same region.
yd.error.code.-360197	A conflict occurred.
yd.error.code.-360198	The destination CIDR block is not specified. The firewall cannot be created.
yd.error.code.-360199	A timeout error occurred while attaching Cloud Firewall to the CEN instance.
yd.error.code.-360200	A timeout error occurred while creating the vSwitch.
yd.error.code.-360201	A timeout error occurred while deleting the vSwitch.
yd.error.code.-360202	The specified network instance ID is invalid.
yd.error.code.-360203	The specified VPC does not exist.
yd.error.code.-360204	A timeout error occurred while creating a VPC.
yd.error.code.-360205	A timeout error occurred while creating a VPC.
yd.error.code.-360206	The specified ECS instance does not exist.
yd.error.code.-360207	An error occurred while disabling the ECS instance. Try again.
yd.error.code.-360208	An error occurred while obtaining the backup ECS instance.
yd.error.code.-360209	You are not allowed to create a firewall for a HUB VPC.
yd.error.code.-360210	The specified CEN instance ID is invalid.
yd.error.code.-360211	The parameter is invalid. Try again.
yd.error.code.-360212	The number of VPCs that are attached to the CEN instance is insufficient. The VPC firewall cannot be enabled.
yd.error.code.-360213	The CEN instance does not exist.
yd.error.code.-360214	The request timed out. Try again.
yd.error.code.-360215	The parameter is invalid. Try again.

Error code	Error message
yd.error.code.-360216	The Express Connect circuit for the data center is invalid.
yd.error.code.-360217	The specified firewall mode is invalid.
yd.error.code.-360218	An error occurred while calling the operation of Apsara Stack Network Operations Platform (NET).
yd.error.code.-360300	A backend error occurred.
yd.error.code.-360301	A backend error occurred.
yd.error.code.-360302	A backend error occurred.
yd.error.code.-360303	A backend error occurred.
yd.error.code.-360304	A backend error occurred.
yd.error.code.-360305	A backend error occurred.
yd.error.code.-360306	A backend error occurred.
yd.error.code.-360307	A backend error occurred.
yd.error.code.-360308	An error occurred while querying the cluster ID.
yd.error.code.-360309	An error occurred while updating the information about the cluster.
yd.error.code.-360310	An error occurred while updating the Express Connect circuit.
yd.error.code.-360311	An error occurred while inserting the VLAN.
yd.error.code.-360312	An error occurred while querying the IP address pool.
yd.error.code.-360313	An error occurred while updating the IP address pool.
yd.error.code.-360314	An error occurred while updating the information about the VPC route.
yd.error.code.-360315	An error occurred while updating the status of the VPC.
yd.error.code.-360316	An error occurred while inserting the firewall ns.
yd.error.code.-360317	An error occurred while updating the VLAN.
yd.error.code.-360318	An error occurred while updating the endpoint information about the firewall.

Error code	Error message
yd.error.code.-360319	An error occurred while updating the network information about the firewall.
yd.error.code.-360320	An error occurred while updating the health check configurations.
yd.error.code.-360321	An error occurred while updating the route table.
yd.error.code.-360322	An error occurred while updating the information about the Express Connect circuit for the data center.
yd.error.code.-360323	An error occurred while updating the information about the route of the data center.
yd.error.code.-360400	An unknown error occurred.
yd.error.code.-360401	No VLAN is available.
yd.error.code.-360402	An error occurred while calling the VPC operation.
yd.error.code.-360403	An error occurred while creating the virtual firewall.
yd.error.code.-360404	An error occurred while creating the Express Connect circuit.
yd.error.code.-360405	An error occurred while enabling the Express Connect circuit.
yd.error.code.-360406	An error occurred while creating the VBR.
yd.error.code.-360407	An error occurred while updating the attributes of the VBR.
yd.error.code.-360408	An error occurred while querying the VBR.
yd.error.code.-360409	An error occurred while creating the RI.
yd.error.code.-360410	An error occurred while updating the attributes of the RI.
yd.error.code.-360411	An error occurred while connecting the RI.
yd.error.code.-360412	An error occurred while creating an Express Connect circuit for the data center.
yd.error.code.-360413	An error occurred while enabling an Express Connect circuit for the data center.
yd.error.code.-360414	An error occurred while querying an RI.

Error code	Error message
yd.error.code.-360415	An error occurred while querying the monitored IP addresses that are used for communications between VPCs.
yd.error.code.-360416	An error occurred while querying the monitored IP addresses that are used for communications between a data center and a VPC.
yd.error.code.-360417	The VPC monitoring mode is abnormal.
yd.error.code.-360418	The status of the instance is invalid.
yd.error.code.-193000	An unknown error occurred.
yd.error.code.-193001	The specified HTTP request method is invalid.
yd.error.code.-193002	An error occurred while calling the operation by using HTTP.
yd.error.code.-193003	Permissions required.
yd.error.code.-193004	Unsupported operation.
yd.error.code.-193005	Authentication failed.
yd.error.code.-193006	An error occurred while accessing the database.
yd.error.code.-193007	Accessed native method.
yd.error.code.-193101	An error occurred while encoding JSON data.
yd.error.code.-193102	An error occurred while parsing JSON data.
yd.error.code.-193103	An error occurred while parsing INT data.
yd.error.code.-193104	An error occurred while parsing BOOL data.
yd.error.code.-193105	An error occurred while parsing the body of the HTTP request.
yd.error.code.-193201	The specified parameters are insufficient.
yd.error.code.-193202	The specified parameter value is invalid.
yd.error.code.-193203	The specified time is invalid.
yd.error.code.-193204	The parameter is invalid.
yd.error.code.-193205	The IP address is not in the value of traffic forwarding configuration.
yd.error.code.-193301	The CIDR block already exists.

Error code	Error message
yd.error.code.-193302	The firewall UUID is invalid.
yd.error.code.-193303	The mode of the firewall is being switched.
yd.error.code.-193304	The mode of the firewall is invalid.
yd.error.code.-193305	The switch of the firewall mode is unauthorized.
yd.error.code.-193306	The mode of the device is being switched.
yd.error.code.-193307	An error occurred during the instance health check. The instance cannot be switched to the normal mode.
yd.error.code.-193308	All devices are bypassed, and the instance mode cannot be switched.
yd.error.code.-193309	The working mode of the instance takes precedence over the working mode of the device.
yd.error.code.-193310	The specified page number is invalid.
yd.error.code.-193311	The route type is invalid.
yd.error.code.-193312	An error occurred while deleting the route.
yd.error.code.-193313	An error occurred while deleting the route.
yd.error.code.-193314	An error occurred while creating the route.
yd.error.code.-193315	An error occurred while creating the route.
yd.error.code.-193316	The ID of the Cloud Firewall instance is invalid.
yd.error.code.-193317	The Cloud Firewall instance must be specified.
yd.error.code.-200100	The request method is invalid.
yd.error.code.-200101	Authentication failed.
yd.error.code.-200102	Invocation failed.
yd.error.code.-200103	The parameter is invalid. Try again.
yd.error.code.-200104	The specified UID is invalid. Try again.
yd.error.code.-200105	An error occurred while paging.
yd.error.code.-200106	The IP address in the address book is invalid. Check the parameter and enter another value.
yd.error.code.-200107	The address book already exists.

Error code	Error message
yd.error.code.-200108	An error occurred. Try again.
yd.error.code.-200109	The address book is in use and cannot be deleted.
yd.error.code.-200110	The specified parameter is invalid.
yd.error.code.-200111	The specified parameter is invalid.
yd.error.code.-200112	The specified parameter is invalid.
yd.error.code.-200113	The specified parameter is invalid.
yd.error.code.-200114	The specified parameter is invalid.
yd.error.code.-200115	The specified parameter is invalid.
yd.error.code.-200116	The specified parameter is invalid.
yd.error.code.-200117	The security group rule does not exist.
yd.error.code.-200118	The specified priority is invalid, or the number of rules reaches the upper limit.
yd.error.code.-200119	The specified priority is invalid, or the number of rules reaches the upper limit.
yd.error.code.-200120	An error occurred. Try again.
yd.error.code.-200121	The domain name is invalid. Check the parameter and enter another value.
yd.error.code.-200122	The number of addresses in the address book exceeds the upper limit.
yd.error.code.-200123	The specified parameter is invalid.
yd.error.code.-200124	The specified parameter is invalid.
yd.error.code.-200125	The specified parameter is invalid.
yd.error.code.-200126	The specified parameter is invalid.
yd.error.code.-200127	The number of ports in the address book exceeds the upper limit.
yd.error.code.-200128	The port in the address book is invalid. Check the parameter and enter another value.
yd.error.code.-200129	The number of address books exceeds the upper limit.

Error code	Error message
yd.error.code.-200130	The number of address books exceeds the upper limit.
yd.error.code.-200200	A backend error occurred.
yd.error.code.-200201	A backend error occurred.
yd.error.code.-200202	A backend error occurred.
yd.error.code.-200203	A backend error occurred.
yd.error.code.-200300	A backend error occurred.
yd.error.code.-200301	A backend error occurred.
yd.error.code.-200302	A backend error occurred.
yd.error.code.-200400	An unknown error occurred.
yd.error.code.-200500	An error occurred while calling the operation.
yd.error.code.200	The request is successful.
yd.error.code.-210100	The request method is invalid.
yd.error.code.-210101	Authentication failed.
yd.error.code.-210102	Invocation failed.
yd.error.code.-210103	The parameter is invalid. Try again.
yd.error.code.-210104	The specified UID is invalid. Try again.
yd.error.code.-210105	An error occurred while paging. Try again.
yd.error.code.-210106	The parameter is invalid. Try again.
yd.error.code.-210107	The parameter is invalid. Try again.
yd.error.code.-210108	The parameter is invalid. Try again.
yd.error.code.-210109	The parameter is invalid. Try again.
yd.error.code.-210110	The parameter is invalid. Try again.
yd.error.code.-210111	The parameter is invalid. Try again.
yd.error.code.-210200	A backend error occurred.
yd.error.code.-210201	A backend error occurred.
yd.error.code.-210202	A backend error occurred.

Error code	Error message
yd.error.code.-210203	A backend error occurred.
yd.error.code.-210300	A backend error occurred.
yd.error.code.-210301	A backend error occurred.
yd.error.code.-210302	An error occurred. Try again.
yd.error.code.-210400	An error occurred. Try again.
yd.error.code.200	Success
yd.error.code.-230100	The request method is invalid.
yd.error.code.-230101	Authentication failed.
yd.error.code.-230102	An error occurred while sending the request to the local server.
yd.error.code.-230103	The operation failed authentication.
yd.error.code.-230104	The parameter is invalid.
yd.error.code.-230105	The policy template already exists.
yd.error.code.-230106	The policy template does not exist.
yd.error.code.-230107	The user ID is invalid.
yd.error.code.-230108	The security group ID is invalid.
yd.error.code.-230109	The security group ID is invalid.
yd.error.code.-230110	The direction of the rule is invalid.
yd.error.code.-230111	An IP protocol error occurred.
yd.error.code.-230112	The rule policy is invalid.
yd.error.code.-230113	The priority of the policy is invalid. Enter another value.
yd.error.code.-230114	The port in the policy is invalid. Enter another value.
yd.error.code.-230115	The CIDR block is invalid. Enter another value.
yd.error.code.-230116	The description is invalid. Enter another value.
yd.error.code.-230117	The policy already exists.
yd.error.code.-230118	The policy does not exist.

Error code	Error message
yd.error.code.-230119	The rule ID is invalid.
yd.error.code.-230120	The number of policies exceeds the limit. We recommend that you delete policies that you no longer use.
yd.error.code.-230121	An error occurred while paging.
yd.error.code.-230122	The rule is being published. Try again.
yd.error.code.-230123	The submission status is invalid.
yd.error.code.-230124	The policy group is rolled back.
yd.error.code.-230125	The submitted information is invalid.
yd.error.code.-230126	The rule is not changed. You do not need to publish the rule.
yd.error.code.-230127	The security group ID is invalid.
yd.error.code.-230128	The IP address in the rule is invalid.
yd.error.code.-230129	The network type of the rule is invalid. Select another value.
yd.error.code.-230130	An error occurred while managing the rule.
yd.error.code.-230131	The policy cannot be submitted.
yd.error.code.-230150	The policy group does not exist. Specify another value.
yd.error.code.-230151	The number of policy groups exceeds the limit.
yd.error.code.-230152	The policy group cannot be modified.
yd.error.code.-230153	The policy group is prestarted.
yd.error.code.-230154	The rule ID is invalid.
yd.error.code.-230200	A backend error occurred.
yd.error.code.-230300	A backend error occurred.
yd.error.code.-230301	A backend error occurred.
yd.error.code.-230302	A backend error occurred.
yd.error.code.-230400	An unknown error occurred.

Error codes specific to Network Detection and Response

Error code	Error message	Description
ErrorNeedLogin.-210204	need login (You are not logged on.)	The error message returned because you are not logged on. Log on first.
ErrorAuthentication.-210101	authentication error (An authentication error occurred.)	The error message returned because an authentication error occurred. Use a RAM role that has the required permissions.
ErrorParametersAliUid.-210902	invalid AliUid (The value of the AliUid parameter is invalid.)	The error message returned because the value of the AliUid parameter is invalid. Specify a valid value.
ErrorParametersIpType.-210920	invalid para ip type (The value of the ipType parameter is invalid.)	The error message returned because the value of the ipType parameter is invalid. Specify a valid value.
ErrorParametersSrcIP.-210919	invalid para src ip (The value of the SrcIP parameter is invalid.)	The error message returned because the value of the SrcIP parameter is invalid. Specify a valid value.
ErrorParametersDstIP.-210921	invalid para dst ip (The value of the dstIP parameter is invalid.)	The error message returned because the value of the dstIP parameter is invalid. Specify a valid value.
ErrorParametersPort.-210208	invalid port, must 0~65535 (The specified port number is invalid. The port number must range from 0 to 65535.)	The error message returned because the specified port number is invalid. Specify a port number ranging from 0 to 65535.
ErrorParametersLiveTime.-210922	invalid para live time (The value of the liveTime parameter is invalid.)	The error message returned because the value of the liveTime parameter is invalid. Specify a valid value.
ErrorDBInsert.-210122	internal error: sql insert (An internal error occurred while executing the INSERT statement.)	The error message returned because an internal error occurred while executing the INSERT statement.
ErrorInnerUuid.-210606	internal error: uuid list is 0 (The internal error of empty UUID list occurred.)	The error message returned because the UUID list is empty.
ErrorDBSelect.-210124	internal error: sql select (An internal error occurred while executing the SELECT statement.)	The error message returned because an internal error occurred while executing the SELECT statement.

Error code	Error message	Description
ErrorParasAddressCidrFeild.-210915	paras addressCidrList filed (Failed to reset the addressCidrList rule.)	The error message returned because the system failed to reset the addressCidrList rule.
ErrorPortAddressGroup.-210303	get port in address group failed (Failed to obtain port information from the address group.)	The error message returned because the system failed to obtain port information from the address group.
ErrorPortAddressGroup.-210303	get port in address group failed (Failed to obtain port information from the address group.)	The error message returned because the system failed to obtain port information from the address group.
ErrorSourceAddressGroup.-210304	get source address in address group failed (Failed to obtain source addresses from the address group.)	The error message returned because the system failed to obtain source addresses from the address group.
ErrorSourceAddressRange.-210306	source address range error, must be like \"192.168.XX.XX/192.168.XX.XX\" (The source address range is invalid. Example: \"192.168.XX.XX/192.168.XX.XX\")	The error message returned because the source address range is invalid. Specify the value in the \"192.168.XX.XX/192.168.XX.XX\" format.
ErrorDestAddressGroup.-210305	get dest address in address group failed (Failed to obtain destination addresses from the address group.)	The error message returned because the system failed to obtain destination addresses from the address group.
ErrorNoBeaverRules.-210226	no beaver rules for online (The specified Network Detection and Response rule does not exist.)	The error message returned because the specified Network Detection and Response rule does not exist.
ErrorDBUpdate.-210121	internal error: sql update (An internal error occurred while executing the UPDATE statement.)	The error message returned because an internal error occurred while executing the UPDATE statement.
ErrorDBDelete.-210123	internal error: sql delete (An internal error occurred while executing the DELETE statement.)	The error message returned because an internal error occurred while executing the DELETE statement.
ErrorMarshalJSON.-210125	internal error: marshal json (An internal error occurred while marshaling JSON data.)	The error message returned because an internal error occurred while marshaling JSON data.