ALIBABA CLOUD

Alibaba Cloud

Apsara Stack Enterprise

Operations and Maintenance Guide

Product Version: 2012, Internal: V3.13.0

Document Version: 20210621

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.Overview ---- 50
2.Get started ---- 52
2.1. Prepare an operations account ---- 52
2.2. Log on to the Apsara Uni-manager Operations Console ---- 52
2.3. Apsara Uni-manager Operations Console homepage ---- 53
2.4. Instructions for the homepage ---- 55
3.Settings ---- 57
3.1. Default operations roles ---- 57
3.2. Security policies ---- 57
3.2.1. Logon policies ---- 57
3.2.2. Physical server passwords ---- 58
3.3. Offline backup ---- 60
3.3.1. Add a backup product ---- 60
3.3.2. Configure backup ---- 61
3.3.3. View the backup details ---- 62
3.3.4. Configure a backup server ---- 62
3.3.5. View the backup server status ---- 63
3.3.6. View the backup status ---- 64
3.3.7. Use cases ---- 65
3.3.7.1. Offline backup of metadata ---- 65
3.3.7.1.1. Preparations ---- 65
3.3.7.1.2. Collect the Apsara Distributed File System inform... ---- 66
3.3.7.1.3. Configure a backup server ---- 67
3.3.7.1.4. Add a backup product ---- 68
3.3.7.1.5. Configure backup parameters ---- 69
3.3.7.1.6. View the backup details ---- 70

3.4. Log clearance 70
3.4.1. Import container or server log cleanup rules 70
3.4.2. Export container or physical server log cleanup rules 71
3.4.3. Modify a log cleanup rule 72
3.4.4. Delete a log cleanup rule 72
3.4.5. Obtain the usage information of containers or physical... 73
3.4.6. Clean up the logs of containers or physical servers 74
3.4.7. Configure automatic cleanups for container or physical... 75
3.4.8. View cleanup records 76
3.5. System settings 77
3.5.1. User management 77
3.5.2. User group management 79
3.5.3. Role management 81
3.5.4. Menu management 82
3.5.4.1. Add a level-1 menu 82
3.5.4.2. Add a submenu 84
3.5.4.3. Hide a menu 86
3.5.4.4. Modify a menu 87
3.5.4.5. Delete a menu 87
3.5.5. Two-factor authentication 87
3.5.6. Department management 88
3.5.7. Region management 89
3.5.8. Operating system logs 90
3.5.9. Operation logs 91
3.5.10. View authorization information 91
3.5.11. Multi-cloud management 94
3.5.11.1. Add multi-cloud configurations 94
3.5.11.2. Modify the name of a data center 95

3.6. Personal Settings 95
3.6.1. Change the logon password 95
3.6.2. Modify logon settings 96
4.Resources 98
4.1. Products 98
4.1.1. Product overview 98
4.1.2. Clusters 99
4.1.3. Service roles 100
4.2. Network 101
4.2.1. Cloud service interconnection 102
4.2.1.1. Dynamic VIP 102
4.2.1.2. Dynamic DNS 104
4.2.1.3. Cross-cloud access 106
4.2.2. Hybrid cloud resources 108
4.2.2.1. Physical topology 109
4.2.2.2. Network element management 112
4.2.2.3. IP address pools 116
4.2.3. Network service provider 118
4.2.3.1. View access gateway instances 118
4.2.3.2. View operation logs 119
4.2.3.3. View network information of bare metal instances i... 120
4.2.3.4. O&M configurations 121
4.2.3.4.1. Apply for a bare metal instance in the VPC 121
4.2.3.4.2. Release a bare metal instance in the VPC 123
4.2.3.4.3. Delete a VPC route table entry 124
4.2.3.4.4. Delete a VBR route table entry 125
4.2.3.4.5. Delete a VPC router interface 127
4.2.3.4.6. Delete a VBR router interface 128

4.2.3.4.7. Delete a VBR 129
4.2.3.4.8. Delete a physical connection 130
4.2.3.4.9. Delete all resources 132
4.2.3.4.10. View the physical connection bandwidth 134
4.2.3.4.11. Modify the physical connection bandwidth 135
4.2.3.4.12. View BD usage 136
4.2.3.4.13. View BM VPN usage 137
4.2.3.4.14. View trunk usage 137
4.3. Data centers 138
4.3.1. View the physical server information 138
4.3.2. Add a physical server 141
4.3.3. Modify a physical server 142
4.3.4. Export server information 143
4.3.5. Delete a physical server 144
4.4. Full stack 144
4.4.1. SLA 145
4.4.1.1. View the current status of a cloud service 145
4.4.1.2. View the history data of a cloud service 145
4.4.1.3. View the availability of an instance 146
4.4.1.4. View the availability of a service 147
4.4.2. Full stack log monitoring 147
5.Alerts 149
5.1. Dashboard 149
5.2. View alerts 150
5.3. Alert settings 153
5.3.1. Policy management 153
5.3.1.1. Alert contacts 154
5.3.1.2. Alert contact groups 154

5.3.1.3. Configure static parameters ---------- 155
5.3.2. Alert templates ---------- 156
5.3.3. Notification management ---------- 157
5.3.4. Alert masking ---------- 159
5.3.4.1. Add masking rules ---------- 159
5.3.4.2. Disable masking ---------- 161
6.O&M ---------- 162
6.1. Automated O&M ---------- 162
6.1.1. View host resources ---------- 162
6.1.2. View Docker resources ---------- 162
6.1.3. Manage scripts ---------- 163
6.1.3.1. Create a script ---------- 163
6.1.3.2. Import a script ---------- 164
6.1.3.3. View scripts ---------- 165
6.1.3.4. Modify a script ---------- 165
6.1.3.5. Export a script ---------- 166
6.1.3.6. Delete a script ---------- 166
6.1.4. Manage software ---------- 166
6.1.4.1. Upload software ---------- 166
6.1.4.2. View software ---------- 167
6.1.4.3. Download software ---------- 167
6.1.4.4. Delete software ---------- 168
6.1.5. Manage processes ---------- 168
6.1.5.1. Create a process ---------- 168
6.1.5.2. Import a process ---------- 174
6.1.5.3. View processes ---------- 174
6.1.5.4. Export a process ---------- 175
6.1.5.5. Modify a process ---------- 175

6.1.5.6. Run a process 175
6.1.5.7. Delete a process 176
6.1.6. Manage O&M jobs 176
6.1.6.1. Create an O&M job 176
6.1.6.2. Import an O&M job 181
6.1.6.3. View O&M jobs 181
6.1.6.4. Export an O&M job 182
6.1.6.5. Modify an O&M job 182
6.1.6.6. Execute an O&M job 182
6.1.6.7. Delete an O&M job 183
6.1.7. Review jobs 183
6.1.8. Review processes 183
6.1.9. View O&M logs 184
6.2. Network Operation Center 184
6.2.1. Dashboard 184
6.2.1.1. View the dashboard 184
6.2.1.2. View the network topology 185
6.2.1.3. Manage custom views 186
6.2.2. Network element management 190
6.2.2.1. Device management 190
6.2.2.1.1. View the network monitoring information 190
6.2.2.1.2. View logs 191
6.2.2.1.3. Collection settings 192
6.2.2.1.3.1. Configure the collection interval 192
6.2.2.1.3.2. Modify the collection interval 193
6.2.2.1.3.3. Add an OOB network segment 193
6.2.2.1.3.4. View the OOB network segment information 194
6.2.2.2. Modify the device password 195

6.2.2.3. Compare device configurations 195
6.2.3. SLB management 196
6.2.3.1. View cluster monitoring information 196
6.2.3.2. View the instance monitoring information 198
6.2.4. Collect IP addresses 199
6.2.5. IP address range management 199
6.2.5.1. Import the planning file 199
6.2.5.2. Manually add the IP address pool information 200
6.2.5.3. Modify the IP address pool information 201
6.2.5.4. Export the IP address pool information 202
6.2.5.5. Delete an IP address pool 202
6.2.6. View Anytunnel information 202
6.2.7. XGW management 203
6.2.7.1. View node information 203
6.2.7.2. View the instance monitoring information 204
6.2.8. Firewall management 205
6.2.9. Alerts 206
6.2.9.1. View and process current alerts 206
6.2.9.2. View historical alerts 207
6.2.10. Alert settings 207
6.2.10.1. Add a trap 207
6.2.10.2. View traps 210
6.2.11. Physical network integration 210
6.2.12. ASW scale-up 212
6.2.13. Push IPv6 configurations 213
6.2.14. Check IP address conflicts 215
6.2.15. Leased line discovery 215
6.2.16. Baseline configuration audit 217

6.2.17. Inspection dashboard 218
6.2.18. Inspection history 219
6.2.19. Inspection management 219
6.2.19.1. Create a one-time task 219
6.2.19.2. Create a scheduled task 221
6.2.19.3. Manage scheduled inspection tasks 221
6.2.20. Inspection templates 222
6.2.20.1. Create a template 222
6.2.20.2. View template details 223
6.2.20.3. Modify a template 223
6.2.20.4. Delete a template 224
6.2.20.5. View inspection items 224
6.2.21. Use cases 225
6.2.21.1. Troubleshoot network failures 225
6.3. Products 228
6.3.1. Product list 228
6.3.2. ISV access settings 229
6.3.2.1. Configure the ISV access information 229
6.3.2.2. Modify the ISV access information 230
6.3.2.3. Delete the ISV access information 231
6.4. Apsara Distributed File System Management 231
6.4.1. View ECS disk size rankings 231
6.4.2. Dashboard 232
6.4.3. Clusters 233
6.4.4. Nodes 235
6.4.5. Operations and maintenance 236
6.4.6. Modify cluster thresholds 237
6.4.7. Load information 239

6.4.7.1. View NC information 239
6.4.7.2. View virtual machine information 245
6.4.7.3. View block device information 246
6.4.8. EBS dashboard 247
6.4.9. Block master operations 248
6.4.10. Block server operations 249
6.4.11. SnapShotServer 251
6.4.12. Block gcworker operations 253
6.4.13. Device operations 255
6.4.14. Enable or disable Rebalance 260
6.4.15. IO hang fault analysis 260
6.4.16. Slow IO analysis 261
6.4.17. Product settings 263
6.5. Task Management 263
6.5.1. Overview 263
6.5.2. View task overview 264
6.5.3. Create a task 265
6.5.4. View the execution status of a task 267
6.5.5. Start a task 268
6.5.6. Delete a task 269
6.5.7. Process tasks to be intervened 269
6.6. Apsara Infrastructure Management Framework O&M 270
6.6.1. Old console 270
6.6.1.1. What is Apsara Infrastructure Management Framewo... 270
6.6.1.1.1. Overview 270
6.6.1.1.2. Basic concepts 270
6.6.1.2. Log on to the Apsara Infrastructure Management Fr... 272
6.6.1.3. Web page introduction 273

6.6.1.3.1. Instructions for the homepage 273
6.6.1.3.2. Instructions for the left-side navigation pane 275
6.6.1.4. Cluster operations 278
6.6.1.4.1. View configuration information of a cluster 278
6.6.1.4.2. View dashboard information of a cluster 280
6.6.1.4.3. View information of the cluster O&M center 283
6.6.1.4.4. View the desired state of a service 286
6.6.1.4.5. View operations logs 287
6.6.1.5. Service operations 288
6.6.1.5.1. View the service list 288
6.6.1.5.2. View dashboard information of a service instanc... 289
6.6.1.5.3. View the server role dashboard 291
6.6.1.6. Machine operations 294
6.6.1.6.1. View the machine dashboard 294
6.6.1.7. Monitoring center 296
6.6.1.7.1. Modify an alert rule 296
6.6.1.7.2. View the status of a monitoring instance 297
6.6.1.7.3. View the alert status 297
6.6.1.7.4. View alert rules 298
6.6.1.7.5. View the alert history 298
6.6.1.8. Tasks and deployment summary 299
6.6.1.8.1. View rolling tasks 299
6.6.1.8.2. View running tasks 301
6.6.1.8.3. View historical tasks 301
6.6.1.8.4. View the deployment summary 302
6.6.1.9. Reports 304
6.6.1.9.1. View reports 304
6.6.1.9.2. Add a report to favorites 305

6.6.1.10. Appendix ---------- 305
6.6.1.10.1. Project component info report ---------- 305
6.6.1.10.2. IP list ---------- 306
6.6.1.10.3. Machine info report ---------- 307
6.6.1.10.4. Rolling info report ---------- 308
6.6.1.10.5. Machine RMA approval pending list ---------- 310
6.6.1.10.6. Registration vars of services ---------- 311
6.6.1.10.7. Virtual machine mappings ---------- 312
6.6.1.10.8. Service inspector report ---------- 312
6.6.1.10.9. Resource application report ---------- 312
6.6.1.10.10. Statuses of project components ---------- 314
6.6.1.10.11. Relationship of service dependency ---------- 316
6.6.1.10.12. Check report of network topology ---------- 316
6.6.1.10.13. Clone report of machines ---------- 317
6.6.1.10.14. Auto healing/install approval pending report ---------- 318
6.6.1.10.15. Machine power on or off statuses of clusters ---------- 318
6.6.2. New console ---------- 320
6.6.2.1. Introduction to Apsara Infrastructure Management F...---------- 320
6.6.2.1.1. What is Apsara Infrastructure Management Fram...---------- 320
6.6.2.1.2. Features ---------- 320
6.6.2.1.3. Terms ---------- 320
6.6.2.2. Log on to the Apsara Infrastructure Management F...---------- 322
6.6.2.3. Instructions for the homepage ---------- 323
6.6.2.4. Operations ---------- 326
6.6.2.4.1. Project operations ---------- 326
6.6.2.4.2. Cluster operations ---------- 326
6.6.2.4.2.1. View the cluster list ---------- 326
6.6.2.4.2.2. View details of a cluster ---------- 328

6.6.2.4.2.3. View configuration information of a cluster 331
6.6.2.4.2.4. View operations logs 333
6.6.2.4.3. Service operations 334
6.6.2.4.3.1. View the service list 334
6.6.2.4.3.2. View details of a server role 335
6.6.2.4.3.3. Block hardware alerts 336
6.6.2.4.4. Machine operations 338
6.6.2.5. View tasks 339
6.6.2.6. Reports 340
6.6.2.6.1. View reports 340
6.6.2.6.2. Add a report to favorites 341
6.6.2.7. Monitoring center 342
6.6.2.7.1. View the status of a metric 342
6.6.2.7.2. View the alert status 342
6.6.2.7.3. View alert rules 343
6.6.2.7.4. View the alert history 344
6.6.2.8. Tools 345
6.6.2.8.1. Use machine operations tools 346
6.6.2.8.2. Shut down a data center 347
6.6.2.8.3. View the clone progress 350
6.6.2.9. Appendix 350
6.6.2.9.1. Project component info report 350
6.6.2.9.2. IP list 351
6.6.2.9.3. Machine info report 351
6.6.2.9.4. Rolling info report 353
6.6.2.9.5. Machine RMA approval pending list 355
6.6.2.9.6. Registration vars of services 356
6.6.2.9.7. Virtual machine mappings 357

6.6.2.9.8. Service inspector report ---------- 357
6.6.2.9.9. Resource application report ---------- 357
6.6.2.9.10. Statuses of project components ---------- 359
6.6.2.9.11. Relationship of service dependency ---------- 361
6.6.2.9.12. Check report of network topology ---------- 361
6.6.2.9.13. Clone report of machines ---------- 362
6.6.2.9.14. Auto healing/install approval pending report ---------- 363
6.6.2.9.15. Machine power on or off statuses of clusters ---------- 363
7.Analysis ---------- 365
7.1. Inventory analysis ---------- 365
7.2. View the ECS inventory ---------- 365
7.3. View the SLB inventory ---------- 366
7.4. View the RDS inventory ---------- 367
7.5. View the OSS inventory ---------- 367
7.6. View the Tablestore inventory ---------- 368
7.7. View the Log Service inventory ---------- 369
7.8. View the EBS inventory ---------- 370
7.9. View the NAS inventory ---------- 371
7.10. View the DFS inventory ---------- 371
8.Network operations ---------- 373
8.1. Apsara Network Intelligence ---------- 373
8.1.1. What is Apsara Network Intelligence? ---------- 373
8.1.2. Log on to the Apsara Network Intelligence console ---------- 373
8.1.3. Query information ---------- 374
8.1.4. Manage cloud service instances ---------- 375
8.1.5. Tunnel VIP ---------- 375
8.1.5.1. Create a Layer-4 listener VIP ---------- 375
8.1.5.2. Query the tunnel VIP of a cloud service ---------- 377

8.1.6. Create a Direct Any Tunnel VIP ---------- 378
8.1.7. Leased line connection ---------- 378
8.1.7.1. Overview ---------- 378
8.1.7.2. Manage access points ---------- 379
8.1.7.3. Manage access devices ---------- 380
8.1.7.4. Establish a leased line connection ---------- 381
8.1.7.5. Create a VBR ---------- 383
8.1.7.6. Create router interfaces ---------- 385
8.1.7.7. Create a routing table ---------- 386
8.1.8. Manage Business Foundation System flows in a VPC ---------- 388
8.1.9. Configure reverse access to cloud services ---------- 388
8.2. Network Management and Operations ---------- 389
8.2.1. Overview ---------- 389
8.2.2. Log on to the Network Management and Operations o...---------- 389
8.2.3. Network Automation ---------- 390
8.2.3.1. Manage devices ---------- 390
8.2.3.2. Configure templates ---------- 391
8.2.3.2.1. Overview ---------- 391
8.2.3.2.2. Create a device template ---------- 392
8.2.3.2.3. Create a user template ---------- 395
8.2.3.3. Manage change tasks ---------- 398
8.2.3.4. Trigger real-time tasks ---------- 398
8.2.3.5. Manage files ---------- 399
8.2.4. Network monitoring ---------- 399
8.2.4.1. Dashboards ---------- 399
8.2.4.1.1. Check the status of a device ---------- 399
8.2.4.1.2. Check the aggregate status ---------- 399
8.2.4.1.3. Check the data view ---------- 400

8.2.4.2. Configuration management 400
8.2.4.2.1. Add a monitoring item 400
8.2.4.2.2. Add a notification group 401
8.2.4.2.3. Subscription management 401
8.2.4.2.3.1. Subscribe to single-device notifications 401
8.2.4.2.3.2. Subscribe to aggregate notifications 402
8.2.4.2.4. Add an aggregate data configuration 404
8.2.4.2.5. Add a port set 404
8.2.4.2.6. Add a data view 405
8.2.5. Security Reinforcement 406
8.2.5.1. Log on to the srs-master.Server container 406
8.2.5.2. Enable SRS 407
8.2.5.3. Disable SRS 407
8.2.5.4. Manage IP address whitelists 408
8.2.5.5. Manage SRS disabled services 409
8.2.6. Sample templates 411
9.Operations of basic cloud products 417
9.1. Elastic Compute Service (ECS) 417
9.1.1. ECS overview 417
9.1.2. Log on to the Apsara Uni-manager Operations Console 417
9.1.3. ECS operations and maintenance 418
9.1.3.1. Overview 418
9.1.3.2. VM 419
9.1.3.2.1. Overview 419
9.1.3.2.2. Query VMs 419
9.1.3.2.3. Start a VM 419
9.1.3.2.4. Stop a VM 420
9.1.3.2.5. Restart a VM 420

9.1.3.2.6. Cold migration 421
9.1.3.2.7. Hot migration 422
9.1.3.2.8. Reset a disk 423
9.1.3.3. Disks 423
9.1.3.3.1. Overview 423
9.1.3.3.2. Query disks 423
9.1.3.3.3. View snapshots 424
9.1.3.3.4. Attach a disk 424
9.1.3.3.5. Detach a disk 424
9.1.3.3.6. Create a snapshot 425
9.1.3.4. Snapshots 425
9.1.3.4.1. Overview 425
9.1.3.4.2. Query snapshots 425
9.1.3.4.3. Delete a snapshot 426
9.1.3.4.4. Create an image 426
9.1.3.5. Images 427
9.1.3.5.1. Overview 427
9.1.3.5.2. Query images 427
9.1.3.6. Security groups 427
9.1.3.6.1. Overview 427
9.1.3.6.2. Query security groups 428
9.1.3.6.3. Add security group rules 428
9.1.3.7. Custom instance types 429
9.1.3.7.1. Add custom instance types 429
9.1.3.7.2. Query custom instance types 430
9.1.3.7.3. Modify custom instance types 430
9.1.3.7.4. Delete custom instance types 431
9.1.4. Apsara Distributed File System Management 431

9.1.4.1. View ECS disk size rankings 431
9.1.4.2. EBS dashboard 432
9.1.4.3. Block master operations 432
9.1.4.4. Block server operations 434
9.1.4.5. SnapShotServer 436
9.1.4.6. Block gcworker operations 438
9.1.4.7. Device operations 440
9.1.4.8. Enable or disable Rebalance 444
9.1.4.9. IO hang fault analysis 445
9.1.4.10. Slow IO analysis 446
9.1.4.11. Product settings 447
9.1.5. VM hot migration 448
9.1.5.1. Overview 448
9.1.5.2. Limits on hot migration 448
9.1.5.3. Complete hot migration on AG 449
9.1.5.4. Modify the position of the NC where the VM is loc... 450
9.1.5.5. FAQ 451
9.1.6. Hot migration of disks 452
9.1.6.1. Overview 452
9.1.6.2. Limits 452
9.1.6.3. O&M after hot migration 453
9.1.7. Upgrade solution 453
9.1.7.1. Overview 453
9.1.7.2. Limits on GPU clusters 454
9.1.7.3. Limits on FPGA clusters 454
9.1.8. Handle routine alarms 454
9.1.8.1. Overview 454
9.1.8.2. API proxy 455

9.1.8.3. API Server 456
9.1.8.4. RegionMaster 456
9.1.8.5. RMS 457
9.1.8.6. PYNC 458
9.1.8.7. Zookeeper 458
9.1.8.8. AG 459
9.1.8.9. Server groups 459
9.1.9. Inspection 460
9.1.9.1. Overview 460
9.1.9.2. Cluster basic health inspection 460
9.1.9.2.1. Overview 460
9.1.9.2.2. Monitoring inspection 460
9.1.9.2.3. Inspection of basic software package versions 460
9.1.9.2.4. Basic public resources inspection 460
9.1.9.3. Cluster resource inspection 461
9.1.9.3.1. Overview 461
9.1.9.3.2. Cluster inventory inspection 461
9.1.9.3.3. VM inspection 462
9.2. Container Service for Kubernetes 463
9.2.1. Components and features 463
9.2.1.1. Console 463
9.2.1.2. Troopers 464
9.2.1.3. Mirana 465
9.2.2. System restart 466
9.2.2.1. Restart a control node 466
9.3. Auto Scaling (ESS) 466
9.3.1. Log on to the Apsara Uni-manager Operations Console 467
9.3.2. Product resources and services 468

9.3.2.1. Application deployment 468
9.3.2.2. Troubleshooting 468
9.3.3. Inspection 469
9.3.3.1. Overview 469
9.3.3.2. Monitoring inspection 469
9.3.3.3. Basic software package version inspection 469
9.4. Resource Orchestration Service (ROS) 469
9.4.1. ROS component O&M 470
9.4.1.1. API Server 470
9.4.1.2. Engine Server 470
9.4.1.3. RabbitMQ clusters 470
9.4.1.4. Notify Server 471
9.4.2. Failed to create a scaling group stack 472
9.4.3. Failed to create an ECS resource stack 473
9.5. Object Storage Service (OSS) 477
9.5.1. Log on to the Apsara Uni-manager Operations Console 477
9.5.2. OSS operations and maintenance 478
9.5.2.1. User data 478
9.5.2.1.1. Basic bucket information 478
9.5.2.1.2. User data overview 478
9.5.2.1.3. Data monitoring 479
9.5.2.2. Cluster data 480
9.5.2.2.1. Inventory monitoring 480
9.5.2.2.2. Bucket statistics 480
9.5.2.2.3. Object statistics 481
9.5.2.2.4. Data monitoring 482
9.5.2.2.5. Resource usage rankings 484
9.5.3. Tools and commands 485

9.5.3.1. Typical commands supported by tsar 485
9.5.3.2. Configure tsar for statistic collection 485
9.6. Tablestore 485
9.6.1. Tablestore Operations and Maintenance System 486
9.6.1.1. Overview 486
9.6.1.2. User data 486
9.6.1.2.1. Instance management 486
9.6.1.3. Cluster management 488
9.6.1.3.1. Cluster information 488
9.6.1.4. Inspection center 491
9.6.1.4.1. Abnormal resource usage 491
9.6.1.5. Monitoring center 492
9.6.1.5.1. Cluster monitoring 492
9.6.1.5.2. Application monitoring 492
9.6.1.5.3. Top requests 493
9.6.1.5.4. Request log search 494
9.6.1.6. System management 494
9.6.1.6.1. Task management 494
9.6.1.6.2. View tasks 495
9.6.1.7. Platform audit 496
9.6.1.7.1. Operation logs 496
9.6.2. Cluster environments 497
9.6.3. System roles 497
9.6.4. Pre-partition a table 498
9.6.4.1. Pre-partitioning 498
9.6.4.2. View partitions 499
9.7. ApsaraDB RDS 499
9.7.1. Architecture 499

9.7.1.1. System architecture 499
9.7.1.1.1. Backup system 499
9.7.1.1.2. Data migration system 500
9.7.1.1.3. Monitoring system 500
9.7.1.1.4. Control system 501
9.7.1.1.5. Task scheduling system 501
9.7.2. Log on to the Apsara Uni-manager Operations Console 501
9.7.3. Manage instances 502
9.7.4. Manage hosts 504
9.7.5. Security maintenance 505
9.7.5.1. Network security maintenance 505
9.7.5.2. Account password maintenance 505
9.7.6. Redline V4.3.3 O&M description 505
9.7.6.1. Services provided by Redline Enterprise 505
9.7.6.2. Paths of files in the Docker container of redline-per... 506
9.7.6.3. Perform environment checks 507
9.7.6.4. O&M operations 509
9.7.6.4.1. Scale in or out a cluster 509
9.7.6.4.2. Upgrade or restart a cluster 509
9.7.6.4.3. Fix connection failures 510
9.7.6.4.4. Activate clusters in the deactived state 510
9.7.6.4.5. Troubleshoot program exceptions 510
9.7.6.4.6. Reset node data 512
9.8. AnalyticDB for PostgreSQL 513
9.8.1. Overview 513
9.8.2. Architecture 513
9.8.3. Routine maintenance 514
9.8.3.1. Check for data skew on a regular basis 514

9.8.3.2. Execute VACUUM and ANALYZE statements 515
9.8.4. Security maintenance 515
9.8.4.1. Network security maintenance 515
9.8.4.2. Account password maintenance 515
9.9. KVStore for Redis 516
9.9.1. O&M tool 516
9.9.2. Architecture diagram 516
9.9.3. Log on to the Apsara Uni-manager Operations Console 516
9.9.4. Manage ApsaraDB for Redis instances 517
9.9.5. Manage hosts 518
9.9.6. Security maintenance 519
9.9.6.1. Network security maintenance 519
9.9.6.2. Password maintenance 519
9.10. ApsaraDB for MongoDB 519
9.10.1. Service architecture 519
9.10.1.1. System architecture 519
9.10.1.1.1. Backup system 519
9.10.1.1.2. Data migration system 520
9.10.1.1.3. Monitoring system 520
9.10.1.1.4. Control system 521
9.10.1.1.5. Task scheduling system 521
9.10.2. ApsaraDB for MongoDB O&M overview 521
9.10.3. Log on to the Apsara Uni-manager Operations Consol... 521
9.10.4. Security maintenance 522
9.10.4.1. Network security maintenance 522
9.10.4.2. Account password maintenance 523
9.11. ApsaraDB for OceanBase 523
9.11.1. Overview 523

9.11.2. Architecture ---------- 524
9.11.2.1. Architecture ---------- 524
9.11.2.2. Deployment solutions ---------- 525
9.11.2.2.1. Create a cluster ---------- 525
9.11.2.2.2. Install OBProxy ---------- 528
9.11.2.3. OCP V2.0 components and their features ---------- 530
9.11.2.3.1. Components and their features ---------- 530
9.11.2.3.2. OcpMetaServer ---------- 532
9.11.2.3.3. OcpMetaInit ---------- 533
9.11.2.3.4. OcpObproxy ---------- 533
9.11.2.3.5. OcpApiV2 ---------- 533
9.11.2.3.6. OcpTengine ---------- 534
9.11.3. Routine maintenance ---------- 534
9.11.3.1. Log on to the ApsaraDB for OceanBase O&M conso...---------- 534
9.11.3.2. View performance metrics ---------- 535
9.11.3.2.1. Description of performance metrics ---------- 535
9.11.3.3. View alert events ---------- 542
9.11.3.4. Upgrade the version of a cluster ---------- 544
9.11.4. Security maintenance ---------- 545
9.11.4.1. Network security maintenance ---------- 545
9.11.4.2. Account password maintenance ---------- 545
9.11.4.3. Establish a fault response mechanism ---------- 545
9.11.5. Backup and recovery ---------- 545
9.11.5.1. Overview ---------- 546
9.11.5.2. Go to the Backup and Recovery page ---------- 546
9.11.5.3. Preparations ---------- 546
9.11.5.4. Manage backup and recovery configuration files ---------- 547
9.11.5.4.1. Add a backup configuration file ---------- 548

9.11.5.4.2. Add a recovery configuration file 549
9.11.5.4.3. Manage a configuration file 551
9.11.5.5. Install backup and recovery agents 551
9.11.5.5.1. Install backup and recovery agents 552
9.11.5.5.2. Manage backup and recovery agents 552
9.11.5.6. Run backup tasks 553
9.11.5.6.1. Cluster backup scheduling 553
9.11.5.6.2. Tenant backup scheduling 554
9.11.5.6.3. Back up now 555
9.11.5.7. Recover backup data 556
9.11.5.8. Monitoring and alert configurations 557
9.11.6. Troubleshooting 559
9.11.6.1. Troubleshooting methods 559
9.11.6.2. Troubleshoot common faults 559
9.11.6.2.1. Insufficient memory 559
9.11.6.2.2. Insufficient disk space 559
9.11.6.2.3. High CPU utilization 560
9.11.6.2.4. High loads 560
9.12. Log Service 560
9.12.1. O&M methods 560
9.12.2. O&M 563
9.12.2.1. View logs on machines 563
9.12.2.2. Use Log Service Portal to view logs 569
9.13. Apsara Stack Security 571
9.13.1. Log on to the Apsara Infrastructure Management Fram... 571
9.13.2. Routine operations and maintenance of Server Guard 572
9.13.2.1. Check the service status 572
9.13.2.1.1. Check the client status 572

9.13.2.1.2. Check the status of Aegiserver 573
9.13.2.1.3. Check the Server Guard Update Service status 574
9.13.2.1.4. Check the Defender module status 574
9.13.2.2. Restart Server Guard 575
9.13.3. Routine operations and maintenance of Network Traff... 576
9.13.3.1. Check the service status 576
9.13.3.1.1. Basic inspection 576
9.13.3.1.2. Advanced inspection 576
9.13.3.2. Common operations and maintenance 577
9.13.3.2.1. Restart the Network Traffic Monitoring System ... 577
9.13.3.2.2. Uninstall Network Traffic Monitoring System 578
9.13.3.2.3. Disable TCP blocking 578
9.13.3.2.4. Enable TCPDump 578
9.13.4. Routine operations and maintenance of Anti-DDoS Se... 579
9.13.4.1. Check the service status 579
9.13.4.1.1. Basic inspection 579
9.13.4.1.2. Advanced inspection 579
9.13.4.2. Common operations and maintenance 581
9.13.4.2.1. Restart Anti-DDoS Service 581
9.13.4.2.2. Troubleshoot common faults 581
9.13.5. Routine operations and maintenance of Threat Detect... 584
9.13.5.1. Check the service status 584
9.13.5.1.1. Basic inspection 584
9.13.5.1.2. Advanced inspection 584
9.13.5.2. Restart Threat Detection Service 585
9.13.6. Routine operations and maintenance of Cloud Firewall 586
9.13.6.1. Check the service status 586
9.13.6.2. Restart Cloud Firewall 587

9.13.7. Routine operations and maintenance of WAF 587
9.13.7.1. Check the service status 587
9.13.7.1.1. Basic inspection 587
9.13.7.1.2. Advanced inspection 588
9.13.8. Routine operations and maintenance of Sensitive Data... 589
9.13.8.1. Check the service status 589
9.13.8.1.1. Basic inspection 589
9.13.8.1.2. Advanced inspection: Check the status of the S... 590
9.13.8.1.3. Advanced inspection: Check the status of the S... 591
9.13.8.1.4. Advanced inspection: Check the status of the S... 592
9.13.8.1.5. Advanced inspection: Check the status of the S... 592
9.13.8.2. Restart SDDP 593
9.13.9. Routine operations and maintenance of Apsara Stack ... 594
9.13.9.1. Check service status 594
9.13.9.1.1. Basic inspection 594
9.13.9.1.2. Advanced inspection 595
9.13.9.2. Restart the secure-console service 595
9.13.10. Routine operations and maintenance of secure-service 596
9.13.10.1. Check the service status 596
9.13.10.1.1. Basic inspection 596
9.13.10.1.2. Advanced inspection: Check the secure-service ... 596
9.13.10.1.3. Check the Dolphin service status 597
9.13.10.1.4. Check the data-sync service status 598
9.13.10.2. Restart secure-service 598
9.14. Key Management Service (KMS) 599
9.14.1. O&M of KMS components 599
9.14.1.1. Overview 599
9.14.1.2. Log on to the Apsara Infrastructure Management F... 600

9.14.1.3. KMS_HOST 601
9.14.1.4. HSA 603
9.14.1.5. ETCD 605
9.14.1.6. Rotator 606
9.14.1.6.1. Primary data center 606
9.14.1.6.2. Secondary data center 607
9.14.2. Log analysis 608
9.14.2.1. Overview 608
9.14.2.2. View logs by using request IDs 608
9.14.2.3. Common KMS errors 609
9.14.2.3.1. Overview 609
9.14.2.3.2. Errors with HTTP status code 4XX 609
9.14.2.3.3. Errors with HTTP status code 500 609
9.14.2.3.4. Errors with HTTP status code 503 609
9.14.2.3.5. Degradation of dependency on a service 610
9.15. Apsara Stack DNS 610
9.15.1. Introduction to Apsara Stack DNS 610
9.15.2. Maintenance 610
9.15.2.1. View operational logs 610
9.15.2.2. Enable and disable a service 610
9.15.2.3. Data backup 611
9.15.3. DNS API 611
9.15.3.1. Manage the API system 611
9.15.3.2. Troubleshooting 613
9.15.4. DNS system 613
9.15.4.1. Check whether a server role is normal 613
9.15.4.2. Troubleshooting 615
9.15.4.3. Errors and exceptions 615

9.15.5. Log analysis 615
9.15.6. View and process data 615
9.16. API Gateway 616
9.16.1. API Gateway introduction 616
9.16.2. Routine maintenance 616
9.16.2.1. View operational logs 616
9.16.2.2. Enable and disable a service 616
9.16.3. API Gateway O&M 617
9.16.3.1. System O&M 617
9.16.3.1.1. Check the desired state of API Gateway 617
9.16.3.1.2. Check the service status of OpenAPI 617
9.16.3.1.3. Check the service status of the API Gateway co... 619
9.16.3.1.4. Check the service status of API Gateway 620
9.16.3.1.5. View results of automated test cases 621
9.16.3.2. Troubleshooting 622
9.16.4. Log analysis 622
10.Operations of middleware products 623
10.1. Enterprise Distributed Application Service (EDAS) 623
10.1.1. O&M overview 623
10.1.1.1. Architecture 623
10.1.1.2. O&M architecture 625
10.1.2. Overview of critical operations 625
10.1.3. O&M preparation 626
10.1.4. Routine maintenance 627
10.1.4.1. Log on to the Apsara Infrastructure Management F... 627
10.1.4.2. Inspection 628
10.1.4.2.1. Component inspection 629
10.1.4.2.1.1. Manual inspection 629

10.1.4.3. Monitoring 630
10.1.4.3.1. Monitoring logs 631
10.1.5. Troubleshooting 631
10.1.5.1. Alert handling 632
10.1.5.1.1. CPU utilization alerts 632
10.1.5.1.2. Memory usage alerts 632
10.1.5.1.3. Disk usage alerts 633
10.1.5.1.4. Inspection alerts 634
10.1.5.2. Service continuity exceptions 634
10.1.5.2.1. EDAS monitoring exceptions 634
10.1.5.2.2. Excessive node logs 635
10.1.5.2.3. Console access failure 636
10.1.5.2.4. Failure to import an ECS instance 636
10.1.5.2.5. TLog data collection errors 637
10.1.6. Log reference 638
10.1.6.1. EDAS console logs 639
10.1.6.2. EDAS admin logs 640
10.1.6.3. EDAS server logs 641
10.1.6.4. DiamondServer logs 642
10.1.6.5. Cai-fs logs 642
10.1.6.6. ConfigServer logs 643
10.1.6.7. Cai-address logs 644
10.1.6.8. EagleEye console logs 644
10.1.7. Configuration reference 645
10.1.7.1. Component configuration 645
10.1.7.2. JVM configuration 649
11.Operations of big data products 651
11.1. Apsara Big Data Manager (ABM) platform 651

11.1.1. Routine maintenance 651
11.1.1.1. Perform routine maintenance 651
11.1.1.2. View the ABM operating status 651
11.1.1.3. Troubleshooting 655
11.1.2. Backup and restore 656
11.2. MaxCompute 656
11.2.1. Concepts and architecture 656
11.2.2. O&M commands and tools 659
11.2.2.1. Before you start 659
11.2.2.2. odpscmd commands 659
11.2.2.3. Tunnel commands 661
11.2.2.4. LogView tool 667
11.2.2.4.1. Before you start 667
11.2.2.4.2. LogView introduction 667
11.2.2.4.3. Preliminary knowledge of LogView 668
11.2.2.4.4. Basic operations and examples 671
11.2.2.4.5. Best practices 673
11.2.2.5. Apsara Big Data Manager 674
11.2.3. Routine O&M 674
11.2.3.1. Configurations 674
11.2.3.2. Routine inspections 674
11.2.3.3. Shut down a chunkserver, perform maintenance, a... 678
11.2.3.4. Shut down a chunkserver for maintenance withou... 682
11.2.3.5. Adjust the virtual resources of the Apsara system ... 683
11.2.3.6. Restart MaxCompute services 686
11.2.4. Common issues and solutions 687
11.2.4.1. View and allocate MaxCompute cluster resources 687
11.2.4.2. Common issues and data skew troubleshooting 696

11.2.5. MaxCompute O&M 703
11.2.5.1. Log on to the ABM console 703
11.2.5.2. Business O&M 704
11.2.5.2.1. O&M overview and entry 704
11.2.5.2.2. Project management 705
11.2.5.2.2.1. Project list 706
11.2.5.2.2.2. Project details 708
11.2.5.2.2.3. Encrypt data 712
11.2.5.2.2.4. Grant access permissions on the metadata ... 714
11.2.5.2.2.5. Perform disaster recovery 715
11.2.5.2.2.6. Migrate projects 718
11.2.5.2.3. Manage quota groups 725
11.2.5.2.4. Job management 727
11.2.5.2.4.1. Job snapshots 727
11.2.5.2.5. Business optimization 729
11.2.5.2.5.1. Merge small files 729
11.2.5.2.5.2. Compress idle files 735
11.2.5.2.5.3. Analyze resources 740
11.2.5.3. Service O&M 743
11.2.5.3.1. Control service O&M 743
11.2.5.3.1.1. O&M features and entry 743
11.2.5.3.1.2. Control service overview 744
11.2.5.3.1.3. Control service health 745
11.2.5.3.1.4. Instances 746
11.2.5.3.1.5. Control service configuration 746
11.2.5.3.1.6. Metadata warehouse for the control service 746
11.2.5.3.1.7. Stop or start a server role 747
11.2.5.3.1.8. Start AdminConsole 748

11.2.5.3.1.9. Collect service logs 749
11.2.5.3.2. Job Scheduler O&M 750
11.2.5.3.2.1. O&M features and entry 750
11.2.5.3.2.2. Overview 751
11.2.5.3.2.3. Job Scheduler health 754
11.2.5.3.2.4. Quotas 754
11.2.5.3.2.5. Instances 756
11.2.5.3.2.6. Job Scheduler compute nodes 757
11.2.5.3.2.7. Enable and disable SQL acceleration 758
11.2.5.3.2.8. Restart a master node of Job Scheduler 760
11.2.5.3.3. Apsara Distribute File System O&M 761
11.2.5.3.3.1. O&M features and entry 761
11.2.5.3.3.2. Overview 762
11.2.5.3.3.3. Instances 765
11.2.5.3.3.4. Apsara Distributed File System health 765
11.2.5.3.3.5. Apsara Distributed File System storage 766
11.2.5.3.3.6. Change the primary master node of Apsara... 768
11.2.5.3.3.7. Clear the recycle bin of Apsara Distributed ... 770
11.2.5.3.3.8. Enable or disable data rebalancing for Aps... 771
11.2.5.3.3.9. Run a checkpoint on a master node of Aps... 773
11.2.5.3.4. Tunnel service 773
11.2.5.3.4.1. O&M features and entry 774
11.2.5.3.4.2. Overview 774
11.2.5.3.4.3. Instances 775
11.2.5.3.4.4. Traffic analysis 776
11.2.5.3.4.5. Restart Tunnel servers 776
11.2.5.4. Cluster O&M 777
11.2.5.4.1. O&M features and entry 778

11.2.5.4.2. Cluster health 778
11.2.5.4.3. Overview 783
11.2.5.4.4. Servers 788
11.2.5.4.5. Scale in and scale out a MaxCompute cluster 788
11.2.5.4.6. Restore environment settings and enable auto ... 793
11.2.5.5. Host O&M 794
11.2.5.5.1. O&M features and entry 794
11.2.5.5.2. Host overview 795
11.2.5.5.3. Host charts 800
11.2.5.5.4. Host health 800
11.2.5.5.5. Host services 805
11.3. DataWorks 805
11.3.1. Basic concepts and structure 805
11.3.1.1. What is DataWorks? 805
11.3.1.2. Benefits 806
11.3.1.3. Introduction to data analytics 807
11.3.1.4. DataWorks architecture in Apsara Stack V3 807
11.3.1.5. Service directories 808
11.3.2. O&M by using Apsara Big Data Manager 809
11.3.2.1. Log on to the ABM console 809
11.3.2.2. DataWorks O&M overview 810
11.3.2.3. Service O&M 812
11.3.2.3.1. Data Warehouse 812
11.3.2.3.1.1. Service overview 812
11.3.2.3.1.2. Service health 815
11.3.2.3.1.3. Service instances 815
11.3.2.3.1.4. Service slots 816
11.3.2.3.1.5. Service nodes 820

11.3.2.3.1.6. Service settings 822
11.3.2.3.2. Data Integration 822
11.3.2.3.2.1. Data integration overview 822
11.3.2.3.2.2. View Data Integration nodes 823
11.3.2.3.2.3. View historical analysis information 824
11.3.2.3.3. Cluster scaling 825
11.3.2.4. Cluster O&M 828
11.3.2.4.1. Cluster overview 828
11.3.2.4.2. Cluster health 832
11.3.2.5. Host O&M 836
11.3.2.5.1. Host overview 836
11.3.2.5.2. Host health 841
11.3.3. Common administration tools and commands 845
11.3.3.1. Find the host where a service resides 845
11.3.3.2. View cluster resources 846
11.3.3.3. Commands to restart services 846
11.3.3.4. View logs of a failed instance 846
11.3.3.5. Rerun multiple instances at a time 847
11.3.3.6. Stop multiple instances at a time 847
11.3.3.7. Commonly used Linux commands 847
11.3.3.8. View the slot usage of resource groups 848
11.3.4. Process daily administration operations 849
11.3.4.1. Daily check 849
11.3.4.1.1. Check the service status and basic server inform... 849
11.3.4.1.2. Check the status of a gateway server 850
11.3.4.1.3. Monitor service roles and servers 851
11.3.4.2. View logs of the services 851
11.3.4.3. Scale out the cluster that runs the base-biz-gatew... 851

11.3.4.4. Scale in the base-biz-gateway cluster 856
11.3.4.5. Restart the base-biz-tenant service 858
11.3.4.6. Restart the Redis services 860
11.3.4.7. Restart the base-biz-dmc service 861
11.3.4.8. Restart the base-biz-alisa service 863
11.3.4.9. Restart the base-biz-phoenix service 865
11.3.4.10. Restart the base-biz-gateway service 867
11.3.4.11. Restart DataWorks Data Service 868
11.3.4.12. Restart base-biz-gateway 868
11.3.4.13. Configure a resource group in a multi-region env... 869
11.3.4.14. Configure a resource group for Data Integration i... 872
11.3.5. Common issues and solutions 874
11.3.5.1. Nodes remain in the Pending (Resources) state 875
11.3.5.2. An out-of-memory (OOM) error occurs when synch... 877
11.3.5.3. A task does not run at the specified time 878
11.3.5.4. The test service of base is not in the desired stat... 878
11.3.5.5. The Data Management page does not display the ... 878
11.3.5.6. Logs are not automatically cleaned up 879
11.3.5.7. The real-time analysis service is not in the desired... 879
11.4. Realtime Compute 880
11.4.1. Job status 880
11.4.1.1. Overview 880
11.4.1.2. Task status 880
11.4.1.3. Health score 880
11.4.1.4. Job instantaneous values 880
11.4.1.5. Running topology 881
11.4.2. Curve charts 883
11.4.2.1. Overview 883

11.4.2.2. Overview 884
11.4.2.3. Advanced view 887
11.4.2.4. Processing delay 889
11.4.2.5. Throughput 889
11.4.2.6. Queue 889
11.4.2.7. Tracing 890
11.4.2.8. Process 890
11.4.2.9. JVM 890
11.4.3. FailOver 891
11.4.4. CheckPoints 891
11.4.5. JobManager 892
11.4.6. TaskExecutor 892
11.4.7. Data lineage 892
11.4.8. Properties and Parameters 892
11.4.9. Performance optimization by using automatic configur... 894
11.4.10. Improve performance by manual configuration 901
11.4.10.1. Overview 901
11.4.10.2. Optimize resource configuration 902
11.4.10.3. Improve performance based on job parameter set... 903
11.4.10.4. Optimize upstream and downstream data storage... 904
11.4.10.5. Apply new configuration 904
11.4.10.6. Concepts 905
11.4.11. O&M of Apsara Big Data Manager 906
11.4.11.1. What is Apsara Big Data Manager? 906
11.4.11.2. Log on to the ABM console 906
11.4.11.3. O&M overview of Realtime Compute for Apache F... 907
11.4.11.4. Business O&M 909
11.4.11.4.1. Projects 909

11.4.11.4.2. Jobs 909
11.4.11.4.3. Queues 910
11.4.11.5. Service O&M 910
11.4.11.5.1. Blink 910
11.4.11.5.2. Yarn 911
11.4.11.5.3. HDFS 912
11.4.11.6. Cluster O&M 914
11.4.11.6.1. Cluster overview 914
11.4.11.6.2. Cluster health 917
11.4.11.6.3. Hosts 922
11.4.11.6.4. Cluster scale-out 922
11.4.11.6.5. Cluster scale-in 924
11.4.11.7. Host O&M 925
11.4.11.7.1. Host overview 925
11.4.11.7.2. Host health 931
11.4.11.7.3. Host charts 935
11.4.11.7.4. Host services 935
11.4.11.8. Job and queue analysis 935
11.4.11.8.1. Job analysis 935
11.4.11.8.2. Queue analysis 937
11.5. Apsara Big Data Manager (ABM) 937
11.6. Quick BI 937
11.6.1. Introduction to O&M and tools 937
11.6.1.1. O&M overview 937
11.6.1.2. Check the Quick BI status in the Apsara Infrastruct... 938
11.6.1.3. Perform O&M on Quick BI in the ABM console 939
11.6.2. Routine maintenance 940
11.6.2.1. Introduction to Quick BI components 940

11.6.2.2. Database initialization components 940
11.6.2.3. Cache components 940
11.6.2.4. Runtime components 941
11.6.2.5. Web service components 941
11.6.2.6. Automated testing components 942
11.6.3. Quick BI O&M 943
11.6.3.1. Log on to the ABM console 943
11.6.3.2. Quick BI O&M 944
11.6.3.3. Service O&M 945
11.6.3.3.1. Service overview 945
11.6.3.3.2. Quick BI service hosts 949
11.6.3.4. Cluster O&M 950
11.6.3.4.1. Cluster overview 950
11.6.3.4.2. Cluster health 953
11.6.3.5. Host O&M 957
11.6.3.5.1. Host overview 957
11.6.3.5.2. Host health 962
11.7. Graph Analytics 967
11.7.1. Operations and maintenance tools and logon methods 967
11.7.1.1. Log on to the ABM console 967
11.7.1.2. Log on to Apsara Infrastructure Management Fram... 968
11.7.1.3. Log on to the Graph Analytics container 969
11.7.2. Operations and maintenance 971
11.7.2.1. Operations and maintenance based on BigData Ma... 971
11.7.2.1.1. O&M overview 971
11.7.2.1.2. Service O&M 972
11.7.2.1.2.1. Service overview 972
11.7.2.1.2.2. Service hosts 976

11.7.2.1.3. Cluster O&M 977
11.7.2.1.3.1. Cluster overview 977
11.7.2.1.3.2. Cluster health 980
11.7.2.1.4. Host O&M 984
11.7.2.1.4.1. Host overview 984
11.7.2.1.4.2. Host health 989
11.7.2.2. O&M on Apsara Infrastructure Management Framew.. 994
11.7.2.3. Operations and maintenance based on the Graph ... 995
11.7.2.3.1. View instances 995
11.7.2.3.2. Log files 996
11.7.2.3.3. Database logs 996
11.7.2.3.4. Stop the service 997
11.7.2.3.5. Restart the service 997
11.7.3. Security maintenance 997
11.7.3.1. Network security maintenance 997
11.7.3.2. Account password maintenance 998
11.7.4. Troubleshooting 998
11.7.4.1. Fault response mechanism 998
11.7.4.2. Troubleshooting methods 998
11.7.4.3. Common failure troubleshooting 998
11.7.4.4. Hardware troubleshooting 998
11.8. Machine Learning Platform for AI 999
11.8.1. Query server and application information 999
11.8.1.1. Apsara Stack Machine Learning Platform for AI 999
11.8.1.1.1. Query server information 999
11.8.1.1.2. Log on to a server 999
11.8.1.1.3. Query configurations 1000
11.8.1.1.4. Restart an application service 1000

11.8.1.2. Online model service 1001
11.8.1.2.1. Query online model service information 1001
11.8.1.2.2. Log on to the online model service container 1001
11.8.1.2.3. Restart a pod 1002
11.8.1.3. GPU cluster and task information 1002
11.8.1.3.1. Query GPU cluster information 1002
11.8.1.3.2. Query GPU task information 1002
11.8.2. Maintenance and troubleshooting 1003
11.8.2.1. Machine Learning Platform for AI maintenance 1003
11.8.2.1.1. Run ServiceTest 1003
11.8.2.1.2. Common faults and solutions 1004
11.8.2.1.2.1. Maintenance commands 1004
11.8.2.1.2.2. pai.xx.xx access failures 1004
11.8.2.1.2.3. Experiment failures 1005
11.8.2.1.2.4. Other failures 1005
11.8.2.2. Online model service maintenance (must be activa... 1005
11.8.2.3. GPU cluster maintenance (deep learning must be ... 1006
11.9. DataHub 1007
11.9.1. Concepts and architecture 1007
11.9.1.1. Terms 1007
11.9.1.2. Architecture 1010
11.9.1.2.1. Architecture 1010
11.9.1.2.2. Technical architecture 1011
11.9.2. Commands and tools 1013
11.9.2.1. Common commands for the Apsara system 1013
11.9.2.2. Common commands for Apsara Distributed File Sys.. 1013
11.9.2.3. Common commands for Job Scheduler 1014
11.9.2.4. Xstream 1015

11.9.2.5. DataHub console 1017
11.9.2.6. Apsara Big Data Manager 1017
11.9.3. Routine maintenance 1017
11.9.3.1. Restore data after a power outage 1017
11.9.3.2. Shut down anomalous chunkserver hosts 1018
11.9.3.3. Shut down a DataHub cluster 1020
11.9.3.4. Replace a hard drive with a new one on the pan... 1021
11.9.4. DataHub O&M 1022
11.9.4.1. Log on to the ABM console 1022
11.9.4.2. Common operations 1023
11.9.4.3. DataHub O&M overview 1030
11.9.4.4. Business O&M 1032
11.9.4.4.1. Business O&M 1032
11.9.4.4.2. Projects 1033
11.9.4.4.3. Topics 1033
11.9.4.4.4. Hotspot analysis 1034
11.9.4.4.5. Archiving latency 1035
11.9.4.5. Service O&M 1035
11.9.4.5.1. Control Service O&M 1035
11.9.4.5.2. Service O&M for Job Scheduler 1035
11.9.4.5.2.1. Job Scheduler O&M entry 1036
11.9.4.5.2.2. Service overview 1036
11.9.4.5.2.3. Service instances 1038
11.9.4.5.2.4. Service health 1038
11.9.4.5.2.5. Compute nodes 1038
11.9.4.5.3. Service O&M for Apsara Distributed File System 1039
11.9.4.5.3.1. Apsara Distributed File System O&M entry 1039
11.9.4.5.3.2. Service overview 1040

11.9.4.5.3.3. Service roles 1043
11.9.4.5.3.4. Service health 1043
11.9.4.5.3.5. Storage nodes 1043
11.9.4.5.3.6. Clear the recycle bin of Apsara Distributed ... 1045
11.9.4.5.3.7. Enable or disable data rebalancing for Apsa.. 1046
11.9.4.5.3.8. Run a checkpoint on master nodes of Apsa... 1048
11.9.4.5.3.9. Change the primary master node of Apsara... 1049
11.9.4.6. Cluster O&M 1051
11.9.4.6.1. Cluster O&M entry 1051
11.9.4.6.2. Cluster overview 1051
11.9.4.6.3. Cluster health 1055
11.9.4.6.4. Cluster hosts 1059
11.9.4.6.5. Cluster scale-out 1059
11.9.4.6.6. Cluster scale-in 1062
11.9.4.6.7. Delete topics from a smoke testing project 1064
11.9.4.6.8. Reverse parse request ID 1065
11.9.4.7. Host O&M 1065
11.9.4.7.1. Host O&M entry 1066
11.9.4.7.2. Host overview 1066
11.9.4.7.3. Host charts 1070
11.9.4.7.4. Host health 1071
11.9.4.7.5. Host services 1075
11.9.5. Exceptions and solutions 1075
11.9.6. Appendix 1076
11.9.6.1. Installation environment 1076
11.9.6.2. Deployment directories and services 1076
11.9.6.3. Error codes 1077
11.10. E-MapReduce (EMR) 1078

11.10.1. Methods for logging on to O&M platforms 1078
11.10.1.1. Log on to Apsara Infrastructure Management Fram... 1079
11.10.2. Routine maintenance 1080
11.10.2.1. O&M in the Apsara Infrastructure Management Fra.. 1080
11.10.3. Troubleshooting 1081
11.10.3.1. Troubleshooting methods 1081
11.11. Dataphin 1081
11.11.1. What is Apsara Big Data Manager? 1081
11.11.2. Log on to the ABM console 1081
11.11.3. O&M overview and entry 1082
11.11.4. Service O&M 1084
11.11.4.1. Service overview 1084
11.11.4.2. Service hosts 1088
11.11.5. Cluster O&M 1088
11.11.5.1. Cluster overview 1088
11.11.5.2. Cluster health 1091
11.11.6. Host O&M 1096
11.11.6.1. Host overview 1096
11.11.6.2. Host health 1101
11.12. Elasticsearch (on ECS) 1105
11.12.1. What is Apsara Big Data Manager? 1105
11.12.2. Log on to the ABM console 1105
11.12.3. Elasticsearch O&M overview 1106
11.12.4. Business O&M 1108
11.12.4.1. Cluster configuration 1108
11.12.4.2. System configuration 1108
11.12.5. Service O&M 1109
11.12.5.1. Service overview 1109

11.12.5.2. Service hosts 1112
11.12.6. Cluster O&M 1113
11.12.6.1. Cluster overview 1113
11.12.6.2. Cluster health 1116
11.12.7. Host O&M 1120
11.12.7.1. Host overview 1120
11.12.7.2. Host charts 1124
11.12.7.3. Host health 1125
11.12.7.4. Host services 1129
11.12.8. Online O&M 1129
11.12.8.1. Cluster health 1129
11.12.9. Common failure troubleshooting 1130
11.12.9.1. Resolve the issue that the health state of an Elas... 1130
11.12.9.2. Query index status 1130
11.12.9.3. Recover an index 1130
12.Appendix 1131
12.1. Operation Access Manager (OAM) 1131
12.1.1. Introduction to OAM 1131
12.1.2. Usage instructions 1131
12.1.3. Quick Start 1132
12.1.3.1. Log on to OAM 1132
12.1.3.2. Create a group 1134
12.1.3.3. Add a group member 1134
12.1.3.4. Add a group role 1135
12.1.3.5. Create a role 1136
12.1.3.6. Add an inherited role to a role 1138
12.1.3.7. Add a resource to a role 1139
12.1.3.8. Assign a role to authorized users 1141

12.1.4. Manage groups 1142
12.1.4.1. Modify group information 1142
12.1.4.2. View group role details 1142
12.1.4.3. Delete a group 1143
12.1.4.4. View authorized groups 1143
12.1.5. Manage roles 1143
12.1.5.1. Query roles 1143
12.1.5.2. Modify role information 1144
12.1.5.3. View the role inheritance tree 1144
12.1.5.4. Transfer a role 1144
12.1.5.5. Delete a role 1145
12.1.5.6. View assigned roles 1145
12.1.5.7. View all roles 1146
12.1.6. Search for resources 1146
12.1.7. View personal information 1146
12.1.8. Default roles and permissions 1147
12.1.8.1. Default roles and their functions 1147
12.1.8.1.1. Default role of OAM 1147
12.1.8.1.2. Default roles of Tablestore Operations and Main... 1147
12.1.8.1.3. Default roles of Apsara Infrastructure Managem... 1148
12.1.8.1.4. Default roles of Webapp-rule 1150
12.1.8.1.5. Default roles of the workflow console 1150
12.1.8.1.6. Default roles of Tianjimon 1151
12.1.8.1.7. Default roles of Rtools 1151
12.1.8.1.8. Default roles of the Apsara Uni-manager Opera... 1152
12.1.8.1.9. Default roles of PaaS 1154
12.1.8.1.10. Default roles of OCP 1155
12.1.8.1.11. Default roles of Apsara Stack Security 1155

12.1.8.1.12. Default roles of Apsara Network Intelligence ---------- 1156
12.1.8.2. Operation permissions on O&M platforms -------------------- 1156
12.1.8.2.1. Permissions on Apsara Infrastructure Manageme...----- 1156
12.1.8.2.2. Permission list of Webapp-rule ------------------------------- 1166
12.1.8.2.3. Permission list of the workflow console ----------------- 1166
12.1.8.2.4. Permissions on Monitoring System of Apsara In...----- 1167
12.1.8.2.5. Permissions on Rtools --- 1167

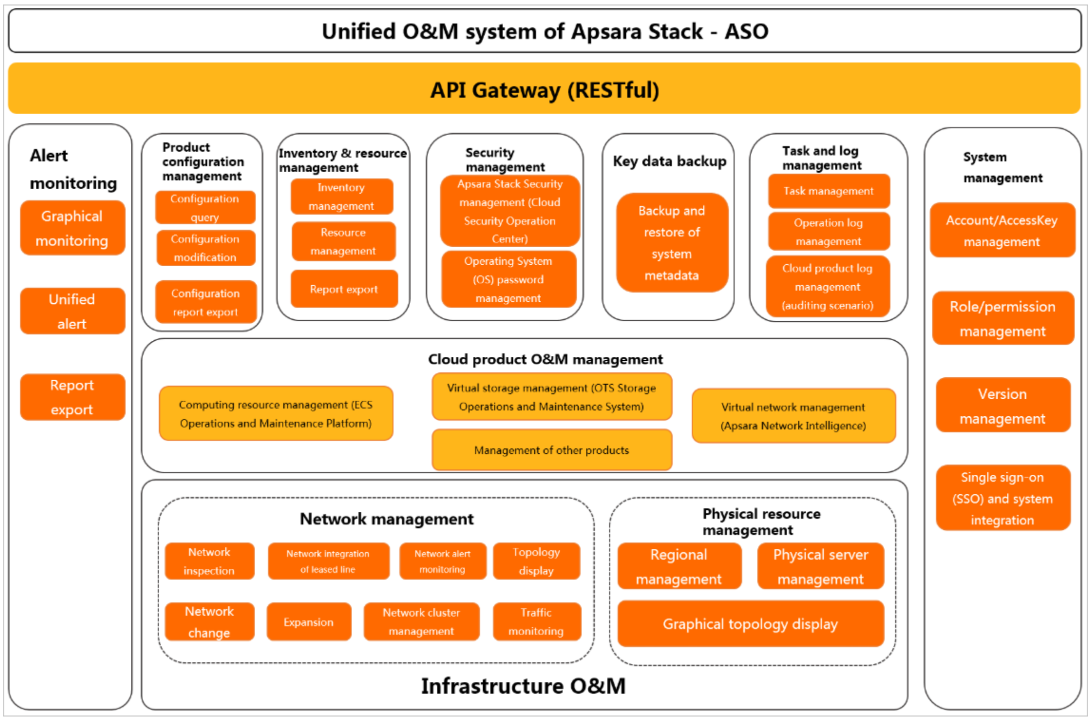
1.Overview

This topic describes the management system of the Apsara Uni-manager Operations service.

In accordance with the Information Technology Infrastructure Library (ITIL) and IT Service Management (ITSM) standards, the operations processes and requirements must be abstract, and automation is implemented by using intelligent operations tools. For customized operations, interfaces and multi-level approval must be used to reduce risks.

Alibaba Cloud Apsara Stack adopts the ISO 20000 standard and references the methods regulated by the Information Technology Service Standards (ITSS) and ITIL frameworks to build the management framework of the Apsara Uni-manager Operations service. The following figure shows the management framework of the Apsara Uni-manager Operations system.

Apsara Uni-manager Operations System


Unified O&M system of Apsara Stack - ASO
API Gateway (RESTful)
Alert monitoring
Graphical monitoring
Unified alert
Report export
Product configuration management
Configuration query
Configuration modification
Configuration report export
Inventory & resource management
Inventory management
Resource management
Report export
Security management
Apsara Stack Security management (Cloud Security Operation Center)
Operating System (OS) password management
Key data backup
Backup and restore of system metadata
Task and log management
Task management
Operation log management
Cloud product log management (auditing scenario)
System management
Account/AccessKey management
Role/permission management
Version management
Single sign-on (SSO) and system integration
Cloud product O&M management
Computing resource management (ECS Operations and Maintenance Platform)
Virtual storage management (OTS Storage Operations and Maintenance System)
Management of other products
Virtual network management (Apsara Network Intelligence)
Network management
Network inspection
Network integration of leased line
Network alert monitoring
Topology display
Network change
Expansion
Network cluster management
Traffic monitoring
Physical resource management
Regional management
Physical server management
Graphical topology display
Infrastructure O&M

The Apsara Uni-manager Operations Console is a unified and intelligent O&M platform. In the Apsara Uni-manager Operations system, cloud operations is classified into the following layers: infrastructure, cloud service, and business operations. The management framework of the Apsara Uni-manager Operations service provides the full lifecycle management methods, management standards, management modes, management supporting tools, management objects, and process-based management methods of IT operations services.

The Apsara Uni-manager Operations Console provides a centralized operations portal that allows you to have a consistent operations experience. The Apsara Uni-manager Operations Console supports interconnections with third-party platforms and provides centralized API operations capabilities to deliver data to third-party systems by using APIs.

The Apsara Uni-manager Operations Console performs centralized operations management, such as automated deployments, upgrades, changes, and configurations, on physical devices, operating systems, computing resources, network, storage, databases, middleware, and business applications in the cloud computing environment. The Apsara Uni-manager Operations Console also provides the features of alert monitoring and automatic analysis, diagnosis, and troubleshooting for faults, performance, and configurations. By analyzing, processing, and evaluating the running status and quality of cloud platforms, the Apsara Uni-manager Operations Console guarantees the continuous and stable running of cloud computing business applications and provides services and support for operations processes to build an improved operations service management platform.

Based on ITIL and ISO 20000, the management framework of the Apsara Uni-manager Operations system uses management supporting tools to adapt to various management modes in a process-oriented, normalized, and standardized manner. This has implemented the systematic management of the overall process of operations services.

Based on the operations experience and data accumulated and collected from three layers, Alibaba Cloud Apsara Stack aggregates data collected by the operations platform to the Configuration Management Database (CMDB) of the platform. The Apsara Uni-manager Operations Console consolidates, analyzes, and comprehensively processes the data and integrates rich practical experience and operations capabilities to the platform operations tools. The Apsara Uni-manager Operations Console is designed to be desired state-oriented and uses unified operations tools for the fault discovery and tracking, link display, ITIL process, and self-repaired faults of the platform to realize the ultimate goal of artificial intelligence for IT operations (AIOps).

In addition to tools, process assurance and personnel management are essential to ensure the integrity of operations. Apsara Stack provides on-site development supporting services for major problems, on-site services, expert escort services, business consulting services, and business optimization services. Apsara Stack provides the first-line, second-line, and third-line supporting systems to support platform problems of customers and provides upgrade channels to support urgent problems of customers. As an autonomous and controllable platform, the Apsara Uni-manager Operations Console ensures that technical problems can be effectively solved in a timely manner.

The Apsara Uni-manager Operations system defines various entities involved in operations activities and relationships between these entities. Relevant entities are well organized and coordinated based on the Apsara Uni-manager Operations service management system and can provide different levels of operations services based on the service agreements.

2.Get started

2.1. Prepare an operations account

Before you perform O&M operations in the Apsara Uni-manager Operations Console, make sure that you have obtained an operations account that have corresponding permissions from an administrator.

Perform the following steps to create an operations account and grant permissions to the account:

1. Log on to the Apsara Uni-manager Operations Console as an administrator.
2. Create a role. For more information, see Role management.
3. Create an operations account and grant the created role to the account. For more information, see User management.

> ⓘ **Note** For a more fine-grained division of the operations role, you can create a basic role as specified in **Appendix > OAM**, grant permissions to the role, and then grant the role to the corresponding operations account as an administrator.

2.2. Log on to the Apsara Uni-manager Operations Console

This topic describes how to log on to the Apsara Uni-manager Operations Console.

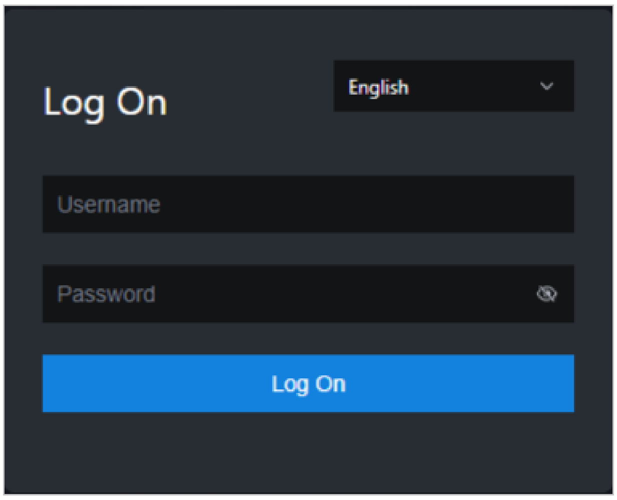
Prerequisites

- The URL, username, and password that are required to log on to the Apsara Uni-manager Operations Console are obtained from the deployment personnel or administrators.

  The URL of the Apsara Uni-manager Operations Console is in the format of *region-id*.ops.console.*intranet-domain-id*.
- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL. Then, press the Enter key.



> Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   > Note To obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console, contact the deployment personnel or administrators.

   If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username as prompted.

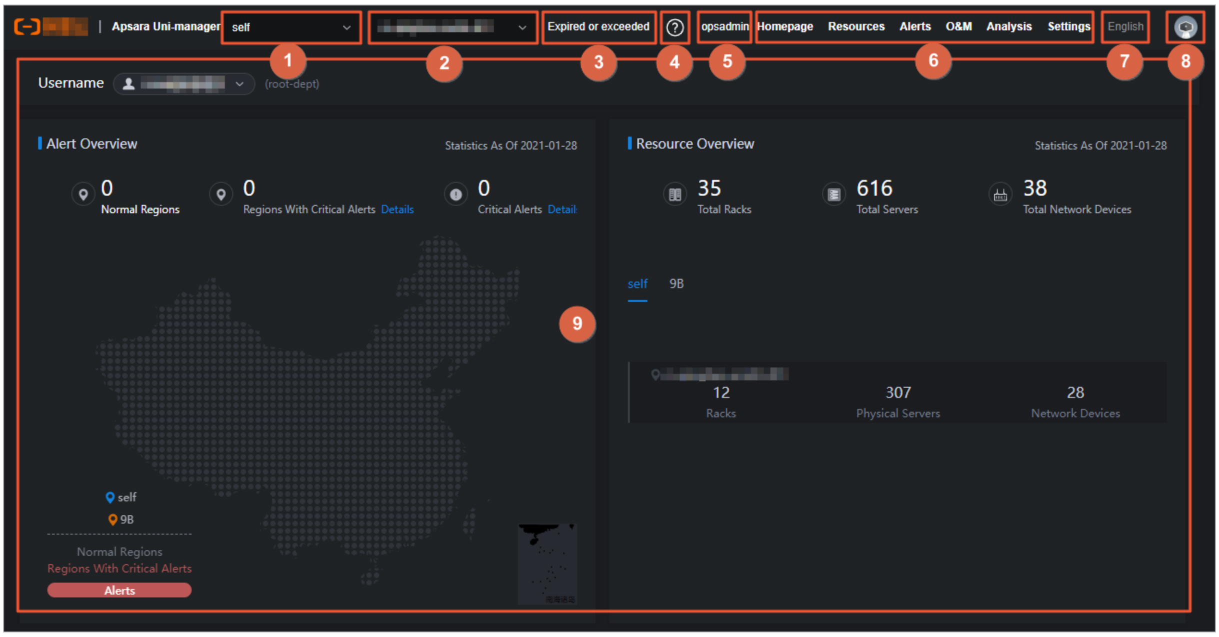
   To enhance security, make sure that the password meets the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password is 10 to 20 characters in length.

4. Click **Log On**.

2.3. Apsara Uni-manager Operations Console homepage

This topic describes the basic operations on and features of the Apsara Uni-manager Operations Console.



[redacted] | Apsara Uni-manager self [redacted] Expired or exceeded ? opsadmin Homepage Resources Alerts O&M Analysis Settings English

Username [redacted] (root-dept)

Alert Overview Statistics As Of 2021-01-28

0	0	0
Normal Regions	Regions With Critical Alerts Details	Critical Alerts Detail

self
9B
Normal Regions
Regions With Critical Alerts
Alerts

Resource Overview Statistics As Of 2021-01-28

35	616	38
Total Racks	Total Servers	Total Network Devices

self 9B

[redacted]

12	307	28
Racks	Physical Servers	Network Devices

The following table describes the sections on the homepage of the console.

NO.	Section	Description
①	Cloud	Switch the cloud from the drop-down list.
②	Region	Switch the region from the drop-down list and centrally manage each region.
③	Authorization information	Click this section to go to the **Authorization** page and then view the authorization conditions of services.
④	Help center	View the alert knowledge base and upload other relevant HTML documents.
⑤	Current user	Show the name of the current logon user.
⑥	Top navigation bar	Select an O&M operation.
⑦	Language	Move the pointer over this section and select a language.
⑧	Current user information	Move the pointer over this section and select an item to view the personal information of the current user, modify the password, configure logon parameters, or log off from the console.

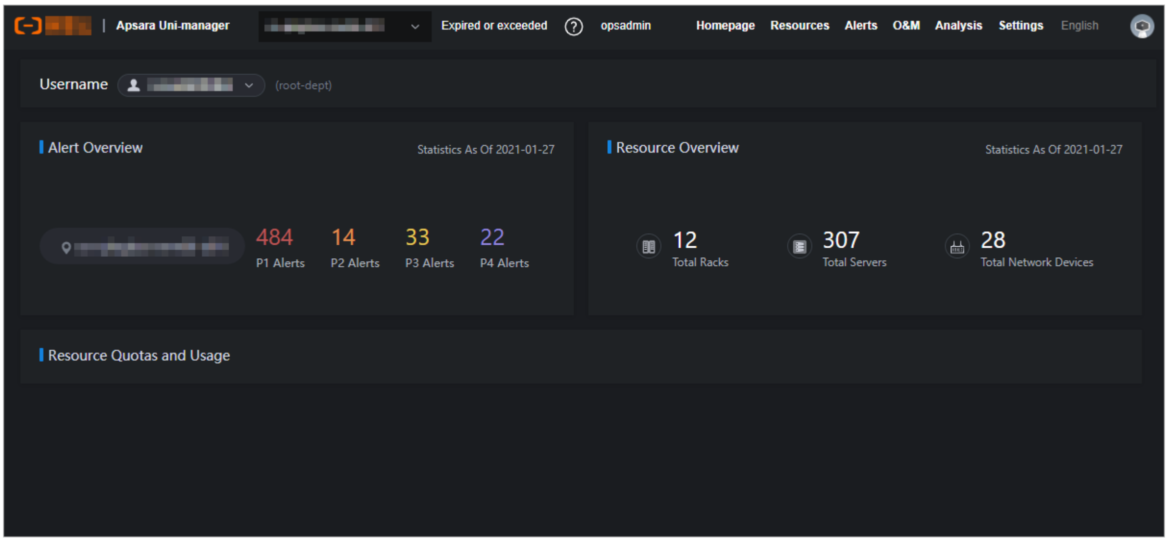
NO.	Section	Description
⑨	Operation	View information and perform operations.

2.4. Instructions for the homepage

The homepage allows you to view the statistics and summary data of Apsara Stack alerts, physical devices, and cloud service inventory.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. On the top navigation bar, click **Homepage**.
3. View the homepage. The homepage consists of the **opsadmin**, **Alert Overview**, **Resource Overview**, and **Resource Quotas and Usage** sections.



- In the **opsadmin** section, select a user. The department to which the user belongs is displayed on the right.
- In the **Alert Overview** section, view the total number of alerts at the P1, P2, P3, and P4 levels.
- In the **Resource Overview** section, view the total number of racks, servers, and network devices.
- In the **Resource Quotas and Usage** section, view the resource quotas and usage related to cloud services.

  The cloud service-related metrics are displayed in the following dimensions: total quantity, used and available resources, and usage.

Cloud service	Statistical metric
ECS	CPU (Core)
	Disk EBS (GB)
	Memory (GB)

Cloud service	Statistical metric
RDS	CPU (Core)
	Disk (GB)
	Memory (GB)
SLB	Internal network VIP
	Public network VIP
OSS	Storage capacity (GB)
DFS	Memory (GB)
SLS	SLS-INNER
	SLS-PUBLIC
OTS	Memory (GB)
NAS	Memory (GB)

3.Settings

3.1. Default operations roles

This topic describes the default roles for the Apsara Uni-manager Operations Console and their responsibilities.

For quick reference, the following roles are preset in the Apsara Uni-manager Operations Console: Operation Administrator Manager (OAM) super administrator, system administrator, security officer, security auditor, and multi-cloud configuration administrator. The following table describes these roles and their responsibilities.

Role	Responsibility
OAM super administrator	The administrator of OAM, with the root permissions of the system. By default, this role is not displayed in the role list.
System administrator	Manages platform nodes, physical devices, and virtual resources, backs up, restores, and migrates product data, as well as searches for and backs up system logs.
Security officer	Manages permissions, security policies, and network security, and reviews and analyzes security logs and activities of auditor officers.
Security auditor	Audits, tracks, and analyzes operations of the system administrator and the security officer.
Multi-cloud configuration administrator	Manages multi-cloud operations, and adds, deletes, and modifies multi-cloud configurations.

3.2. Security policies

3.2.1. Logon policies

As an administrator, you can configure logon policies to control the logon time and IP addresses that are permitted to log on.

Context

The system provides a default policy. You can configure logon policies based on your needs to better control the read and write permissions of users and improve the system security.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Security > Logon Policy**.
4. On the **Logon Policies** page, perform the following operations:
   - Query policies

In the upper-left corner of the page, enter a policy name in the **Policy Name** field and click **Search** to view the policy information in the list. You can click **Reset** to clear the specified search conditions.

- Add a policy

  Click **Add Policy**. In the Add Policy dialog box, set the policy name, start time, end time, and logon IP addresses. Click **OK**. If you select blacklist for logon settings, the specified IP addresses are prohibited from logging on to the Apsara Uni-manager Operations Console. If you select whitelist for logon settings, the specified IP addresses are allowed to log on to the Apsara Uni-manager Operations Console. For more information about operations on logon settings, see Modify logon settings.

- Modify a policy

  Find the policy that you want to modify, and click **Modify** in the **Actions** column. In the **Modify Policy** dialog box, modify the parameters and click **OK**.

- Delete a policy

  Find the policy that you want to delete and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

  > **Notice** A logon policy that is bound to a user cannot be deleted. You must unbind the policy before you can delete it.

3.2.2. Physical server passwords

The Server Password module allows you to configure and manage passwords, as well as query the historical passwords of all physical servers in the Apsara Stack environment.

Context

Server password management covers the passwords of all servers in the Apsara Stack environment.

- The system collects the information of all servers in the Apsara Stack environment.
- The server password is updated periodically.
- You can configure the password expiration period and password length.
- You can manually update the passwords of one or more servers at a time.
- The system records the history of server password updates.
- You can search for server passwords by product, hostname, or IP address.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Security > Server Password**.

   The **Manage Passwords** tab appears. The **Manage Passwords** tab shows the passwords of all the servers in the current Apsara Stack environment.
4. Perform the following operations:
   - Query servers

On the **Manage Passwords** tab, select a product or host name, or enter an IP address, and then click **Search**. You can also click **Reset** to clear the previous search conditions.

- Query a password

  a. On the **Manage Passwords** tab, find a server.

  b. Click the 👁 icon in the corresponding **Password** column. The server password in plaintext is displayed and turns into cipher text after 10 seconds. Alternatively, click the 👁 icon to show the cipher text.

- Update a password

  a. On the **Manage Password** tab, find a server.

  b. Click **Update Password** in the corresponding **Actions** column.

  c. In the dialog box that appears, enter **New Password** and **Confirm Password** and click **OK**.

     The password of the server is updated.

- Batch update passwords

  a. On the **Manage Password** tab, select multiple servers.

  b. Click **Batch Update** in the upper part of the tab.

  c. In the dialog box that appears, enter **New Password** and **Confirm Password** and click **OK**.

     The passwords of the selected servers are updated.

- Configure the password expiration period

  a. On the **Manage Password** tab, select one or more servers.

  b. Click **Configure** in the upper part of the tab.

  c. In the **Configuration Items** dialog box, specify **Password Expiration Period** and **Unit** and click **OK**.

     Server passwords are updated immediately and are updated again after the expiration period.

- Query the update history of server passwords

  Click the **History Password** tab. Select a product, hostname, or IP address, and then click Search to view the update history of server passwords in the search results.

- Query historical passwords of a server

  a. On the **History Password** tab, find a server.

  b. Click the 👁 icon in the corresponding **Password** column. The server password in plaintext is displayed and turns into cipher text after 10 seconds. Alternatively, click the 👁 icon to show the cipher text.

- Query and modify the password configuration policies

a. Click the **Configuration** tab and view the metadata of server password management, including the initial password, password length, and retry times. Notes:
   - **Initial Password** indicates the password assigned when server password management is deployed in the Apsara Stack environment. This parameter is necessary to change the password of a server in the Apsara Stack environment.
   - **Password Length** indicates the length of passwords updated by the system.
   - **Retry Times** indicates a limit of how many times a password can fail to be updated before the system stops trying.
   - **Status** indicates whether the configuration takes effect. By default, the switch is turned off. To show the status, turn on ○.

b. Click **Save**.

3.3. Offline backup

Offline Backup is used to back up the key metadata of Apsara Stack. Only the metadata of Apsara Distributed File System can be backed up. The backup metadata information is used for quick recovery from Apsara Stack failures.

3.3.1. Add a backup product

The Product Management module allows you to add product backup information. Only the metadata of Apsara Distributed File System can be backed up.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Offline Backup > Product Management**.
4. Click **Add Product**.
5. In the **Add Product** dialog box, add the information of a product as described in the following table and click **OK**.

Parameter	Description
Product	The product name. Set this parameter to pangu to back up the Apsara Distributed File System data.
Backup Item	The name of the backup item. Set this parameter based on the Apsara Distributed File System information of the cloud product to be backed up in the product name_pangu format. Example: ecs_pangu.
Script	The name of the backup script. Example: metadata_backup.py.
Retry Times	The number of times to retry after an error occurs. Typically, set this parameter to 3.

6. To add more product backup items, perform the preceding steps again.

> ? **Note** You can click **Modify** or **Delete** in the **Actions** column to modify or delete a product backup item.

Result

You can view the added product on the **Backup Configurations** page.

3.3.2. Configure backup

After you add a product backup item, you must configure the backup in the Apsara Uni-manager Operations Console.

Prerequisites

A product backup item is added. For more information about how to add a product backup item, see Add a backup product.

Context

The backup item is the minimum unit for backup. You can back up the metadata of Apsara Distributed File System for different products, such as ecs pangu and ots pangu.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Offline Backup > Backup Configurations**. In the left side of the Backup Configurations page, the current backup configurations is displayed in a hierarchical tree-like structure. The root node is a product list and shows the products whose data can be backed up in the current backup system. Only the metadata of Apsara Distributed File System can be backed up.
4. Click a product backup item on the left and then configure the parameters on the right.

Parameter	Description
Product Cluster IP Address	The IP address of the actual transfer server.
Backup File Folder	A folder on the transfer server. You are required only to enter a value in the field instead of manually creating a folder. Example: /apsarapangu/disk8/pangu_master_bak/*product name*_pangu/bak
Script Execution Folder	A folder on the transfer server. You are required only to enter a value in the field instead of manually creating the folder. Example: /apsarapangu/disk8/pangu_master_bak/*product name*_pangu/bin

Parameter	Description
Script Parameters	The execution parameters for the script. You must enter the value in the `--ip=xxx.xxx.xxx.xxx` format, in which the IP address is one of the IP addresses of the pangu master.
Backup Schedule	The execution period of recurring executions. In this example, a value of 1 is entered to specify that the backup is performed only once.
Backup Schedule Unit	The unit of the execution period. Valid values: **Day**, **Hour**, and **Minute**. In this example, **Hour** is selected to specify that the backup is performed by hour.
Timeout Period	The timeout period, in seconds. In this example, set the value to **3600**.

5. Click **Modify** to complete the configurations and trigger the backup.
6. Perform the preceding steps to configure all the product backup items.

3.3.3. View the backup details

During the backup, you can view the backup details of each backup item on the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Offline Backup > Backup Details**.
4. On the **Backup Details** page, enter the service and backup item, select the start date, and then click **Search**.
5. View the backup details of a backup item, including the product, backup item, the name of the file to be backed up, start time, and status.

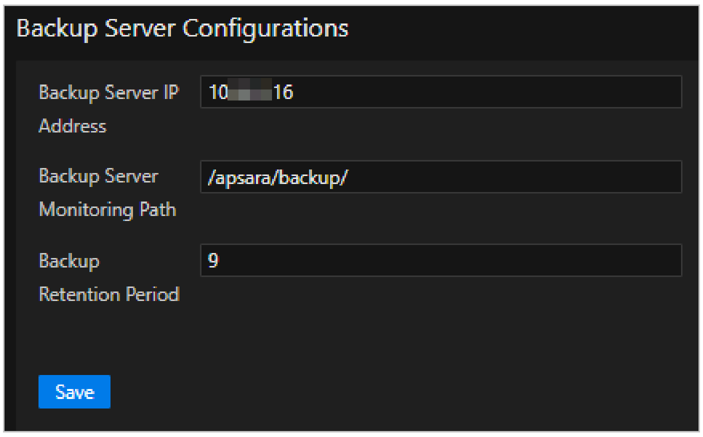
   The backup status includes **Not started**, **In transmission**, **Complete**, **Time-out**, and **Failed**.
6. (Optional) click **Reset** to clear the previous search conditions.

3.3.4. Configure a backup server

You can configure a backup server for the subsequent storage of backup files.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Offline Backup > Backup Server Configurations**. The **Backup Server Configurations** page appears.



Backup Server Configurations

Backup Server IP Address: 10[redacted]16

Backup Server Monitoring Path: /apsara/backup/

Backup Retention Period: 9

4. Configure the backup server parameters. The following table describes the backup server parameters.

Parameter	Description
Backup Server IP Address	The IP address of the backup server. The backup server must meet the following requirements: ○ The backup server is an independent physical server. ○ The backup server is managed and controlled by Apsara Infrastructure Management Framework. ○ The network of the backup server is connected to other servers in Apsara Stack. ○ Apsara Distributed File System cannot be deployed on the server or on the disk where backup metadata is stored.
Backup Service Monitoring Path	The storage path of backup files on the backup server. The backup service detects new backup files by monitoring the specified folder on the backup server and determines whether the backup is successful by comparing the MD5 value of the backup file with that of the original file.
Backup Retention Period	The maximum time period in days that backup files are stored. Backup files whose retention periods exceed the specified time period are deleted.

5. Click **Save**.

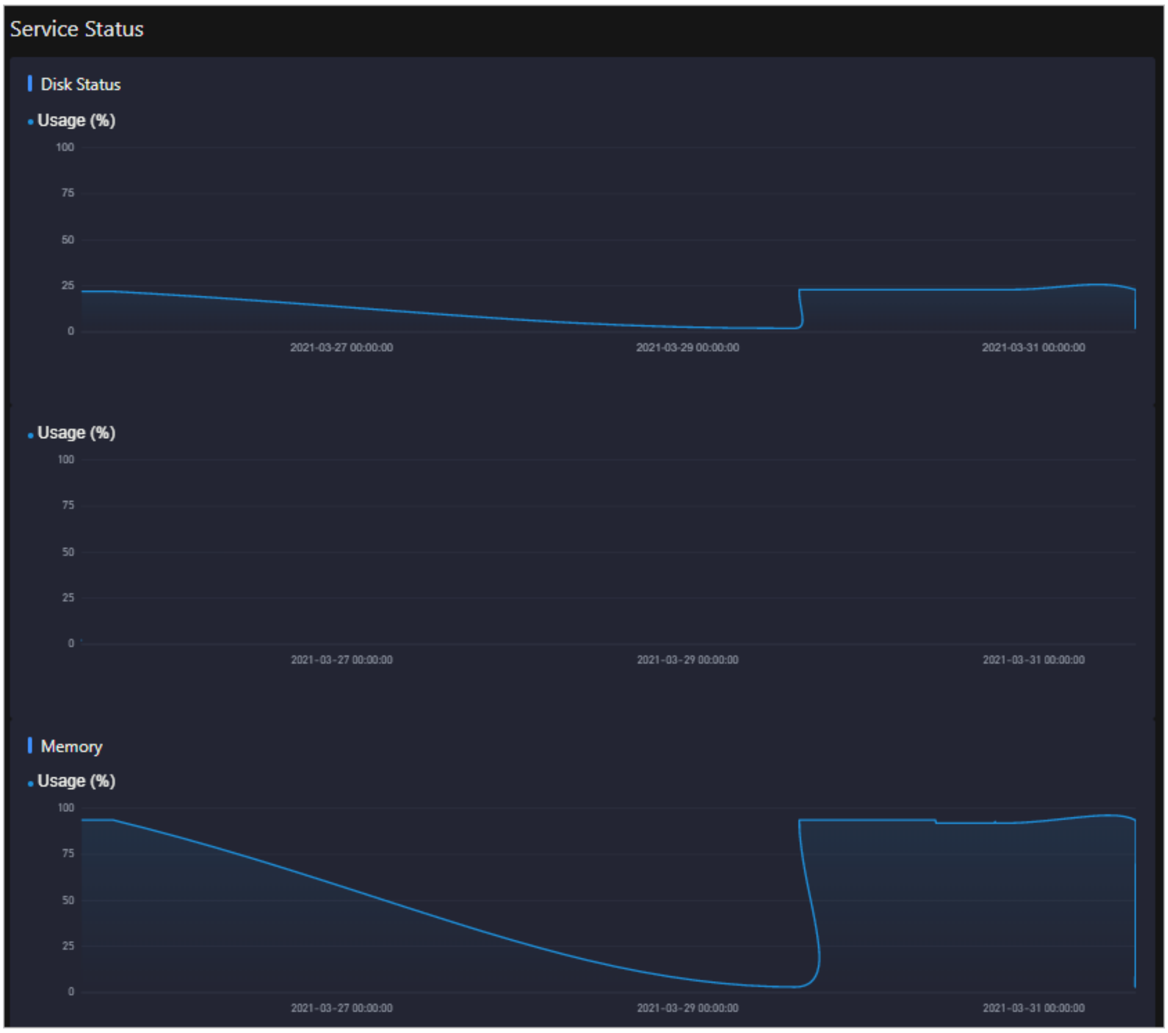
3.3.5. View the backup server status

You can view the memory and disk usage, as well as the CPU utilization of the current backup server before and after the backup.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.

3. In the left-side navigation pane, choose **Offline Backup** > **Service Status**.
4. On the **Service Status** page, view the memory and disk usage, as well as the CPU utilization of the current backup server.

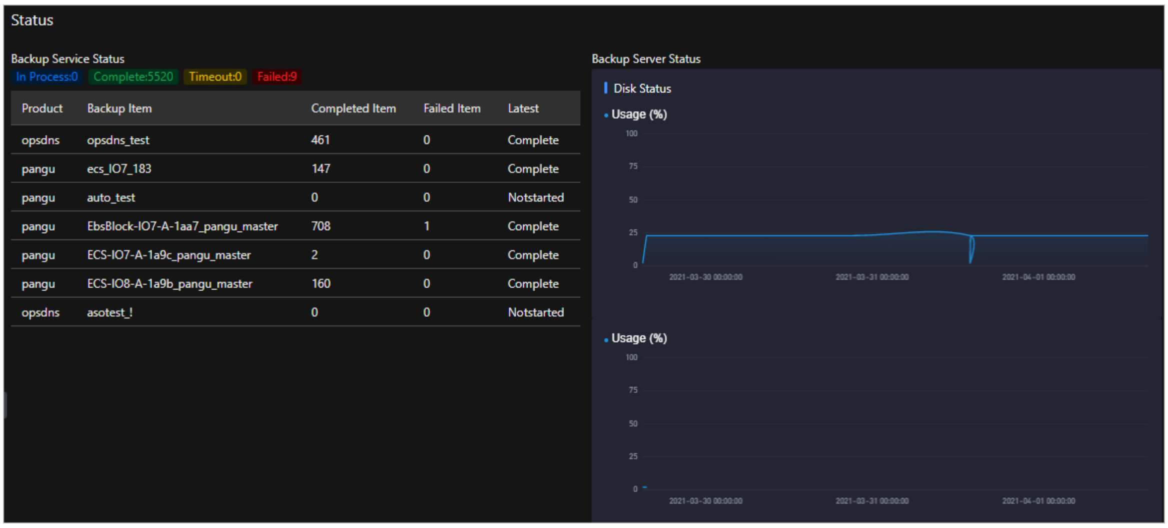


3.3.6. View the backup status

You can view the status of the current backup server and backup service, including the backup product, completed backup items, timeout and failed backup items.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Offline Backup** > **Status**.



Status

Backup Service Status

In Process:0 Complete:5520 Timeout:0 Failed:9

Product	Backup Item	Completed Item	Failed Item	Latest
opsdns	opsdns_test	461	0	Complete
pangu	ecs_IO7_183	147	0	Complete
pangu	auto_test	0	0	Notstarted
pangu	EbsBlock-IO7-A-1aa7_pangu_master	708	1	Complete
pangu	ECS-IO7-A-1a9c_pangu_master	2	0	Complete
pangu	ECS-IO8-A-1a9b_pangu_master	160	0	Complete
opsdns	asotest_!	0	0	Notstarted

4. On the **Status** page, view the current backup status.
   - View the number of backup items that are in the **In Process**, **Complete**, **Timeout**, and **Failed** state.
   - View the status of the latest backup item of the current service.

     The backup status includes **Not started**, **In transmission**, **Complete**, **Timeout**, and **Failed**.
   - On the right side of the page, view the status of the current backup server, including the memory and disk usage, as well as the CPU utilization.

3.3.7. Use cases

3.3.7.1. Offline backup of metadata

To guarantee the availability of cloud platforms, you must back up the pangu data of each product.

3.3.7.1.1. Preparations

This topic describes preparations to make before you perform backup operations.

Before the backup, take note of the following items:

- A buffer server is required as the backup server.

  If no buffer servers are available, select a physical server that has a large disk capacity and good network performance. Otherwise, the security of the backup data cannot be ensured.

  > **Note** Offline backup files cannot be stored on objects to be backed up. If no more physical servers are available and if disk capacity is insufficient in the on-site environment, the system is unable to perform offline backup. In this case, you must add physical servers or increase disk capacity before the offline backup.

- A transfer server is required to store one-time backup data and backup scripts of each product.

  No other requirements are needed for transfer servers.

- The network of the backup server must be connected with that of the Docker container where the offline backup service is located. This ensures that backup containers in the clusters of the Apsara

Uni-manager Operations Console can log on to the transfer server and backup server by using SSH key pairs, without the need to provide the username and password.

3.3.7.1.2. Collect the Apsara Distributed File System information of each product

The Products module allows you to collect the Apsara Distributed File System information of products to be backed up, which helps add the backup product information to the Apsara Uni-manager Operations Console.

Context

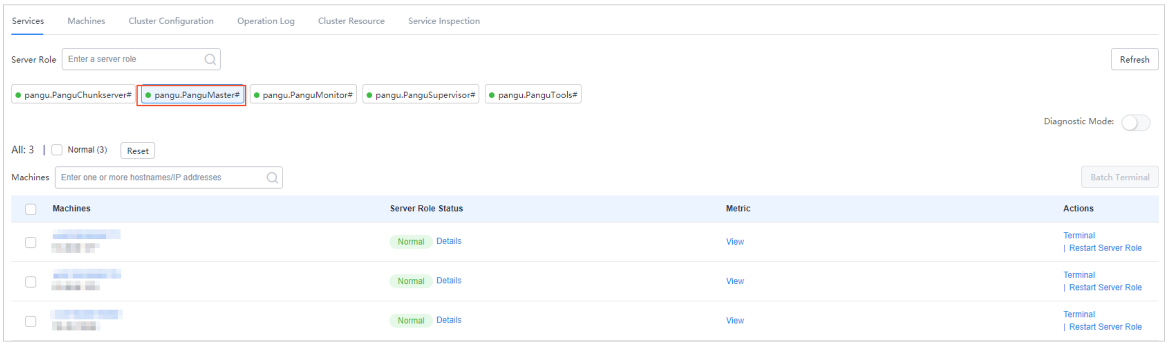
In this topic, product names are customized as oss, ecs, ads, and ots, and the information of these products are collected. The products for which you are about to collect Apsara Distributed File System information are subject to the on-site environment.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
   i. Log on to the Apsara Uni-manager Operations Console.
   ii. In the top navigation bar, click **O&M**.
   iii. In the left-side navigation pane, choose **Product Management > Products**.
   iv. In the **Apsara Stack O&M** section, choose **Basic O&M > Apsara Infrastructure Management Framework**.

> **Note** In this topic, operations are performed in the new Apsara Infrastructure Management Framework console.

2. In the left-side navigation pane, choose **Operations > Service Operations**.
3. Enter **pangu** in the **Service** search box to search for the Apsara Distributed File System service.
4. Click **Operations** in the **Actions** column corresponding to pangu to go to the service details page.
5. Click the **Clustes** tab.
6. Click the name of a cluster.
7. On the **Services** tab, click **pangu.PanguMaster#**.



□ Machines	Server Role Status	Metric	Actions
□ [redacted]	Normal Details	View	Terminal | Restart Server Role
□ [redacted]	Normal Details	View	Terminal | Restart Server Role
□ [redacted]	Normal Details	View	Terminal | Restart Server Role

8. View and record the IP addresses of Apsara Distributed File System master in the server list. Record one of the three IP addresses of **PanguMaster#**.

9. Repeat Steps 6 to 8 to view and record the Apsara Distributed File System information of each product. The recorded results are similar to those in the following table.

Cluster name	pangumaster IP	Product name
AdvanceOssCluster-A-xx	10.10.10.1	oss
ECS-IO7-A-xx	10.10.10.2	ecs
ads-A-xx	10.10.10.3	ads
otsv3_p-A-xx	10.10.10.4	ots

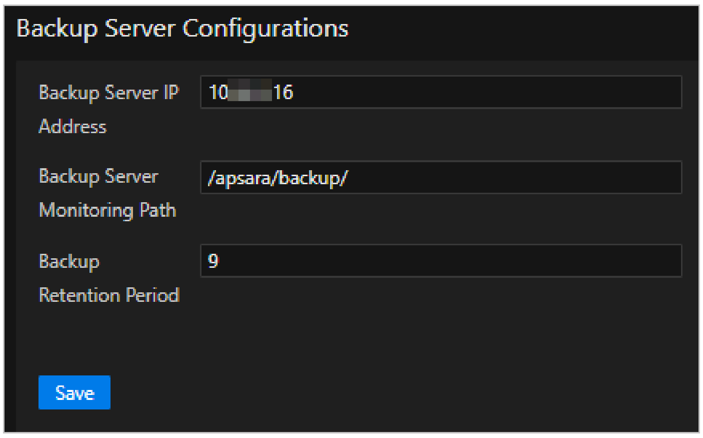
> **Note** You can customize the product name. Make sure that the product name is unique and recognizable.

3.3.7.1.3. Configure a backup server

The Backup Server Configurations module allows you to configure parameters related to a backup server.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Offline Backup > Backup Server Configurations**. The **Backup Service Configurations** page appears.



Backup Server Configurations

Backup Server IP Address: 10[redacted]16

Backup Server Monitoring Path: /apsara/backup/

Backup Retention Period: 9

4. Configure the backup server parameters. The following table describes the parameters.

Parameter	Description

Parameter	Description
Backup Server IP Address	The IP address of the server. The backup server must meet the following requirements: ○ The backup server is an independent physical server. ○ The backup server is managed and controlled by Apsara Infrastructure Management Framework. ○ The network of the backup server is connected to other servers in Apsara Stack. ○ Apsara Distributed File System cannot be deployed on the server or on the disk on which backup metadata is stored.
Backup Service Monitoring Path	The storage path of backup files on the backup server. The backup service detects new backup files by monitoring the specified folder on the backup server and determines whether the backup is successful by comparing the MD5 value of the backup file with that of the original file.
Backup Retention Period	The amount of time in days that stored backup files are retained. Backup files whose retention periods exceed the specified time period are deleted.

5. Click **Save**.

3.3.7.1.4. Add a backup product

The Product Management module allows you to add backup product information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Offline Backup > Product Management**.
4. Click **Add Product**.
5. In the **Add Product** dialog box, add information of a product as described in the following table and click **OK**.

Parameter	Description
Product	The product name. Set this parameter to pangu to back up the Apsara Distributed File System data.

Parameter	Description
Backup Item	The name of the backup item. Set this parameter based on the product information described in the Collect the Apsara Distributed File System information of each product topic in the *product name*_pangu format. Example: oss_pangu.
Script	The name of the backup script. Example: metadata_backup.py.
Retry Times	The number of times to retry after an error occurs. Typically, set this parameter to 3.

6. Repeat the preceding steps to add all the backup items.

Result

You can view the added product on the **Backup Configurations** page.

3.3.7.1.5. Configure backup parameters

After you add backup items, you must configure the backup in the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Offline Backup > Backup Configurations**.
4. Click a product backup item on the left and then configure the parameters on the right.

Parameter	Description
Product Cluster IP Address	The IP address of the actual transfer server.
Backup File Folder	A folder on the transfer server. You are required only to enter a folder path in the field without manually creating a folder to store backup files. Example: /apsarapangu/disk8/pangu_master_bak/*product name*_pangu/bak
Script Execution Folder	A folder on the transfer server. You are required only to enter a folder path in the field without manually creating a folder to store backup files. Example: /apsarapangu/disk8/pangu_master_bak/*product name*_pangu/bin

Parameter	Description
Script Parameters	The execution parameters for the script. You must enter the value in the `--ip=xxx.xxx.xxx.xxx` format, in which the IP address is one of the IP addresses of the pangu master described in the Collect the Apsara Distributed File System information of each product topic.
Backup Schedule	The execution period of recurring executions. In this example, a value of 1 is entered to specify that the backup is performed only once.
Backup Schedule Unit	The unit of the execution period. Valid values: **Day**, **Hour**, and **Minute**. In this example, **Hour** is selected to specify that the backup is performed by hour.
Timeout Period	The timeout period, in seconds. In this example, set the value to **3600**.

5. Click **Modify** to complete the configurations and trigger the backup.
6. Perform the preceding steps to configure all the product backup items.

3.3.7.1.6. View the backup details

After you configure backup items, you can check whether the backup items function normally in the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Offline Backup** > **Backup Details**.
4. On the **Backup Details** page, specify the product and backup item, select the start date and end date, and then click **Search**.

   If the status of a backup item is **Complete**, the backup item functions normally.

   > Note When a backup task is complete, you must check whether the MD5 values of the offline backup service and the backup server are consistent with each other. If yes, the backup was successful.

3.4. Log clearance

The Log Clearance module allows you to clean up logs from specified log files in the specified containers (Docker) or physical machines (virtual machines or bare metal machines) in the system.

3.4.1. Import container or server log cleanup rules

If you have configured log cleanup rules on your computer, you can batch import multiple cleanup rules for containers or physical servers.

Context

Before you import cleanup rules, take note of the following items:

- Imported rules are added incrementally.
- You must check the values of Product, Service, ServerRole, SrcPath, MatchFile, Threshold, and Method to determine whether a cleanup rule already exists. If all values in the environment are the same as the values specified in the rule to be imported, the rule already exists. If a rule already exists, it is deduplicated and is not imported.
- Before you import rules, you must contact technical support and request the encryption sequence.
- After you import rules, special characters such as spaces, carriage returns, line feeds, and tabs in the rules are automatically deleted.
- The maximum disk usage range specified by a rule is [0%,100%], and the value before the percent sign (%) must be an integer. Otherwise, the rule is automatically filtered out when you import it. We recommend that you set the maximum disk usage to 75%.
- Make sure that cleanup methods specified by rules are tested and can be executed normally. Otherwise, exceptions may occur when you use the methods to clean up logs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance > Rules**.
4. Click the **Container** or **Servers** tab.
5. Click **Import**.
6. Select the XLS or XLSX files that you want to import and click **Open** to import multiple log cleanup rules. After you import rules, corresponding execution plans are asynchronously generated.

3.4.2. Export container or physical server log cleanup rules

You can batch export multiple container or physical server log cleanup rules.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance > Rules**.
4. Click the **Containers** or **Servers** tab.
5. Perform the following operations to export the log cleanup rules of containers or physical servers:
   - Click **Export** to export all cleanup rules.
   - In the upper part of the page, select a product, service, and service role, and click **Search**. In the search result, select the cleanup rules that you want to export and click **Export**.

Note By default, the **Product**, **Service**, and **Service Role** parameters on the tab do not have any options in their drop-down lists. When you specify these parameters for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down list.

3.4.3. Modify a log cleanup rule

You can modify log cleanup rules to suit your business needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance** > **Rules**.
4. Click the **Containers** or **Servers** tab.
5. (Optional)In the upper part of the tab, select the product, service, and service role, and then click **Search** to query the cleanup rules that meet the search conditions.

   Note By default, no values are available for **Product**, **Service**, and **Service Role** on the tab. When you specify the product, service, and service role for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system loads all available data in the list.

6. Find the cleanup rule that you want to modify and click **Modify** in the **Actions** column.
7. In the panel that appears, modify the maximum disk usage and specify whether to automatically clean up logs that match the cleanup rule.

   Note The maximum disk usage range is [0%,100%], and the value before the percent sign (%) must be an integer We recommend that you set the maximum disk usage to 75%.

8. Click **OK**.

3.4.4. Delete a log cleanup rule

You can delete log cleanup rules that are no longer needed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance** > **Rules**.
4. Click the **Containers** or **Servers** tab.
5. (Optional)In the upper part of the tab, select the product, service, and service role, and then click **Search** to query cleanup rules that meet the search conditions.

> Note By default, the **Product**, **Service**, and **Service Role** parameters on the tab do not have any options in their drop-down lists. When you specify these parameters for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system shows all available data in the drop-down list.

6. Find the cleanup rule that you want to delete and click **Delete** in the **Actions** column.
7. In the message that appears, click **OK**.

> Note The execution plan corresponding to a cleanup rule is not deleted when you delete the rule. At 02:00 every day, the system cleans up existing execution plans and generates new execution plans based on the current cleanup rules.

3.4.5. Obtain the usage information of containers or physical servers

The Log Clearance module allows you to query the disk usage information of containers or physical servers.

Method 1

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance > Plans**.
4. Click the **Containers** or **Servers** tab.
5. Perform the following operations to obtain the disk usage information of a container or physical server:
    - In the upper part of the page, select a product, service, and service role, and click **Search**. In the search results, find the container or physical server in which you want to query the disk usage information and click **Obtain Watermark** in the **Actions** column to obtain the disk usage information of a single container or physical server.

      > Note By default, the **Product**, **Service**, and **Service Role** parameters on the tab do not have any options in their drop-down lists. When you specify these parameters for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down list.

    - Select multiple containers or physical servers and click **Obtain Watermarks** to obtain the disk usage information of multiple containers or physical servers.

      > Note The operation for obtaining the usage information is asynchronous. You must refresh the page to view the results. If the current usage of the disk is higher than the specified maximum disk usage, the value is displayed in red.

Method 2

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance** > **Rules**.
4. Click the **Containers** or **Servers** tab.
5. (Optional)In the upper part of the page, select a product, service, and service role, and click **Search**.

   > ? **Note** By default, the **Product**, **Service**, and **Service Role** parameters on the tab do not have any options in their drop-down lists. When you specify these parameters for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down list.

6. In the search result, select the cleanup rule of the container or physical server in which you want to obtain the disk usage information and click **Execution Plan** in the **Actions** column. The **Execution Plan** page appears.
7. Perform the following operations to obtain the disk usage information of a container or physical server:
   - Find the container or physical server for which you want to obtain disk usage information and click **Obtain Watermark** in the **Actions** column.
   - Select multiple containers or physical servers and click **Obtain Watermarks** to obtain the disk usage information of multiple containers or physical servers.

     > ? **Note** The operation for obtaining the usage information is asynchronous. You must refresh the page to view the results. If the current usage of the disk is higher than the specified maximum disk usage, the value is displayed in red.

3.4.6. Clean up the logs of containers or physical servers

You can clean up the logs of containers or physical servers in a timely manner based on disk usage information of the containers or physical servers.

Method 1

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance** > **Plans**.
4. Click the **Containers** or **Servers** tab.
5. Perform the following operations to clean up the logs of containers or physical servers:
   - In the upper part of the page, select a product, service, and service role, and click **Search**. In the search results, find the container or physical server for which you want to clean up logs and click **Clear** in the **Actions** column.

> Note By default, the **Product**, **Service**, and **Service Role** parameters on the tab do not have any options in their drop-down lists. When you specify these parameters for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down list.

- Select multiple containers or physical servers and click **Clear Logs** in the upper part of the tab to clean up the log information of multiple containers or physical servers at a time.

> Note The log cleanup operation is asynchronous. You must view the log cleanup results on the **Records** page.

Method 2

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance** > **Rules**.
4. Click the **Containers** or **Servers** tab.
5. (Optional)In the upper part of the page, select a product, service, and service role, and click **Search**.

   > Note By default, the **Product**, **Service**, and **Service Role** parameters on the tab do not have any options in their drop-down lists. When you specify these parameters for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down list.

6. In the search result, find the cleanup rule of the container or physical servers for which you want to clean up logs and click **Execution Plans** in the **Actions** column. The **Plans** page appears.
7. Perform the following operations to clean up logs of containers or physical servers:
   - Find the container or physical server for which you want to clean up logs and click **Clear** in the **Actions** column to clean up the logs of a single container or physical server.
   - Select multiple containers or physical servers and click **Clear Records** in the upper part of the tab to clean up the logs of multiple containers or physical servers at a time.

   > Note The log cleanup operation is asynchronous, and you must view the log cleanup results on the **Records** page.

3.4.7. Configure automatic cleanups for container or physical server logs

You can configure automatic cleanups for container or physical server logs that meet the specified cleanup rules.

Context

The system deletes the existing execution plans at 02:00 every day and generates corresponding execution plans based on the current cleanup rules. If you turn on **Automatic Deletion** or enable automatic cleanup, the system cleans up the container or physical server logs that meet the cleanup rules based on execution plans at 02:30 every day.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance > Rules**.
4. Click the **Containers** or **Servers** tab.
5. Perform the following operations to configure automatic cleanups for container or physical server logs that meet the specified cleanup rules:
    - In the upper part of the page, select a product, service, and service role, and then click **Search**. In the search result, find the cleanup rule for which you want to set automatic cleanups and turn on **Automatic Deletion**. The system cleans up the container or physical server logs that meet the cleanup rule.

      > ⓘ **Note** By default, the **Product**, **Service**, and **Service Role** parameters on the tab do not have any options in their drop-down lists. When you specify these parameters for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down list.

      If you want to disable the automatic cleanup feature, you can turn off **Automatic Deletion**.

    - Select multiple cleanup rules and click **Turn on Automatic Cleanup**. The system cleans up the container or physical server logs that meet the selected cleanup rules.

      To disable the automatic cleanup feature, click **Turn off Automatic Cleanup**.

3.4.8. View cleanup records

After you clean up logs, you can view detailed cleanup records.

Context

When you perform operations on the **Records** page, take note of the following items:

- Each time you perform a log cleanup operation, the values of Execution Times, Server Roles, and Servers are increased by one.
- Cleared Log Files shows the number of log files that match all the available rules and can be cleaned up, rather than the number of log files that have been cleaned up.
- Cleared Space shows the accumulated total space that are available after you clean up logs.

Method 1

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance > Records**.
4. (Optional)In the upper part of the page, select a product, service, and service role, and click

Search.

> Note By default, the **Product**, **Service**, and **Service Role** parameters on the tab do not have any options in their drop-down lists. When you specify these parameters for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down list.

5. Find the cleanup record that you want to view, and click **View Details** in the **Details** column to view the detailed cleanup information.

Method 2

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Log Clearance > Plans**.
4. Click the **Containers** or **Servers** tab.
5. (Optional)In the upper part of the page, select a product, service, and service role, and click **Search**.

   > Note By default, the **Product**, **Service**, and **Service Role** parameters on the tab do not have any options in their drop-down lists. When you specify these parameters for the first time, you must enter the product, service, and service role in the list and select the corresponding search result. In subsequent queries, the system shows all available options in the drop-down list.

6. In the search result, find the execution plan for which you want to view the cleanup records and click **Clear Records** in the **Actions** column. The **Records** page appears.
7. Find the cleanup record that you want to view and click **View Details** in the **Details** column to view the detailed cleanup information.

3.5. System settings

The System Settings module allows you to manage departments, roles, and users involved in the Apsara Uni-manager Operations Console in a centralized manner. This makes it easy to grant different resource access permissions to different users. The System Settings module is a core module in managing permissions. It integrates the features such as department management, role management, logon policy management, user management, and password management.

3.5.1. User management

You can create users and assign different user roles to meet different requirements for system access control as an administrator.

Prerequisites

Before you create a user, make sure that the following requirements are met:

- A department is created. For more information, see Department management.
- A custom role is created based on your needs. For more information, see Role management.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > User Management**.

   The **Users** tab appears.
4. On the **Users** tab, perform the following operations:
   - Query users

     > **Note** To search for users in the Apsara Uni-manager Operations Console, you must have the security officer role or system administrator role.

     In the upper part of the page, set **Username**, **Role**, and **Department**, and then click **Search** to view information about the user in the list.

     (Optional) you can click **Reset** to clear the last search conditions.
   - Add a user

     > **Note** To add a user in the Apsara Uni-manager Operations Console, you must have the security officer role.

     Click **Add** in the upper part of the tab. In the **Add User** dialog box, set **User Name** and **Password** and click **OK**.

     The added user is displayed in the user list. The value in the **Primary Key Value** column corresponding to the added user is used to call API operations of applications. When you want to call applications in the Apsara Uni-manager Operations Console for other applications, you must use the primary key value for authentication.
   - Modify a user

     > **Note** To modify a user in the Apsara Uni-manager Operations Console, you must have the security officer role.

     In the user list, find the user that you want to modify and click **Modify** in the **Actions** column. In the **Modify User** dialog box, modify the parameters and click **OK**.
   - Delete a user

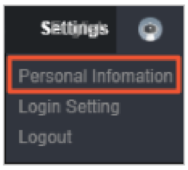
     In the user list, find the user that you want to delete and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

     > **Note** Deleted users are displayed on the **Locked Instances** tab. To restore a deleted user, click the **Locked Instances** tab. Find the user to be restored and click **Recover** in the **Actions** column. In the message that appears, click **OK**.
   - Bind a logon policy

     In the user list, find the user to which you want to bind a logon policy and click **Bind Logon Policy** in the upper part of the page. In the **Bind Logon Policy** dialog box, select the logon policy to bind and click **OK**.

- Query personal information of the current user

  Move the pointer over the profile picture in the upper-right corner of the page and click **Personal Information**. On the **User Profile** page, view the personal information of the current user, such as the **Username** and **Department**.

  On the **User Profile** page, you can also change the password that the current user uses to log on to the Apsara Uni-manager Operations Console. For more information about how to change the logon password, see Change the logon password.

- Configure logon settings

  Move the pointer over the profile picture in the upper-right corner of the page and click **Login Setting**. On the **Logon Settings** page, you can modify the logon timeout period, whether to allow multi-terminal logon, maximum allowed password retries, logon policy, and validity period of the current account. For more information about how to modify logon settings, see Modify logon settings.

3.5.2. User group management

You can add multiple users to a user group and add the same roles to them as an administrator for centralized management.

Create a user group

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > User Group Management**.
4. In the upper part of the page, click **Add**.
5. In the **Add User Group** dialog box, enter a user group name, select a department, and then click **OK**.

Modify the name of a user group

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > User Group Management**.
4. (Optional)Select a department name, enter a user group name and user name, and then click **Search**. You can also click **Advanced**, select a department name and role name, enter a user group name and user name, and then click **Search**. If you have defined filter conditions, you can click **Reset** to remove the conditions with one click.
5. In the user group list, find the user group that you want to modify and click **Edit User Group** in the **Actions** column.
6. In the dialog box that appears, modify the user group name.
7. Click **OK**.

Manage users in a user group

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > User Group Management**.
4. (Optional)Select a department name, enter a user group name and user name, and then click **Search**. You can also click **Advanced**, select a department name and role name, enter a user group name and user name, and then click **Search**. If you have defined filter conditions, you can click **Reset** to remove the conditions with one click.
5. In the user group list, find the user group for which you want to manage users and click **Manage Users** in the **Actions** column.
6. In the dialog box that appears, you can add users to or delete users from the user group.
    - Click **Add**. In the **Add** dialog box, select one or more users and click **OK**.
    - Click the 🗑 icon to delete the user.
7. Click **OK**.

    The added users are displayed in the **Users** column corresponding to the user group.

    The deleted users are no longer displayed in the **Users** column corresponding to the user group.

Add a role to a user group

You can add only one role to a user group.

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > User Group Management**.
4. (Optional)Select a department name, enter a user group name and user name, and then click **Search**. You can also click **Advanced**, select a department name and role name, enter a user group name and user name, and then click **Search**. If you have defined filter conditions, you can click **Reset** to remove the conditions with one click.
5. In the user group list, find the user group to which you want to add a role and click **Add Role** in the **Actions** column.
6. Select a role from the **Role** drop-down list.
7. Click **OK**.

    The added role is displayed in the **Role** column corresponding to the user group. All users in the user group are granted the permissions of this role.

Delete a role

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > User Group Management**.
4. (Optional)Select a department name, enter a user group name and user name, and then click **Search**. You can also click **Advanced**, select a department name and role name, enter a user group name and user name, and then click **Search**. If you have defined filter conditions, you can click **Set** to remove the conditions with one click.

5. In the user group list, find the user group from which you want to delete a role and click **Delete Role** in the **Actions** column.
6. In the message that appears, click **OK**. The deleted role is no longer displayed in the **Role** column corresponding to the user group. The users in the user group do not have the permissions of the role.

Delete a user group

> **Notice** Before you delete a user group, make sure that no users or roles are bound to the user group.

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > User Group Management**.
4. (Optional)Select a department name, enter a user group name and user name, and then click **Search**. You can also click **Advanced**, select a department name and role name, enter a user group name and user name, and then click **Search**. If you have defined filter conditions, you can click **Reset** to remove the conditions with one click.
5. In the user group list, find the user group that you want to delete and click **Delete User Group** in the **Actions** column.
6. In the message that appears, click **OK**.

3.5.3. Role management

You can customize roles in the Apsara Uni-manager Operations Console to achieve more flexible and efficient permission control.

Context

A role is a collection of access permissions. You can assign different roles to different users to meet requirements for system access control. Roles are classified into basic and custom roles. Basic roles, also known as atomic roles, are preset by the Operation Access Manager (OAM) system. You cannot modify or delete these roles. Custom roles can be modified and deleted.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Role Management**.
4. On the **Role Management** page, perform the following operations:
   - Query roles

     > **Note** To query roles in the Apsara Uni-manager Operations Console, you must have the ASO security officer role or system administrator role.

     In the upper-left corner of the page, enter a role name in the **Role** field and click **Search** to view the role information in the list.

- Add a role

  > Note Only users that have security officer roles of the Apsara Uni-manager Operations Console can add a role in the console.

  Click **Add** in the upper part of the tab. In the **Add Role** dialog box, set **Role Name**, **Role Description**, and **Base Role**, and then click **OK**.

- Modify a role

  > Note Only users that have security officer roles of the Apsara Uni-manager Operations Console can modify a role in the console.

  Find the role to be modified in the role list and click **Edit** in the **Actions** column. In the **Edit Role** dialog box, modify **Role Name** and **Role Description**, select a basic role, and then set menu permissions. Click **OK**.

- Delete a role

  > Notice Before you delete a role, make sure that the role is not bound to any users. Otherwise, the role cannot be deleted.

  Find the role that you want to delete in the role list and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

3.5.4. Menu management

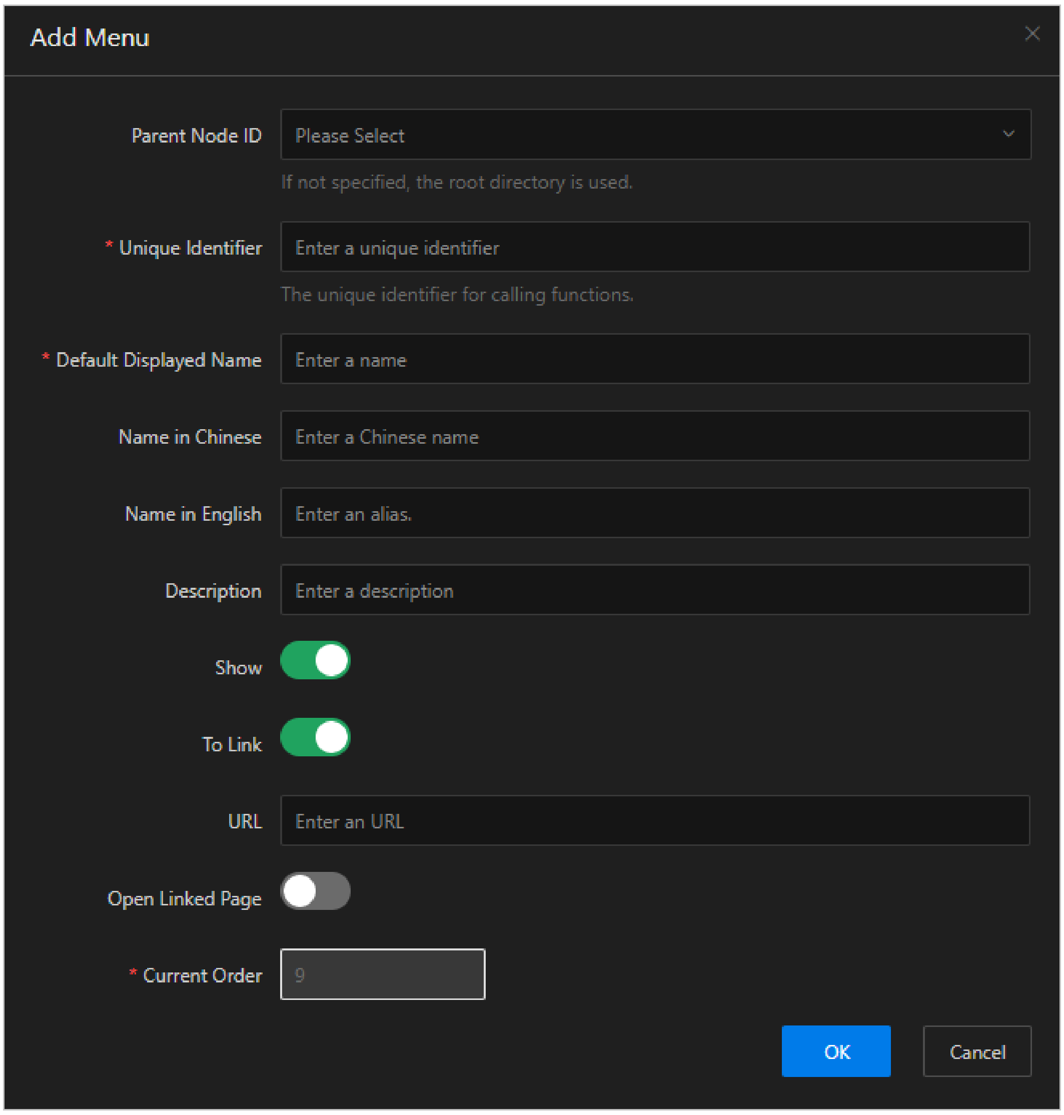
The Menu Settings module allows you to add, hide, modify, or delete a menu based on your business needs.

3.5.4.1. Add a level-1 menu

This topic describes how to add a level-1 menu.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Menu Settings**.
4. In the upper part of the page, click **Add Menu Data**.
5. In the Add Level-1 Menu panel, configure the menu parameters.



Add Menu

Parent Node ID: Please Select
If not specified, the root directory is used.

* Unique Identifier: Enter a unique identifier
The unique identifier for calling functions.

* Default Displayed Name: Enter a name

Name in Chinese: Enter a Chinese name

Name in English: Enter an alias.

Description: Enter a description

Show: ●

To Link: ●

URL: Enter an URL

Open Linked Page: ○

* Current Order: 9

The following table describes the parameters.

Parameter	Description
Parent Node ID	The parent menu. You do not need to specify this parameter when you add a level-1 menu.
Unique Identifier	The unique identifier used to call functions. It must be made up of only letters and can be 5 to 20 characters in length.
Default Displayed Name	The default display name of the menu.
Name in Chinese	The menu name in Chinese. In the Chinese language environment, if the Chinese name of the menu is specified, the default display name of the menu is the specified Chinese name.
Name in English	The menu name in English. In the English language environment, if the English name of the menu is specified, the default display name of the menu is the specified English name.

Parameter	Description
Description	The description of the menu.
Show	Specifies whether to show the menu after it is added. You can turn on or off **Show**. By default, the switch is on.
To Link	Specifies whether to go to another page when you click the menu. You can turn on or off **To Link**. By default, the switch is off.
URL	This parameter appears only when **To Link** is turned on. Set this parameter to the URL to jump to when you click the menu. ○ If the URL of a page within the current system is used, enter the absolute path or a relative path of the page. Example: /aso/aso-alarm/dashboard. ○ If the URL of a third-party system is used, enter the absolute path of the page. Example: http://example.com/TaskManageTool/#/taskView.
Open Linked Page	Specifies whether to open a new page for the URL to jump to after you click the menu. You can turn on or off the **Open Linked Page** switch. By default, the switch is turned off.
Current Order	The order of the menu among all level-1 menus. You cannot configure the order in the panel. You can modify the configuration on the **Menu Settings** page after you create the menu.

6. Click **OK**.

Result

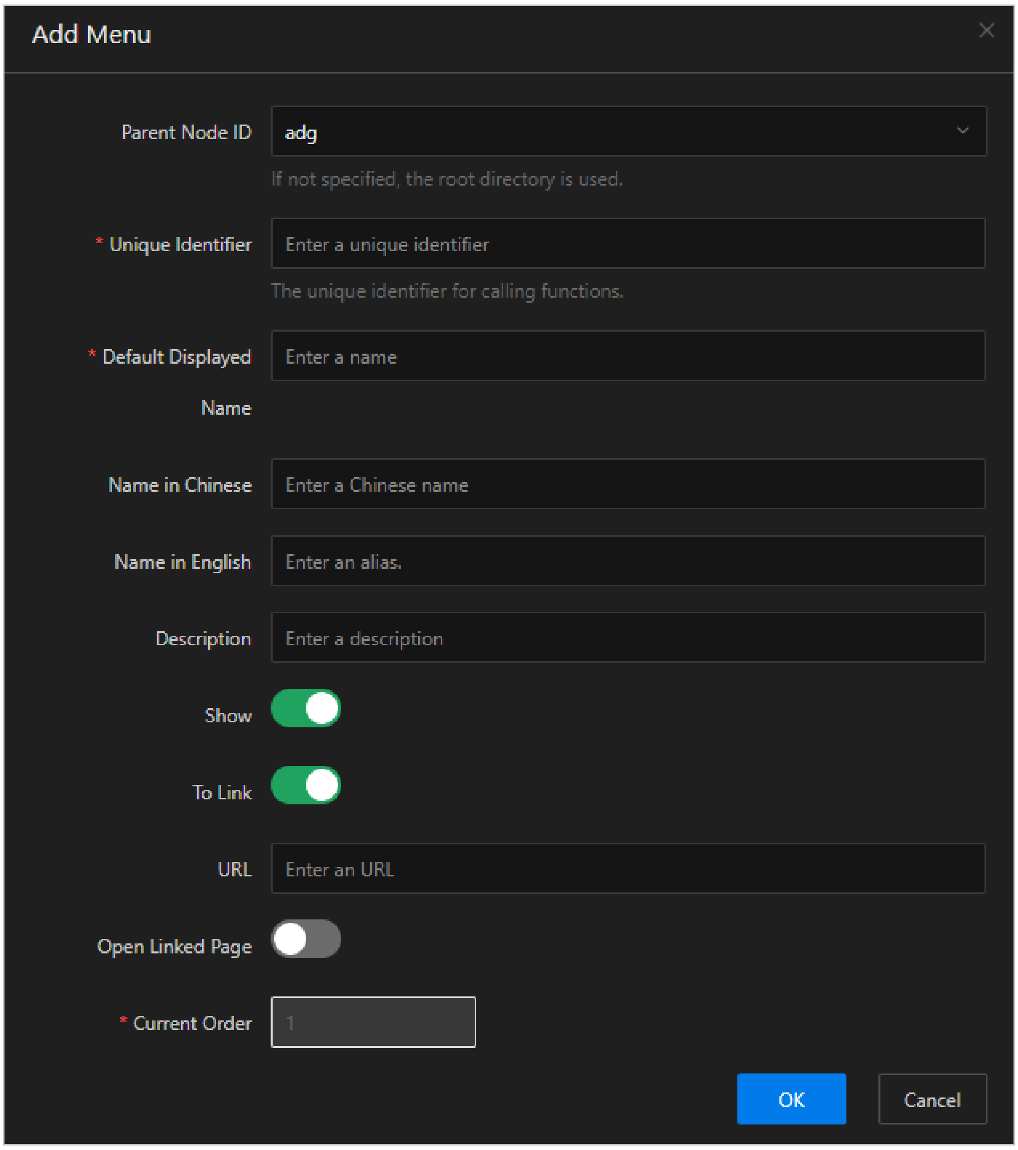
Then, you can view the added level-1 menu in the menu list and the top navigation bar.

3.5.4.2. Add a submenu

This topic describes how to add a submenu.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Settings > Menu Settings**.
4. Add a submenu.
   i. Find the menu to which you want to add a submenu and click **Add Submenu** in the **Actions** column.
   ii. In the Add Submenu panel, configure the submenu parameters.



Add Menu

Parent Node ID: adg

If not specified, the root directory is used.

* Unique Identifier: Enter a unique identifier

The unique identifier for calling functions.

* Default Displayed Name: Enter a name

Name in Chinese: Enter a Chinese name

Name in English: Enter an alias.

Description: Enter a description

Show: on

To Link: on

URL: Enter an URL

Open Linked Page: off

* Current Order: 1

The following table describes the parameters.

Parameter	Description
Parent Node ID	The parent menu to which the submenu belongs.
Unique Identifier	The unique identifier used to call functions. It can consist only of letters and can be 5 to 20 characters in length.
Default Displayed Name	The default display name of the menu.
Name in Chinese	The menu name in Chinese. In the Chinese language environment, if the Chinese name of the menu is specified, the default display name of the menu is the specified Chinese name.
Name in English	The menu name in English. In the English language environment, if the English name of the menu is specified, the default display name of the menu is the specified English name.

Parameter	Description
Description	The description of the menu.
Show	Specifies whether to show the menu after it is added. You can turn on or off **Show**. By default, the switch is on.
To Link	Specifies whether to go to another page when you click the menu. You can turn on or off **To Link**. By default, the switch is off.
URL	This parameter appears only when **To Link** is turned on. Set this parameter to the URL to jump to when you click the menu. ■ If the URL of a page within the current system is used, enter the absolute path or a relative path of the page. Example: /aso/aso-alarm/dashboard. ■ If the URL of a third-party system is used, enter the absolute path of the page. Example: http://example.com/TaskManageTool/#/taskView.
Open Linked Page	Specifies whether to open a new page for the URL to jump to after you click the menu. You can turn on or off **Open Linked Page**. By default, the switch is off.
Current Order	The order of the submenu under the selected parent menu. You cannot configure the order in the panel. You can modify the configuration on the **Menu Settings** page after you create the menu.

iii. Click **OK**.
After you add a submenu, you can view it under the corresponding parent menu in the menu list and in the left-side navigation pane.

> Note We recommend that you create a menu hierarchy of no more than five levels.

3.5.4.3. Hide a menu

This topic describes how to hide a menu.

Prerequisites

> Notice Only custom menus and submenus can be hidden. After a menu or submenu is hidden, submenus under it are also hidden.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Menu Settings**.

4. In the menu list, find the menu or submenu that you want to hide and click **Modify** in the **Actions** column.
5. In the Modify Menu panel, turn off **Show** and click **OK**.

3.5.4.4. Modify a menu

After you add a menu or submenu, you can modify its configuration and sorting.

Prerequisites

> **Notice** Only custom menus and submenus can be modified. Built-in menus and submenus only support sorting.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Menu Settings**.
4. In the menu list, find the menu or submenu that you want to modify and click **Modify** in the **Actions** column.
5. In the Modify Menu panel, modify the parameters and click **OK**.
6. In the **Actions** column, click **Move Up** or **Move Down** to change the order of the menu.

3.5.4.5. Delete a menu

This topic describes how to delete a menu or submenu that is no longer needed.

Prerequisites

> **Notice** Only custom menus and submenus can be deleted.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Menu Settings**.
4. In the menu list, find the menu or submenu that you want to delete and click **Delete** in the **Actions** column.
5. In the message that appears, click **OK**.

3.5.5. Two-factor authentication

To make user logon more secure, you can configure two-factor authentication for users.

Context

The Apsara Uni-manager Operations Console supports only Google two-factor authentication.

This authentication method uses a password and mobile app to provide a two-layer protection for accounts. You can obtain the logon key after you configure users in the Apsara Uni-manager Operations Console, and then enter the key in the Google Authenticator app on your mobile phone. The app dynamically generates a verification code for logon based on the time and key.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Two-factor Authentication**.
4. On the Two Factor Authentication page, perform the following operations:
    - Google two-factor authentication
        a. Set **Current Authentication Method** to **Google Two-Factor Authentication**.
        b. In the upper-right corner of the page, click **Add User**. In the Add User dialog box, enter a username and click OK. The added user is displayed in the user list.
        c. Find the username for which you want to enable Google two-factor authentication and click **Create Key** in the **Actions** column. When the **Added** message appears, the **Show Key** button appears in the **Actions** column. Click **Show Key**, and the key is displayed in plaintext in the Key column.
        d. Enter the key in the Google Authenticator app on your mobile phone. The app dynamically generates a verification code for logon based on the time and key. While two-factor authentication is enabled, you are required to enter the verification code on your app whenever you log on to the system.

        > **Note** The Google Authenticator app and server generate the verification code by using public algorithms and based on the time and key, and can work offline without connecting to the Internet or Google server. Therefore, you must keep your key confidential.

        e. To disable two-factor authentication, click **Delete Key** in the **Actions** column.
    - No authentication

        Set **Current Authentication Method** to **No Authentication**. Two-factor authentication is then disabled and all two-factor authentication methods become invalid.

3.5.6. Department management

The Department Management module allows administrators to create, modify, delete, and search for departments, as well as create users or user groups for departments.

Context

After the Apsara Uni-manager Operations Console is deployed, a root organization is automatically generated. You can create other departments under the root department.

Departments are displayed in a hierarchy, and you can create sub-departments under each level of departments. Up to five levels of departments can be created.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Department Management**. On the **Department Management** page, you can view the tree structure of all created departments and the user information under each department.
4. (Optional)In the upper-left corner of the page, enter a department name in the search box and click the search icon to find the department on which you want to perform operations.
5. Perform the following operations:
   - Add a department

     In the left catalog tree, select the department to which you want to add other sub-departments. Click the ▨ icon in the upper part of the page and select **Add Department**. In the **Add Department** dialog box, set **Department Name**, **Department Leader**, and **Department Role**, and then click **OK**. Then, you can view the created department in the left catalog tree.

     > **Note** When you add a department, you can select one or more department administrators.

   - Modify a department

     In the left catalog tree, select the department that you want to modify. Click the ▨ icon in the upper part of the page and select **Modify Department**. In the **Modify Department** dialog box, set **Department Name**, **Department Leader**, and **Department Role**, and then click **OK**.

   - Delete a department

     > **Notice** Before you delete a department, make sure that no users exist in the department. Otherwise, the department cannot be deleted.

     In the left catalog tree, select the department that you want to delete. Click the ▨ icon in the upper part of the page and select **Delete Department**. In the message that appears, click **OK**.

   - Add a user to a department

     In the left catalog tree, select the department to which you want to add a user. In the **Users** section on the right, click **Create User**. In the **Add User** dialog box, set **Username**, **Password**, and **Confirm Password**. Click **OK**.

     Then, you can choose **System Settings > User Management** to view the added user information on the **Users** tab.

   - Add a user group to a department

     In the left catalog tree, select the department to which you want to add a user group. In the **User Group** section on the right, click **Create User Group**. In the **Create User Group** dialog box, enter a user group name and click **OK**.

     Then, you can choose **System Settings > User Group Management** to view the added user group information .

3.5.7. Region management

In multi-region scenarios, the system administrator can bind a department to a region. After you bind a department to a region, users in the department can manage and view resources in the region.

Context

In multi-region scenarios, a region is managed by its own administrator. After administrators log on to the Apsara Uni-manager Operations Console, each administrator can manage only resources in the region that they are authorized to manage.

Relationship between departments and regions:

- A department can be bound to multiple regions.
- A region can be bound to multiple departments.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Region Management**.
4. (Optional)In the upper-left corner of the page, enter a department name in the search box and click the search icon to find the department that you want to bind.
5. In the left catalog tree, click a department and select one or more regions in the **Regions** list on the right.
6. Click **Update Association**.

3.5.8. Operating system logs

The Operating System Logs module allows you to collect statistics on the number of logs and identify events related to the operating system.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Operating System Logs**.
4. On the **Operating System Logs** page, select **Time** and set **Range** by specifying IP, HostName, or MachineGroup. Select the **Search by Keyword** check box, enter **Keyword**, and then click **Search**. View the number of logs, the number of events, and the logs generated around the time point when the event occurred. Specify **EventType**, **DataSource**, and **LogLevel** to further filter information. The default value of each parameter is **Total**.

Parameter	Description
EventType	The exception category, which can be kernel, security, or system.
DataSource	The system application from which logs are generated.
LogLevel	The log error level, which can be debug, info, notice, warning, err, or crit.

5. In the section below the graphs, click the + icon and select an event. Click the > icon before the

event to show the detailed log information around the time point when the event occurred. Click **Export** to export the full log information within the time range.

3.5.9. Operation logs

You can view logs to view the resource usage and running status of all function modules on the platform.

Context

The Operation Logs page allows you to view all the records of backend API calls, including audit operations. The auditor can filter logs by username and time, view call details, and export selected logs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Operation Logs**.
4. On the **Log Management** page, perform the following operations:
    - Query logs

      In the upper part of the page, enter **User Name** and select a **Time Period**. Click **Search** to view related logs in the list below.
    - Delete logs

      Select the logs that you want to delete and click **Delete**. In the message that appears, click **OK**.
    - Export logs

      Select the logs that you want to export and click the ⬇ icon. If you do not select logs, when you click the ⬇ icon, all displayed logs are exported.

      > ? **Note** If the number of logs to be exported is greater than 10,000, only the first 10,000 logs can be exported.

3.5.10. View authorization information

The Authorization module allows customers, field engineers, and operations engineers to query services experiencing authorization problems and troubleshoot the problems.

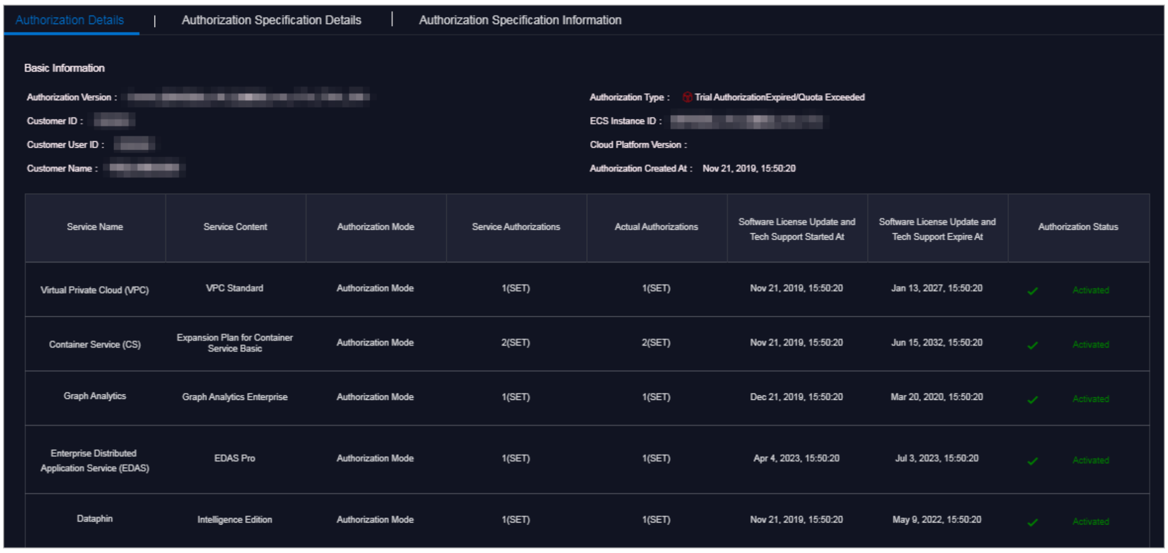
Prerequisites

Make sure that the current logon user has administrator permissions. Only after you are granted administrator permissions, are you allowed to view the trial authorization information or enter the authorization code to view the formal authorization information on the **Authorization Details** tab.

If you are not granted administrator permissions, when you access this tab, a message indicating that the user has insufficient permissions is displayed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Authorization**. The **Authorization Details** tab appears.



Authorization Details
Authorization Specification Details
Authorization Specification Information

Basic Information

Authorization Version : [redacted]

Customer ID : [redacted]

Customer User ID : [redacted]

Customer Name : [redacted]

Authorization Type : Trial AuthorizationExpired/Quota Exceeded

ECS Instance ID : [redacted]

Cloud Platform Version :

Authorization Created At : Nov 21, 2019, 15:50:20

Service Name	Service Content	Authorization Mode	Service Authorizations	Actual Authorizations	Software License Update and Tech Support Started At	Software License Update and Tech Support Expire At	Authorization Status
Virtual Private Cloud (VPC)	VPC Standard	Authorization Mode	1(SET)	1(SET)	Nov 21, 2019, 15:50:20	Jan 13, 2027, 15:50:20	✓ Activated
Container Service (CS)	Expansion Plan for Container Service Basic	Authorization Mode	2(SET)	2(SET)	Nov 21, 2019, 15:50:20	Jun 15, 2032, 15:50:20	✓ Activated
Graph Analytics	Graph Analytics Enterprise	Authorization Mode	1(SET)	1(SET)	Dec 21, 2019, 15:50:20	Mar 20, 2020, 15:50:20	✓ Activated
Enterprise Distributed Application Service (EDAS)	EDAS Pro	Authorization Mode	1(SET)	1(SET)	Apr 4, 2023, 15:50:20	Jul 3, 2023, 15:50:20	✓ Activated
Dataphin	Intelligence Edition	Authorization Mode	1(SET)	1(SET)	Nov 21, 2019, 15:50:20	May 9, 2022, 15:50:20	✓ Activated

4. Perform the following operations to view the authorization information.

> **Note** For formal authorization, you must enter the authorization code to view the authorization information. Obtain the authorization code in the authorization letter attached by the project contract or contact the business manager (CBM) of your project to obtain the authorization code.

- On the **Authorization Details** tab, view the basic authorization information.

  You can view authorization information, including authorization version, customer information, authorization type, Elastic Compute Service (ECS) instance ID, cloud platform version, the creation time of authorization, and the authorization information of all cloud services in different data centers.

  The following table describes the detailed authorization information.

Item	Description
Authorization Version	You can use the BP number in the version to associate with a project or contract. Notes: ▪ **TRIAL** in the version indicates that the authorization is trial authorization. The trial authorization is valid for 90 days after the date of deployment. ▪ **FORMAL** in the version indicates that the authorization is a formal one. The authorization information of the service comes from the signed contract.

Item	Description
Authorization Type	Indicates the current authorization type and authorization status. - The following authorization methods are available: - **Trial Authorization** - **Formal Authorization** - The following authorization status is available: - **Not Activated** - **Expire Soon** - **Activated** - **Expired** - **Expired/Quota Exceeded**
Customer Information	The information includes the customer name, customer ID, and customer user ID.
ECS Instance ID	The ECS instance ID in the deployment planner of the field environment.
Cloud Platform Version	The Apsara Stack version of the current cloud platform.
Authorization Created At	The start time of the authorization.
Licensing Details of Apsara Stack Products (IDC Level)	The authorization information of cloud services within different regions, including the service name, service content, current authorization mode, service authorization quantity, actual authorization quantity, software license update and technical support start time, software license update and technical support end time, and real-time product authorization status. If the following information appears in the **Authorization Status** column of a service, take note of the following items: - **RENEW Service Expired** Indicates that the customer must renew the subscription as soon as possible. Otherwise, field operations services (including ticket processing) are terminated. - **Specification Quota Exceeded** Indicates that the specifications deployed for a service have exceeded the contract quota, and the customer must scale up the service as soon as possible.

- Click the **Authorization Specification Details** tab to view the authorization specification information of services across different data centers or regions.

  The following table describes the authorization specification items.

Column name	Description
Service Name	The name of the authorized service.
Specification Name	The specification name of an authorized service.
Specifications	The total number of current authorizations of a specification for a service.
Specification Quota	The authorization quota of a specification for a service.
Specification Status	The current authorization status of a specification for a service.

- Click the **Authorization Specification Information** tab to view the authorization specification information and the authorization specification excess information of services.

  Set **Licensing Specification Level**, **Region ID** or **IDC ID**, **Service Name**, and time range, and then click **Search**. You can view the authorization specification information of a service in the current environment, including the maximum and minimum number of specifications and their occurrence time points as well as the average number of specifications within the specified time range.

  In the **Authorization Specification Information** or **Authorization Specification Excess Information** section, click the + icon to the left of a service to view the number of authorization specifications, specification quota, and recorded time of authorization specifications on the latest day of the specified time range for the specification of the service. Click **View More** to view the authorization specification information of the service within the specified time range by date.

3.5.11. Multi-cloud management

The Multi-cloud Management module provides the function of multi-cloud configurations. By using the multi-cloud configurations, you can perform Operations & Maintenance (O&M) operations on different data centers on an operations and maintenance platform.

3.5.11.1. Add multi-cloud configurations

When a multi-cloud environment is used, you can add multi-cloud configurations as a multi-cloud configuration administrator or super administrator. After you add multi-cloud configurations, you can switch to different data centers in the same console and then view or perform related operations.

Prerequisites

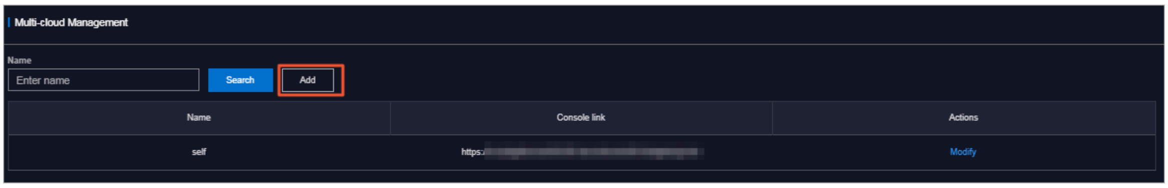
Before you add multi-cloud configurations, make sure that the following requirements are met:

- Data centers are interconnected and share accounts that have the same usernames and passwords with each other.
- You are granted the permissions of a multi-cloud configuration administrator or super administrator.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.

3. In the left-side navigation pane, choose **Settings > Multi-cloud Management**.
4. In the upper part of the page, click **Add**.



Name	Console link	Actions
self	https://[redacted]	Modify

5. In the dialog box that appears, add the console link of another data center and click **OK**.

Parameter	Description
Cloud Name	The name of another data center.
Central region Console link	The console link of another data center. Make sure that the console link is correct. Otherwise, an error message is returned.

After you add multi-cloud configurations, you can log on to the Apsara Uni-manager Operations Console by using a shared account to switch to different data centers and perform related operations.

3.5.11.2. Modify the name of a data center

After you add multi-cloud configurations, you can modify the name of a data center as a multi-cloud configuration administrator or super administrator.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **System Settings > Multi-cloud Management**.
4. (Optional)In the **Cloud Name** field, enter the name of the data center that you want to modify and click **Search**.
5. Find the data center that you want to modify and click **Modify** in the **Actions** column.
6. In the dialog box that appears, modify the name of the data center and click **OK**.

3.6. Personal Settings

The Personal Settings module allows you to modify the logon password and logon settings of the current account.

3.6.1. Change the logon password

The Logon Settings module allows you to change the password that you use to log on to the Apsara Uni-manager Operations Console.

Context

For security reasons, we recommend that you change your logon password on a regular basis.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Personal Settings > Personal Information**.
4. View the personal information of the current user, such as **Username** and **Department**.
5. Click **Change Password** to change the password that you use to log on to the Apsara Uni-manager Operations Console.
6. In the **Change Password** dialog box, enter **Current Password**, **New Password**, and **Confirm Password**, and then click **OK**.

3.6.2. Modify logon settings

The Logon Settings module allows you to modify the logon timeout period, whether to allow multi-terminal logon, maximum allowed password retries, logon policy, and validity period of the account you are using.

Context

To improve system security, you can modify the logon settings based on your scenario.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Settings**.
3. In the left-side navigation pane, choose **Personal Settings > Logon Settings**.
4. On the **Logon Settings** tab, modify the following parameters.
   - **Logon Timeout Period (Minutes)**: Set the logon timeout period of the current account. If the logon time exceeds the specified time period, the system prompts you that the logon timed out and you can try to log on again.
   - **Multi-Terminal Logon Settings**: Set whether the current account allows multi-terminal logon. You can select **Multi-Terminal Logon Allowed**, **Forbid Multi-Terminal Logon in ASO**, or **Forbid Multi-Terminal Logon in O&M**.
     - **Multi-Terminal Logon Allowed**: allows the current account to log on to the Apsara Uni-manager Operations Console from multiple terminals at the same time.
     - **Forbid Multi-Terminal Logon in ASO**: The current account is not allowed to log on to the Apsara Uni-manager Operations Console from multiple terminals at the same time, but is allowed to go to another console from the Apsara Uni-manager Operations Console.

       For example, User A uses the current account to go to another console from the Apsara Uni-manager Operations Console. At the same time, User B uses the current account to log on to the Apsara Uni-manager Operations Console. The system disables the logon of User A only after User A returns to the Apsara Uni-manager Operations Console.
     - **Forbid Multi-Terminal Logon in O&M**: The current account is not allowed to log on to the Apsara Uni-manager Operations Console or the console redirected from the Apsara Uni-manager Operations Console from multiple terminals.
   - **Maximum Allowed Password Retries**: Set the maximum number of password retries before

the account may be locked. When the number of retries reaches the specified number, the account is locked. After the account is locked, you must use the system administrator account to unlock it.

- **Logon Policies**: Set the logon policy of the current account. You can select **Blacklist** or **Whitelist**. For information about how to create logon policies, see Logon policies.
    - **Blacklist**: If this option is selected, IP addresses configured in logon policies are not allowed to log on to the Apsara Uni-manager Operations Console.
    - **Whitelist**: If this option is selected, IP addresses configured in logon policies are allowed to log on to the Apsara Uni-manager Operations Console.

5. Click **Save**.
6. Click the **Account Validity Period** tab and set **Account Validity (Days)**.

> ? **Note** When your account expires, you must use the system administrator account to unlock it.

7. Click **Save**.

4.Resources

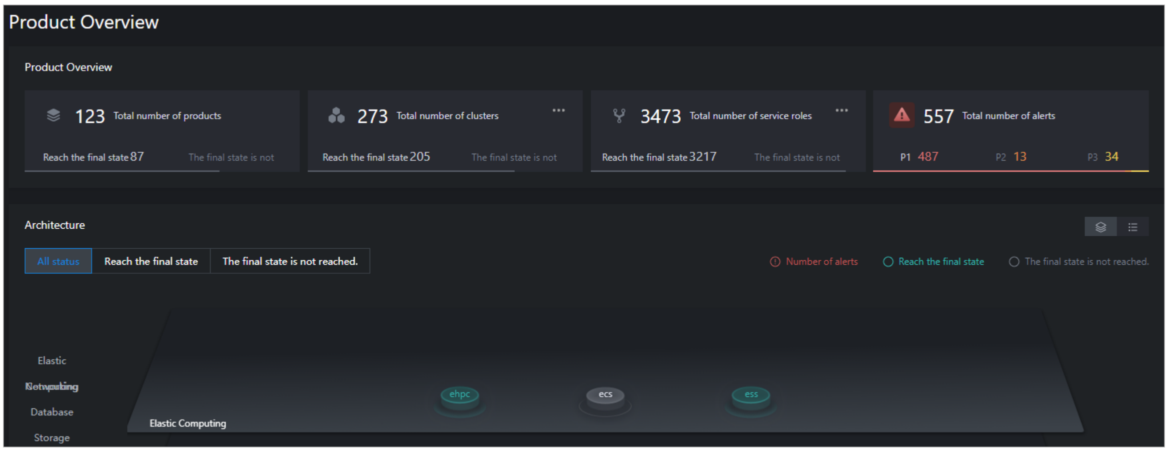
4.1. Products

4.1.1. Product overview

On the Product Overview page, you can view the information of each product and its clusters, service roles, machines, alerts, and final-state status.

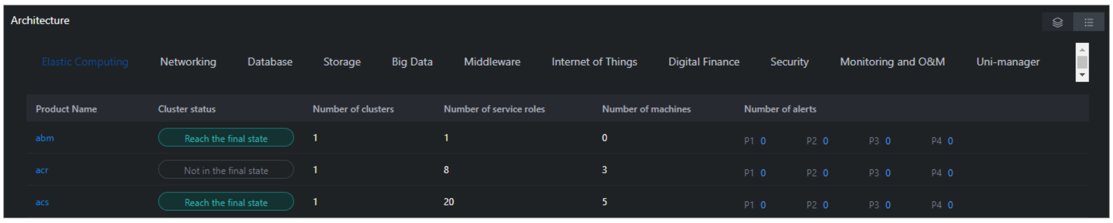
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Products**.
3. On the **Product Overview** page, view the information of clusters, service roles, machines, alerts, and final-state statuses.



- ○ In the **Product Overview** section, view the total numbers of products, clusters, service roles, and alerts as well as the final-state status of these products, clusters, and service roles.
  - ■ Click the ••• icon next to **Total number of clusters** and view the information of the clusters on the **Cluster list** page.
  - ■ Click the ••• icon next to **Total number of service roles** and view the information of the service roles on the **Service role** page.
- ○ View the information of the products in the **Architecture** section.
  - ■ Click the **All status**, **Reach the final state**, or **The final state is not reached.** tab to view the information of the products in the corresponding state.
  - ■ Click a product type in the left-side product type list to view the final-state status and alerts of the products of the corresponding type.

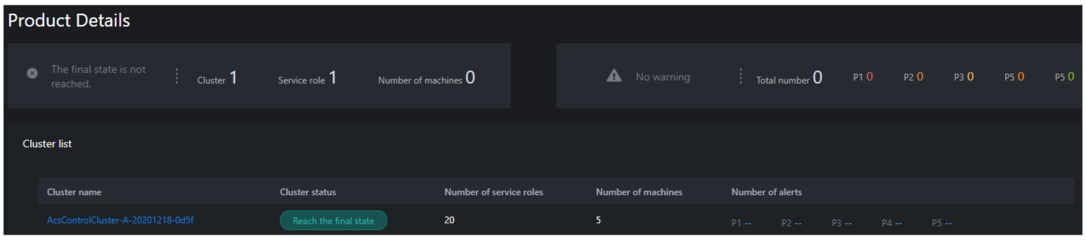
- Click the ☰ icon in the upper-right corner to view the cluster status and the numbers of clusters, service roles, machines, and alerts in a list form.



Architecture

Product Name	Cluster status	Number of clusters	Number of service roles	Number of machines	Number of alerts
abm	Reach the final state	1	1	0	P1 0 P2 0 P3 0 P4 0
acr	Not in the final state	1	8	3	P1 0 P2 0 P3 0 P4 0
acs	Reach the final state	1	20	5	P1 0 P2 0 P3 0 P4 0

- Click a product type in the upper product type list to view the information of the products of the corresponding type.
- Click a product name in the Product Name column to view the details of the product on the **Product Details** page.



Product Details

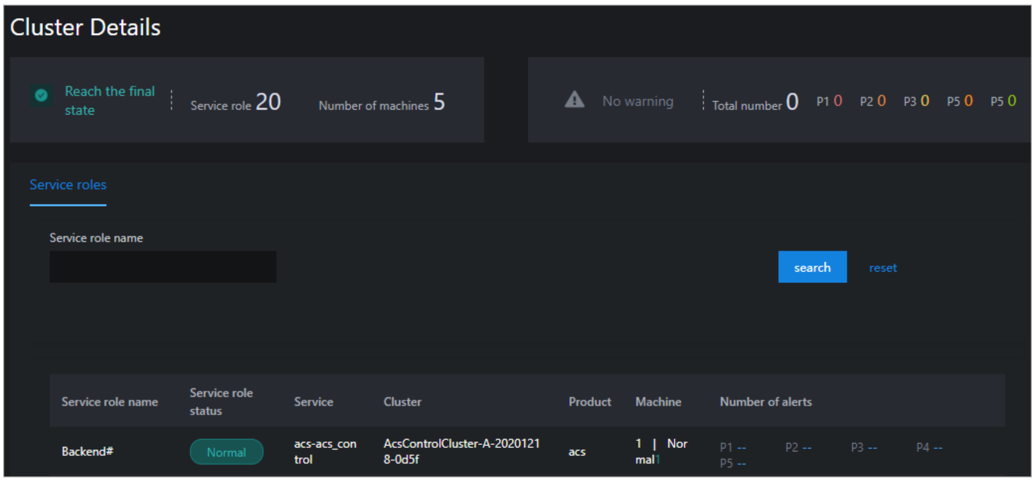
The final state is not reached. Cluster 1 Service role 1 Number of machines 0

No warning Total number 0 P1 0 P2 0 P3 0 P5 0 P5 0

Cluster list

Cluster name	Cluster status	Number of service roles	Number of machines	Number of alerts
AcsControlCluster-A-20201218-0d5f	Reach the final state	20	5	P1 -- P2 -- P3 -- P4 -- P5 --

a. Click a cluster name in the Cluster Name column to view the details of the cluster on the **Cluster Details** page.



Cluster Details

Reach the final state Service role 20 Number of machines 5

No warning Total number 0 P1 0 P2 0 P3 0 P5 0 P5 0

Service roles

Service role name

Service role name	Service role status	Service	Cluster	Product	Machine	Number of alerts
Backend#	Normal	acs-acs_control	AcsControlCluster-A-20201218-0d5f	acs	1 | Normal	P1 -- P2 -- P3 -- P4 -- P5 --

b. Enter a service role name in the **Service Role Name** search box and click **search** to view the details about the service role.

c. (Optional) Click **reset** to clear the search conditions.

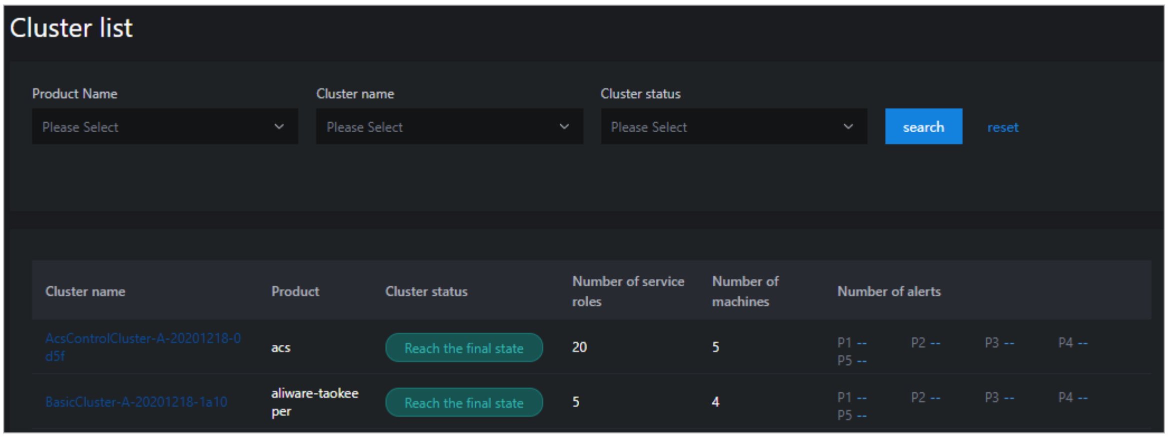
- Click the icon in the upper-right corner to view the information about the products in a graphical form.

4.1.2. Clusters

You can view the status and alerts of all the deployed clusters and their service roles on the Cluster list page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources** > **Products**.
3. In the left-side navigation pane, click **Clusters**.
4. On the **Cluster list** page, select a product from the **Product Name** drop-down list, select a cluster from the **Cluster Name** drop-down list, and then select a state from the **Cluster Status** drop-down list. Then, click **search** to view the search results.

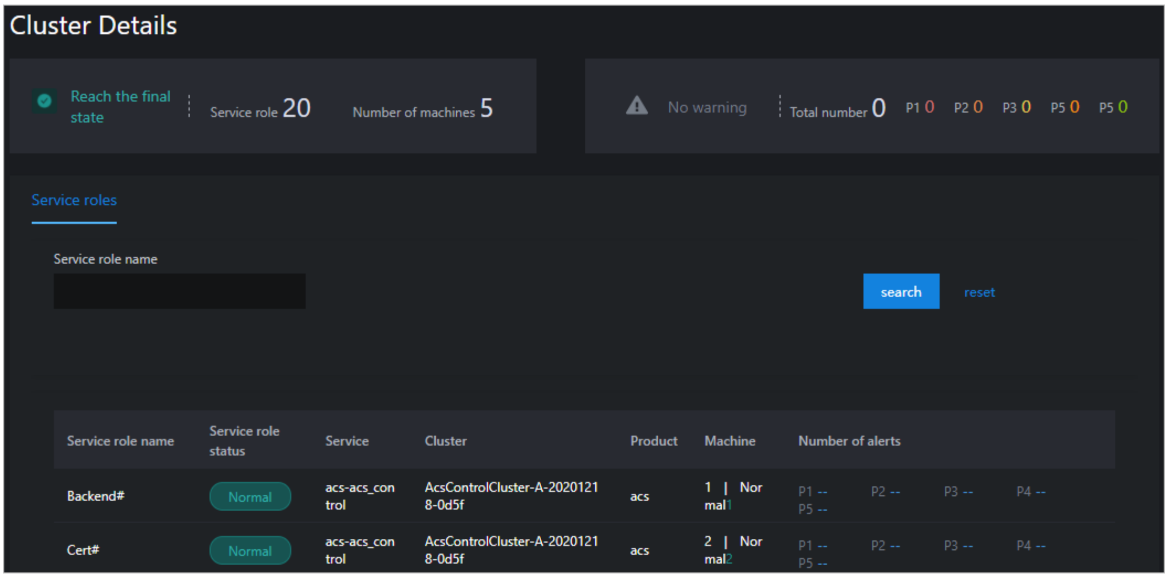


Cluster list

Product Name	Cluster name	Cluster status
Please Select	Please Select	Please Select

Cluster name	Product	Cluster status	Number of service roles	Number of machines	Number of alerts
AcsControlCluster-A-20201218-0d5f	acs	Reach the final state	20	5	P1 -- P2 -- P3 -- P4 -- P5 --
BasicCluster-A-20201218-1a10	aliware-taokeeper	Reach the final state	5	4	P1 -- P2 -- P3 -- P4 -- P5 --

5. (Optional) Click **reset** to clear the filter conditions.
6. Click a cluster name in the Cluster Name column to view the details of the cluster on the **Cluster Details** page.



Cluster Details

Reach the final state | Service role 20 | Number of machines 5

No warning | Total number 0 | P1 0 | P2 0 | P3 0 | P5 0 | P5 0

Service role name	Service role status	Service	Cluster	Product	Machine	Number of alerts
Backend#	Normal	acs-acs_control	AcsControlCluster-A-20201218-0d5f	acs	1 | Normal1	P1 -- P2 -- P3 -- P4 -- P5 --
Cert#	Normal	acs-acs_control	AcsControlCluster-A-20201218-0d5f	acs	2 | Normal2	P1 -- P2 -- P3 -- P4 -- P5 --

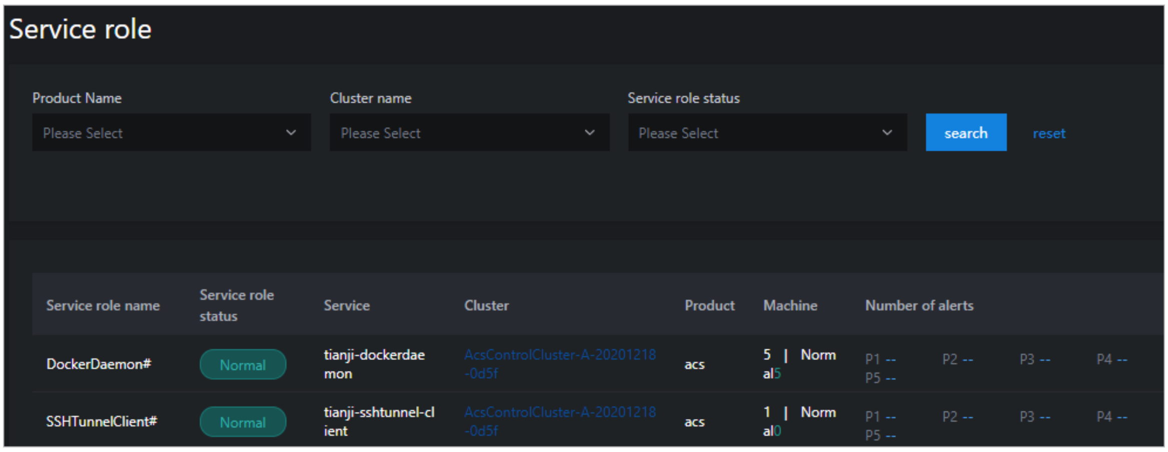
7. Enter a service role name in the **Service Role Name** search box and click **search** to view the details of the service role.
8. (Optional) Click **reset** to clear the filter conditions.

4.1.3. Service roles

On the Service role page, you can view the service role of a specific product or cluster and the status and alerts of the cluster.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Products**.
3. In the left-side navigation pane, click **Service Roles**.
4. On the **Service role** page, select a product from the **Product Name** drop-down list, select a cluster from the **Cluster name** drop-down list, and then select a state from the **Service role status** drop-down list. Then, click **search** to view the search results displayed below.

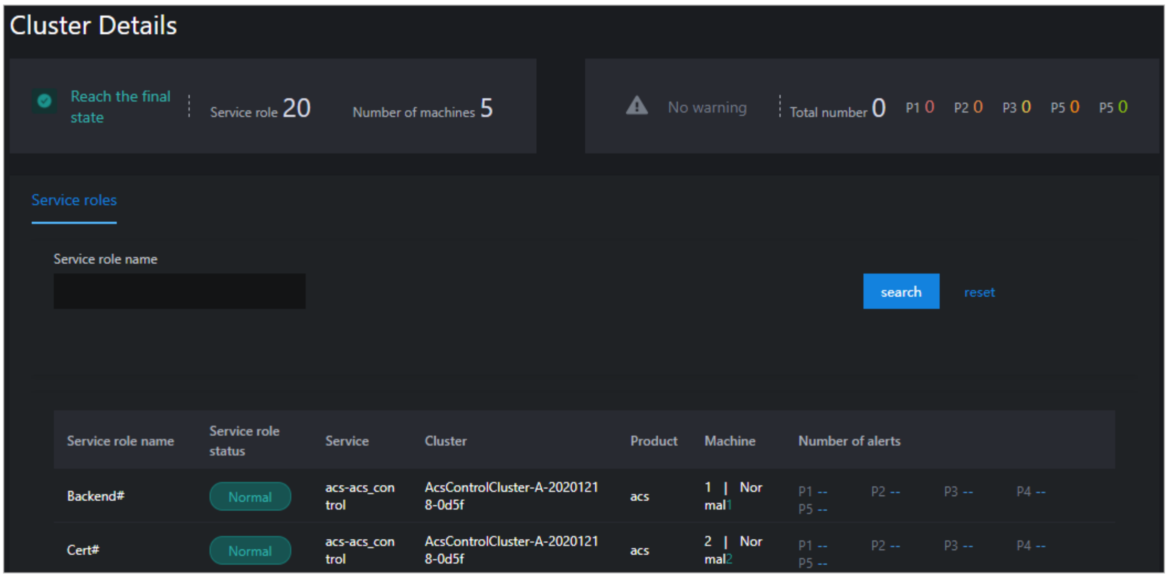


Service role

Product Name: Please Select
Cluster name: Please Select
Service role status: Please Select

Service role name	Service role status	Service	Cluster	Product	Machine	Number of alerts			
DockerDaemon#	Normal	tianji-dockerdaemon	AcsControlCluster-A-20201218-0d5f	acs	5 | Normal5	P1 -- P5 --	P2 --	P3 --	P4 --
SSHTunnelClient#	Normal	tianji-sshtunnel-client	AcsControlCluster-A-20201218-0d5f	acs	1 | Normal0	P1 -- P5 --	P2 --	P3 --	P4 --

5. (Optional) Click **reset** to clear the filter conditions.
6. Click a cluster name in the Cluster column to view the details of the cluster on the **Cluster Details** page.



Cluster Details

Reach the final state | Service role 20 | Number of machines 5

No warning | Total number 0 P1 0 P2 0 P3 0 P5 0 P5 0

Service role name	Service role status	Service	Cluster	Product	Machine	Number of alerts			
Backend#	Normal	acs-acs_control	AcsControlCluster-A-20201218-0d5f	acs	1 | Normal1	P1 -- P5 --	P2 --	P3 --	P4 --
Cert#	Normal	acs-acs_control	AcsControlCluster-A-20201218-0d5f	acs	2 | Normal2	P1 -- P5 --	P2 --	P3 --	P4 --

7. Enter a service role name in the **Service role name** search bar and click **search** to view the details of the service role.
8. (Optional) Click **reset** to clear the filter conditions.

4.2. Network

The network module provides the cloud service interconnection and network resource management features for the hybrid cloud network. The user is the network administrator of Apsara Stack.

4.2.1. Cloud service interconnection

The cloud service interconnection feature provides network access to cloud services, configuration of VIPs and DNS, and mutual access between cloud services in multiple clouds, IDCs, and Apsara Stack.

4.2.1.1. Dynamic VIP

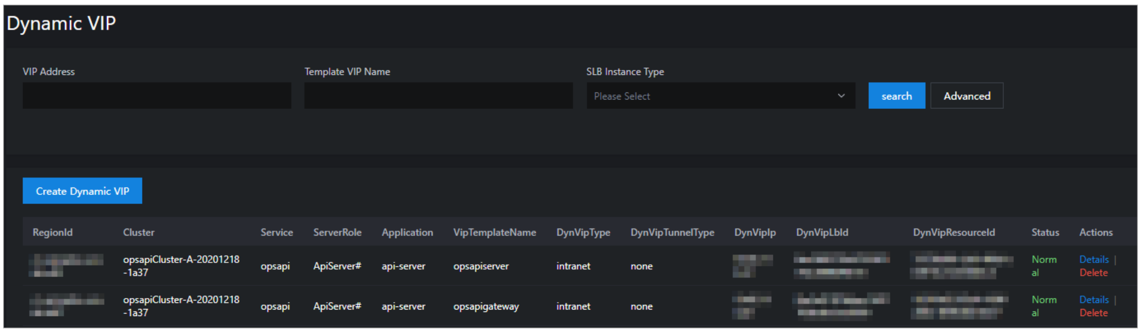
The dynamic VIP feature expands the network capabilities of cloud service interconnection. It allows you to create dynamic VIPs by using VIP resources applied for by the cloud services in Apsara Infrastructure Management Framework as templates. You can modify the type, tunnel_type, and ipprotocol properties when you create a dynamic VIP. Other properties are the same as those in the template VIP resources defined by the cloud products. During scaling, upgrades, and downgrades of products, dynamic VIP resources and template VIP resources can be updated simultaneously by linking with Apsara Infrastructure Management Framework.

Context

- In scenarios that require large storage capacities, the dynamic VIP feature can be used to scale out multiple OSS Intranet VIP resources to bypass the single-VIP network speed of 5 Gbit/s.
- In hybrid cloud scenarios, you must access the Apsara Uni-manager Operations Console over the Internet and use the dynamic VIP feature to create Internet VIP resources for the Apsara Uni-manager Operations Console.
- The dynamic VIP tunnel type can be set only to classic_to_any_tunnel.

Procedure

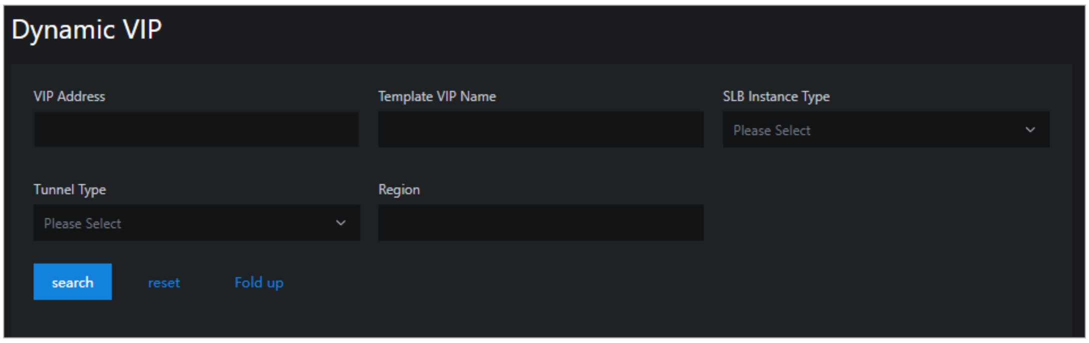
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources** > **Network**.
3. On the **Dynamic VIP** page, view the dynamic VIPs.
   - Enter a VIP name in the **VIP Address** search box, enter a template VIP name in the **Template VIP Name** search box, and then select a type from the **SLB Instance Type** drop-down list. Then, click **search** to view the dynamic VIPs. Click **Details** in the Actions column corresponding to a dynamic VIP to view the details of the dynamic VIP.



RegionId	Cluster	Service	ServerRole	Application	VipTemplateName	DynVipType	DynVipTunnelType	DynVipIp	DynVipLbId	DynVipResourceId	Status	Actions
[redacted]	opsapiCluster-A-20201218-1a37	opsapi	ApiServer#	api-server	opsapiserver	intranet	none	[redacted]	[redacted]	[redacted]	Normal	Details | Delete
[redacted]	opsapiCluster-A-20201218-1a37	opsapi	ApiServer#	api-server	opsapigateway	intranet	none	[redacted]	[redacted]	[redacted]	Normal	Details | Delete

   - Use more filter conditions to view the information of dynamic VIPs.

a. Click **Advanced**, select a type from the **Tunnel Type** drop-down list (you can select multiple types), and enter a region name in the **Region** search box. Then, click **search** to view the dynamic VIPs.

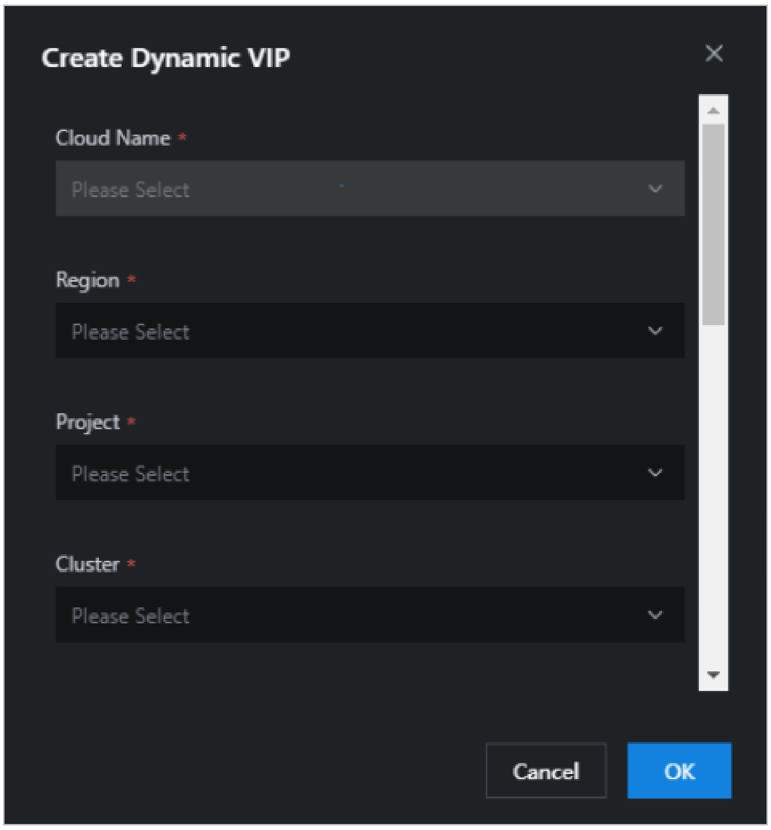


b. (Optional) Click **reset** to clear the filter conditions.

c. (Optional) Click **Fold up** to hide the **Tunnel Type** and **Region** options.

4. Create, update, and delete dynamic VIPs.

   - Click **Create Dynamic VIP** above the dynamic VIP list. In the Create Dynamic VIP dialog box, configure the parameters. Then, click **OK** to create a dynamic VIP.



Parameters:

- Cloud Name: the name of the cloud instance.
- Region: the ID of the region.
- Project: the name of the product.
- Cluster: the name of the cluster.
- Service: the name of the service.

- ServerRole: the name of the service role.
- Application: the name of the application.
- Template VIP Name: the name of the template VIP.
- DynVipType: the type of the instance.
- DynVipTunnelType: the type of the tunnel.
- Ipprotocol: the type of the dynamic VIP.

- Update a dynamic VIP.

  If the basic properties of a dynamic VIP are inconsistent with those of a template VIP, or if an operation on the dynamic VIP fails, **Abnormal** is displayed in the **Status** column corresponding to the dynamic VIP. When the system detects an exception in the dynamic VIP status, the system automatically checks and deletes DNS records associated with the abnormal dynamic VIP to reduce the impact on your business.

  The O&M personnel must check whether the abnormal dynamic VIP status is caused by resource changes during product upgrades or scaling and perform the following operations accordingly:

  - If the abnormal dynamic VIP status is caused by resource changes during product upgrades or scaling, click **Update** in the Actions column corresponding to the dynamic VIP. The system queries the template VIP parameters through calls to Apsara Infrastructure Management Framework API operations and combine these parameters with the variable properties of the dynamic VIP to update the dynamic VIP.
  - If the abnormal dynamic VIP status is not caused by resource changes during product upgrades or scaling, submit a ticket to contact Apsara Stack technical support.

- To delete a dynamic VIP, click **Delete** in the Actions column corresponding to the dynamic VIP. In the message that appears, click **OK**.

  > **Notice** Risks may arise if you delete dynamic VIPs. Proceed with caution. Before you delete a dynamic VIP, make sure that the VIP does not have sessions and that DNS records can no longer be resolved to the dynamic VIP.

4.2.1.2. Dynamic DNS

Dynamic DNS works with the dynamic VIP feature. It allows you to implement horizontal network expansion by resolving DNS resources in cloud services to multiple VIPs (one static VIP and multiple dynamic VIPs).

Context

Dynamic DNS is applicable to scenarios such as multi-cloud geo-disaster recovery and hybrid clouds. The following features are supported:

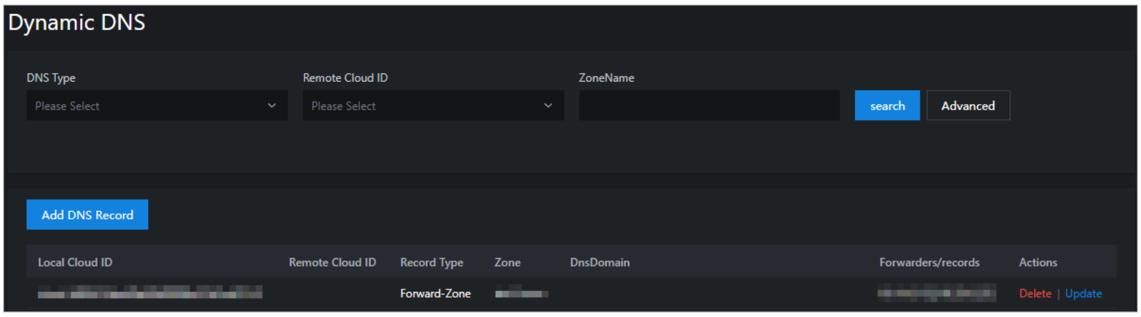
- Adds domain names for zones corresponding to ops-dns intranet-domain and internet-domain. By default, ops-dns returns the resolution records in rotation mode.
- Adds the forwarding records of a tenant DNS to forward domain name resolution requests in a specified zone to external DNS servers such as DNS servers in Apsara Stack, heterogeneous clouds, and Alibaba Cloud.

> **Notice** Before you resolve DNS domain names in the Apsara Infrastructure Management

Framework console, make sure that the parameters of the dynamic VIPs and the static VIP are exactly the same, and VIP listening on access is normal. Otherwise, network exceptions may occur.

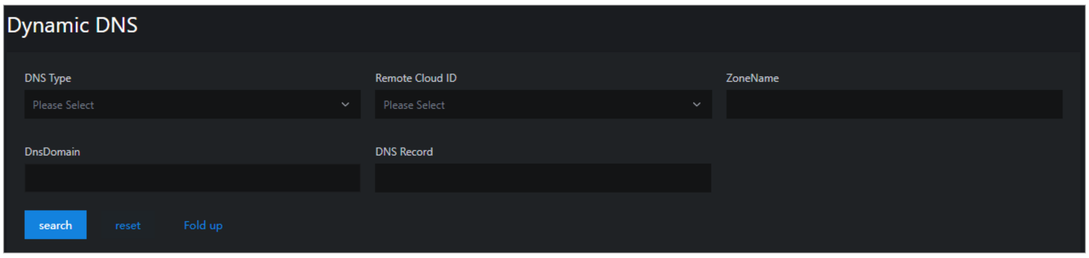
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Dynamic DNS**. On the **Dynamic DNS** page, view the information about dynamic DNS.
   - Select a type from the **DNS Type** drop-down list, select a cloud ID from the **Remote Cloud ID** drop-down list, and then enter a domain name in the **ZoneName** search box. Then, click **search** to view the dynamic DNS records.

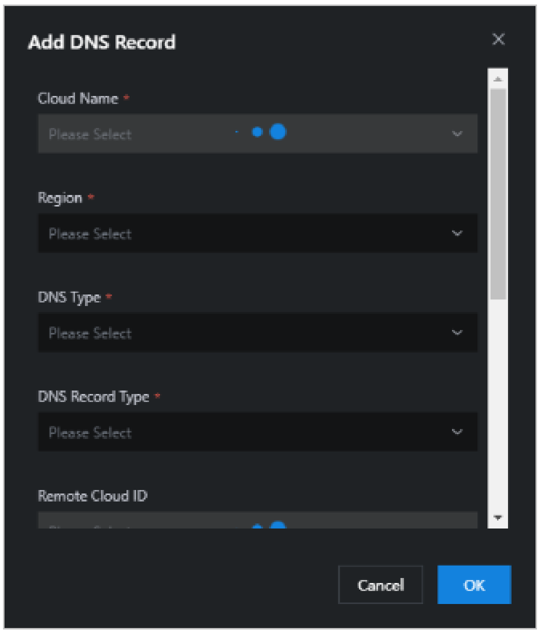


Local Cloud ID	Remote Cloud ID	Record Type	Zone	DnsDomain	Forwarders/records	Actions
[redacted]		Forward-Zone	[redacted]		[redacted]	Delete | Update

   - Use more filter conditions to search for the dynamic DNS records.
     a. Click **Advanced**, enter a domain name in the **DnsDomain** search box, and then enter a DNS record in the **DNS Record** search box. Then, click **search** to view the dynamic DNS records.



     b. (Optional) Click **reset** to clear the filter conditions.
     c. (Optional) Click **Fold up** to hide the **DnsDomain** and **DNS Record** options.
4. Update and delete the dynamic DNS records or create new dynamic DNS records.
   - Click **Add DNS Record** above the dynamic DNS record list. In the Add DNS Record dialog box, configure the parameters. Then, click **OK** to create a dynamic DNS record.



Add DNS Record

Cloud Name *: Please Select

Region *: Please Select

DNS Type *: Please Select

DNS Record Type *: Please Select

Remote Cloud ID

Parameters:

- Cloud Name: the name of the cloud instance.
- Region: the ID of the region.
- DNS Type: the DNS type. Valid values: dns product and ops dns.
- DNS Record Type: the type of the DNS record. Valid values: Forward-Zone and A.
- Remote Cloud ID: the ID of the cloud instance in the current cloud.
- DnsZone: the DNS zone. Separate multiple zones with commas (,).
- Forwarders: the forwarding IP addresses. Separate multiple IP addresses with commas (,).
- DnsDomain: the DNS domain address.
- DnsRecord: the IP address of the DNS record.

- Click **Update** in the Actions column corresponding to the DNS record. In the dialog box that appears, modify the Remote Cloud ID and DnsRecord parameters. Then, click **OK**.
- To delete a DNS record, click **Delete** in the Actions column corresponding to the DNS record. In the message that appears, click **OK**.

> **Notice** Risks may arise if you delete DNS records. Proceed with caution. Before you delete a DNS record, make sure that an alternate DNS record is available for the domain name or that no other clients have access to this domain name.

4.2.1.3. Cross-cloud access

Cross-cloud access allows you to manage data for network access of cloud services in hybrid clouds.

Context

Before you enable cross-cloud access, you must configure IP network routing based on the access matrix data and grant the network access permissions.

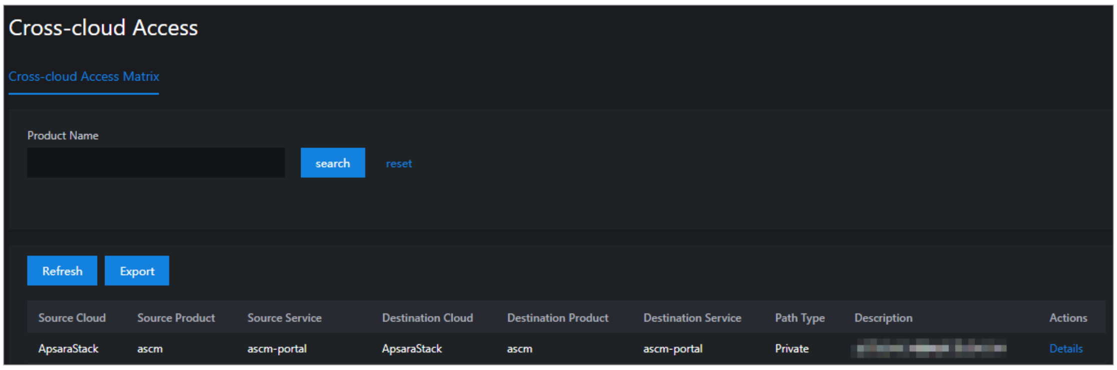
Cross-cloud access is applicable to the following scenarios:

- Connection between Apsara Stack Enterprise and public cloud VPCs through dedicated lines: Public cloud VPCs and Apsara Stack VPCs can be connected by using dedicated lines.
- Connection between Apsara Stack Enterprise and public cloud VPCs over the Internet: Apsara Stack provides Internet egresses, so that public cloud VPCs and Apsara Stack VPCs can be connected over the Internet.
- Connection between Apsara Stack Agility ZStack and public cloud VPCs over the Internet: Apsara Stack Agility is connected to the Internet and ZStack VPCs are connected to public cloud VPCs over the Internet by using the IPSec VPN.
- Connection between Apsara Stack Enterprise and public cloud services through dedicated lines: Apsara Stack is connected to the public cloud by using dedicated lines to implement cloud management and network connection.
- Connection between Apsara Stack Enterprise, Apsara Stack Agility, and all-in-one cloud services (management) over the Internet: Apsara Stack Enterprise, Apsara Stack Agility, and all-in-one cloud services provide Internet egresses and can access cloud services on the Internet based on the NAT capabilities provided by user-managed firewalls.
- Hybrid clouds for multi-cloud remote disaster recovery: Hybrid clouds are connected to implement remote disaster recovery across regions.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Cross-cloud Access**. On the **Cross-cloud Access** page, view the information about access matrices.

   i. Enter a product name in the **Product Name** search box and click **search**. The access matrices are displayed in the lower part of the page.

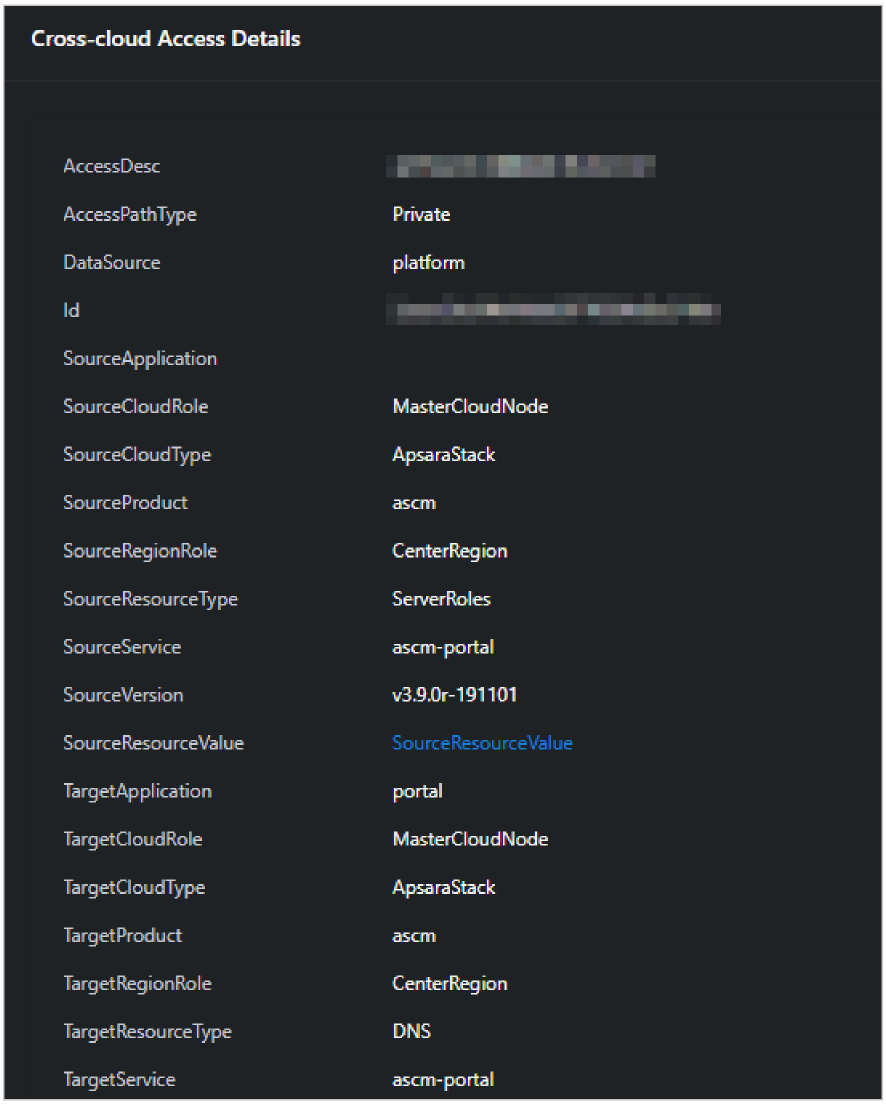


Cross-cloud Access

Product Name

Source Cloud	Source Product	Source Service	Destination Cloud	Destination Product	Destination Service	Path Type	Description	Actions
ApsaraStack	ascm	ascm-portal	ApsaraStack	ascm	ascm-portal	Private	[redacted]	Details

ii. Click **Details** in the Actions column corresponding to an access matrix to view the details of the access matrix.



Cross-cloud Access Details

AccessDesc	[redacted]
AccessPathType	Private
DataSource	platform
Id	[redacted]
SourceApplication	
SourceCloudRole	MasterCloudNode
SourceCloudType	ApsaraStack
SourceProduct	ascm
SourceRegionRole	CenterRegion
SourceResourceType	ServerRoles
SourceService	ascm-portal
SourceVersion	v3.9.0r-191101
SourceResourceValue	SourceResourceValue
TargetApplication	portal
TargetCloudRole	MasterCloudNode
TargetCloudType	ApsaraStack
TargetProduct	ascm
TargetRegionRole	CenterRegion
TargetResourceType	DNS
TargetService	ascm-portal

> **Note** If the cloud instance has multiple product clusters deployed or manages multiple lower-level cloud instances, each of the **SourceResourceValue** and **TargetResourceValue** parameters has multiple values. You must configure the network based on the source to the destination full mash.

iii. (Optional) Click **reset** to clear the filter conditions.

4. Click **Refresh**. Apsara Infrastructure Management Framework API is called to query the VIP, DNS, and SR resource values to refresh the **SourceResourceValue** and **TargetResourceValue** values.
5. Click **Export** to download the access matrix to your computer.

4.2.2. Hybrid cloud resources

You can manage hybrid cloud network resources such as physical network devices, network topology, and IP addresses in a centralized manner.

4.2.2.1. Physical topology

You can view the physical network topologies of hybrid clouds from multiple perspectives on the Physical Topology page.

Context

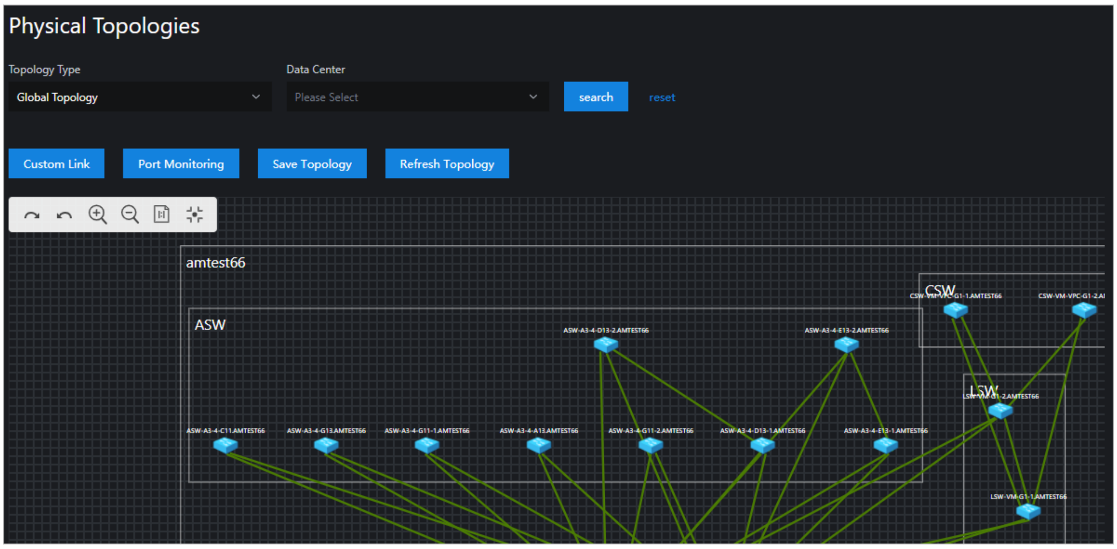
You can view the following types of physical network topologies:

- Standard topology: the physical network topology of the Apsara Stack data center. The initial data comes from Deployment Planner.
- IDC topology: the physical network topology of a self-managed IDC. The data comes from user-defined network devices or links.
- Global topology: the physical network topology of multiple data centers, including the standard topology and all IDC topologies. Data of interconnection links across data centers comes from user-defined links.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, choose **Hybrid Cloud Resources > Physical Topology**. On the **Physical Topologies** page, view the physical topologies.

i. Select the required options from the **Topology Type** and **Data Center** drop-down lists and click **search** to view the physical topologies.



Physical Topologies

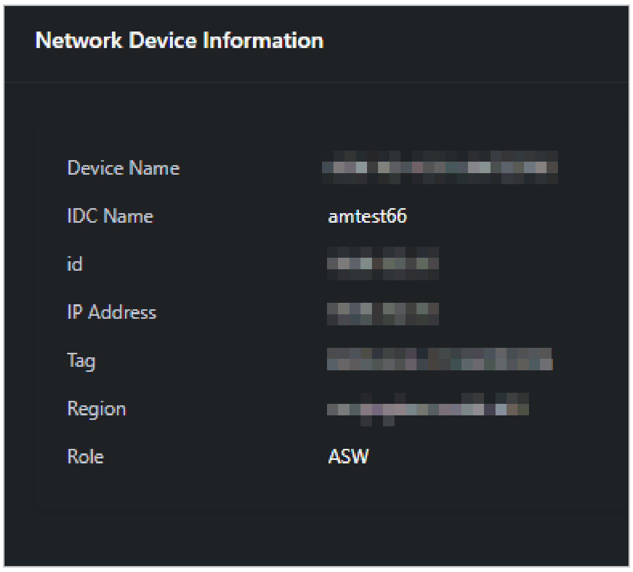
Topology Type: Global Topology

Data Center: Please Select

Note Action icons:

- ↷: proceeds with the next step.
- ↶: goes back to the previous step.
- ⊕: zooms in.
- ⊖: zooms out.
- 1:1: scales in proportion to the original aspect ratio.
- ⛶: scales to fit canvas.

ii. Click a node in the physical topology graph and the network device information of the node appears on the right side of the page.



Network Device Information

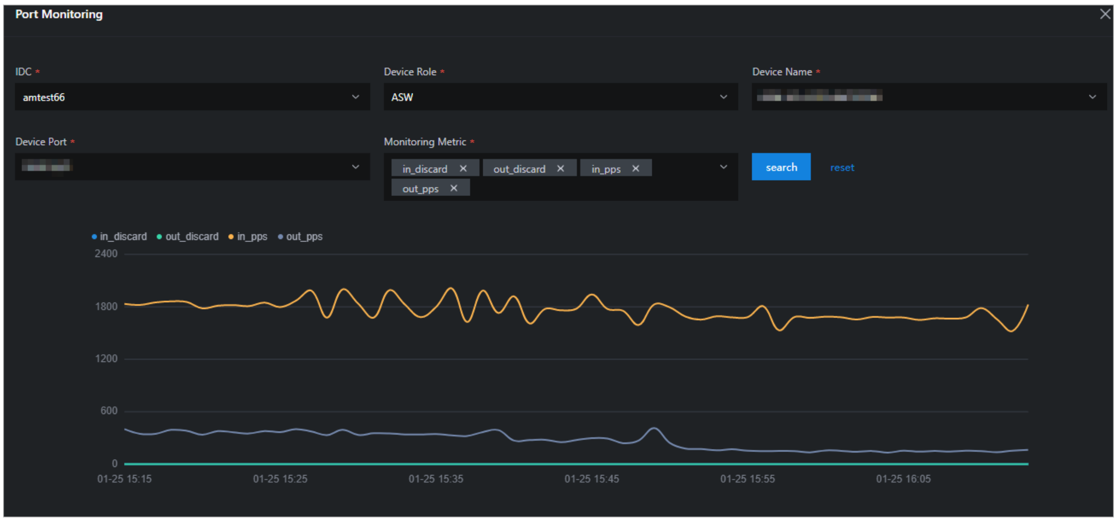
Device Name	[redacted]
IDC Name	amtest66
id	[redacted]
IP Address	[redacted]
Tag	[redacted]
Region	[redacted]
Role	ASW

iii. (Optional) Click **reset** to clear the filter conditions.

4. On the **Physical Topologies** page, click **Custom Link**. In the Custom Link dialog box, configure the parameters and click **OK** to set the link.
5. On the **Physical Topologies** page, click **Port Monitoring** to view the status of the ports.

i. On the Port Monitoring page, configure the parameters and click **search** to view the port status trend chart.

> Note You can select multiple options for **Monitoring Metric** at a time.



Port Monitoring

IDC *: amtest66

Device Role *: ASW

Device Name *: [redacted]

Device Port *: [redacted]

Monitoring Metric *: in_discard ✕ out_discard ✕ in_pps ✕ out_pps ✕

Monitoring metrics:

- in_discard: the inbound packet loss rate
- out_discard: the outbound packet loss rate
- in_pps: the inbound packet rate
- out_pps: the outbound packet rate
- in_bps: the inbound byte rate
- out_bps: the outbound byte rate
- in_error: the inbound packet error rate
- out_error: the outbound packet error rate

ii. (Optional) Click **reset** to clear the filter conditions.

6. If you move a node, click **Save Topology** to save the new coordinates of the node.
7. Click **Refresh Topology** to generate coordinates for the nodes in the background.

4.2.2.2. Network element management

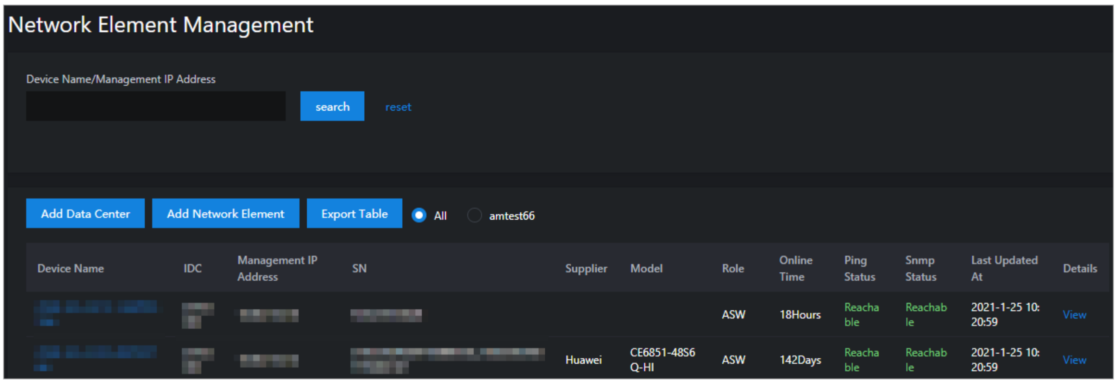
You can manage Apsara Stack data centers and user-managed data centers as well as their network element devices on the Network Element Management page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, choose **Hybrid Cloud Resources > Network Element Management**. On the **Network Element Management** page, view the details of the network element devices.

i. Enter a keyword in the **Device Name/Management IP Address** search box and click **search** to view the information about the network element device.

> **Note** The current Apsara Stack version supports status monitoring only for network elements in the Apsara Stack data center.



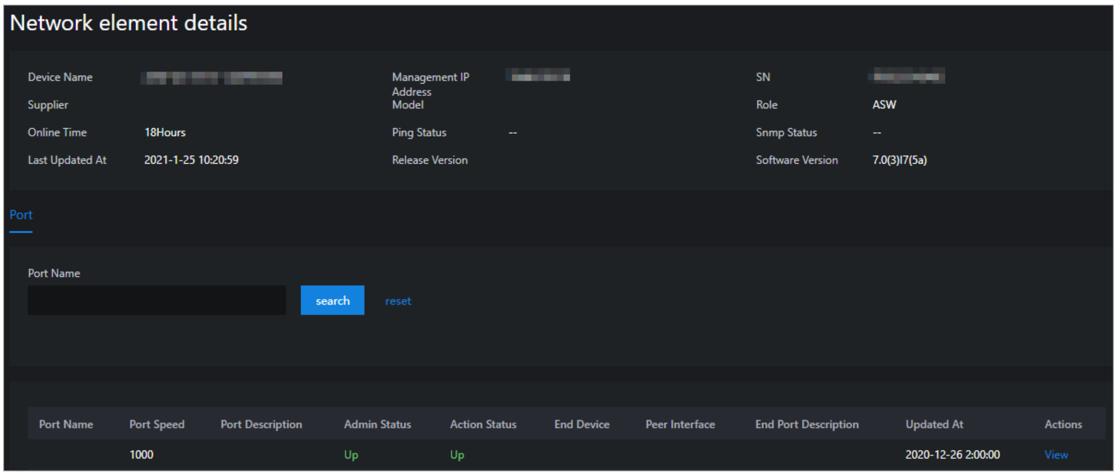
Network Element Management

Device Name/Management IP Address

Device Name	IDC	Management IP Address	SN	Supplier	Model	Role	Online Time	Ping Status	Snmp Status	Last Updated At	Details
[redacted]	[redacted]	[redacted]	[redacted]			ASW	18Hours	Reachable	Reachable	2021-1-25 10:20:59	View
[redacted]	[redacted]	[redacted]	[redacted]	Huawei	CE6851-48S6Q-HI	ASW	142Days	Reachable	Reachable	2021-1-25 10:20:59	View

ii. Click **View** in the Details column corresponding to a network element device. On the **Network element details** page, enter a port name in the **Port Name** search box and click **search** to view the port information. Click **View** in the Actions column to view the details of the port.

> **Note** The current Apsara Stack version supports management and monitoring only for network element ports in the Apsara Stack data center.



Network element details

Device Name [redacted]
Supplier
Online Time 18Hours
Last Updated At 2021-1-25 10:20:59

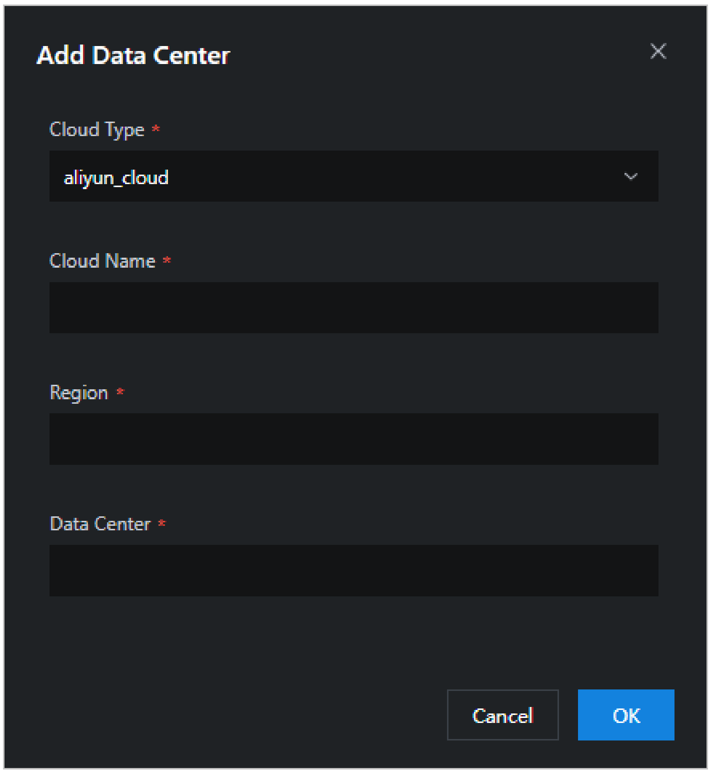
Management IP Address [redacted]
Model
Ping Status --
Release Version

SN [redacted]
Role ASW
Snmp Status --
Software Version 7.0(3)I7(5a)

Port Name	Port Speed	Port Description	Admin Status	Action Status	End Device	Peer Interface	End Port Description	Updated At	Actions
	1000		Up	Up				2020-12-26 2:00:00	View

iii. (Optional) Go back to the **Network Element Management** page and click **reset** to clear the filter conditions.

4. Click **Add Data Center**. In the Add Data Center dialog box, configure the parameters and click **OK** to add a data center.



Add Data Center

Cloud Type *: aliyun_cloud

Cloud Name *

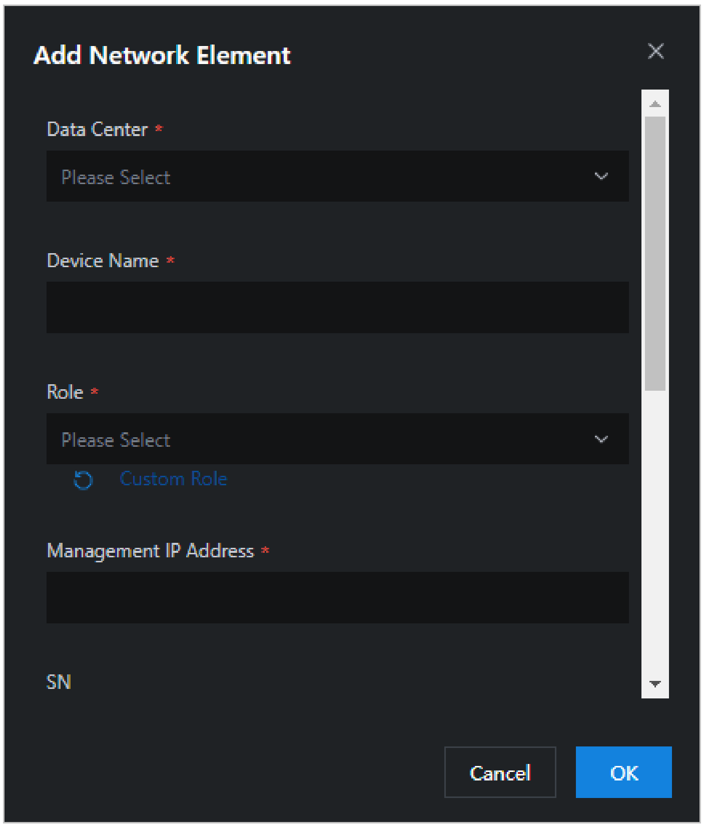
Region *

Data Center *

Parameter	Description	Example
Cloud Type	The type of the cloud instance.	apasara_stack
Cloud Name	The name of the cloud instance.	gddgzwy
Region	The region where the cloud instance resides.	cn-qingdao-envxxx
Data Center	The name of the data center.	amtestxx

5. Add a network element.

   i. Click **Add Network Element**. In the Add Network Element panel, configure the parameters.



Add Network Element

Data Center *

Please Select

Device Name *

Role *

Please Select

Custom Role

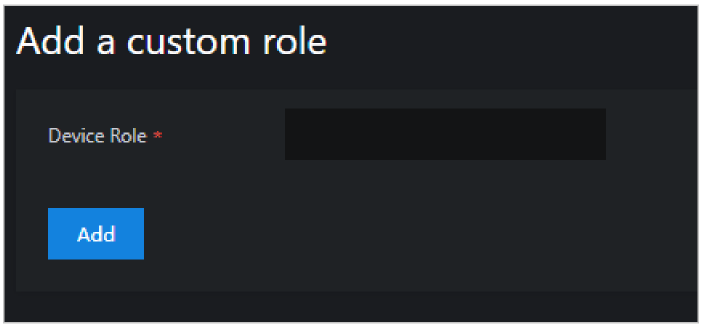
Management IP Address *

SN

Parameter	Description	Example
Data Center	The name of the data center where the network element device is located.	amtest11
Device Name	The name of the network element device.	DSW-VM-G1-P-1.xxxx
Role	The role of the network element device.	ASW
Management IP Address	The management IP address of the network element device.	10.66.1.1
SN	The serial number of the network element device.	FDO23511111
Software Version	The version number of the software run by the network element device.	7.1.070
Release Version	The release version of the network element device.	V200R002C50SPC800
Supplier	The supplier of the network element device.	Ruijie

Parameter	Description	Example
Model	The model of the network element device.	S6510-48VS8CQ

ii. Click **Custom Role** below **Role**. On the **Add a custom role** page, enter a device role name in the **Device Role** search box and click **Add**.



iii. In the **Add Network Element** panel, click **OK** to add the network element.

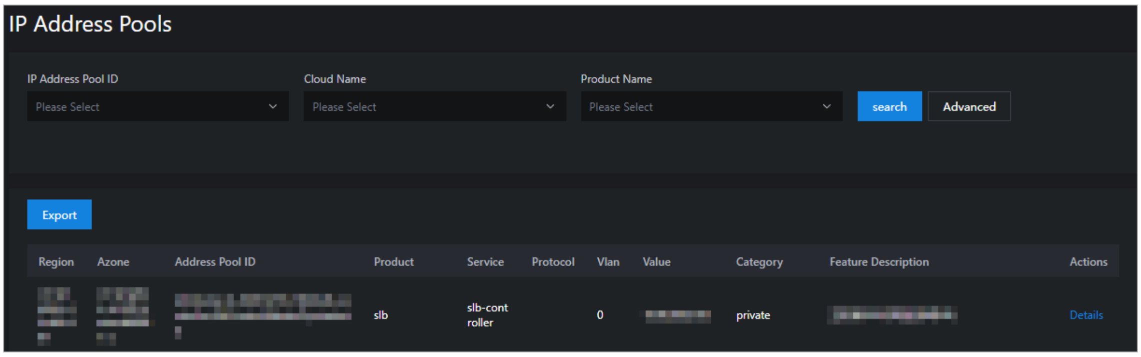
6. Click **Export Table** to download the information about the network element device to your computer.

4.2.2.3. IP address pools

Multiple cloud services may be deployed on a single cloud instance and you may need to view the IP addresses of the cloud services in scenarios such as network changes and security audits. You can view the IP address pool of each cloud service on a cloud instance on the IP Address Pools page.

Procedure

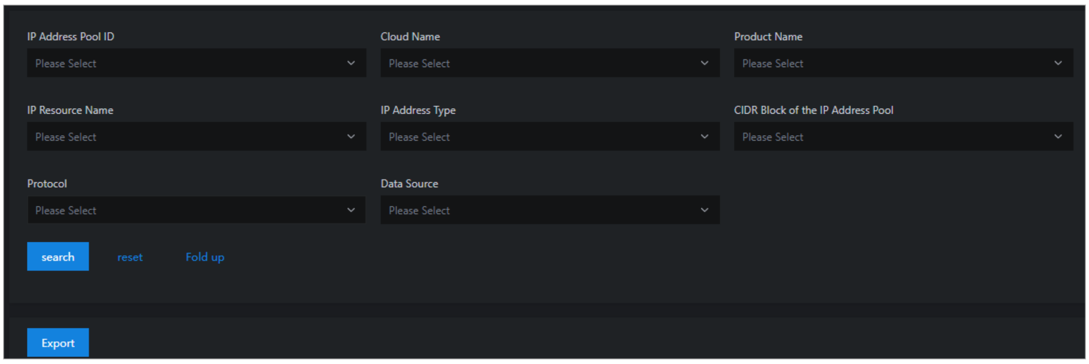
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources** > **Network**.
3. In the left-side navigation pane, choose **Hybrid Cloud Resources** > **IP Address Pools** to view the IP address pools.
   - Select the required options from the **IP Address Pool ID**, **Cloud Name**, and **Product Name** drop-down lists, and click **search** to view the information about the IP address pool.



Region	Azone	Address Pool ID	Product	Service	Protocol	Vlan	Value	Category	Feature Description	Actions
[redacted]	[redacted]	[redacted]	slb	slb-controller		0	[redacted]	private	[redacted]	Details

   - Use more filter conditions to view the information about the IP address pool.

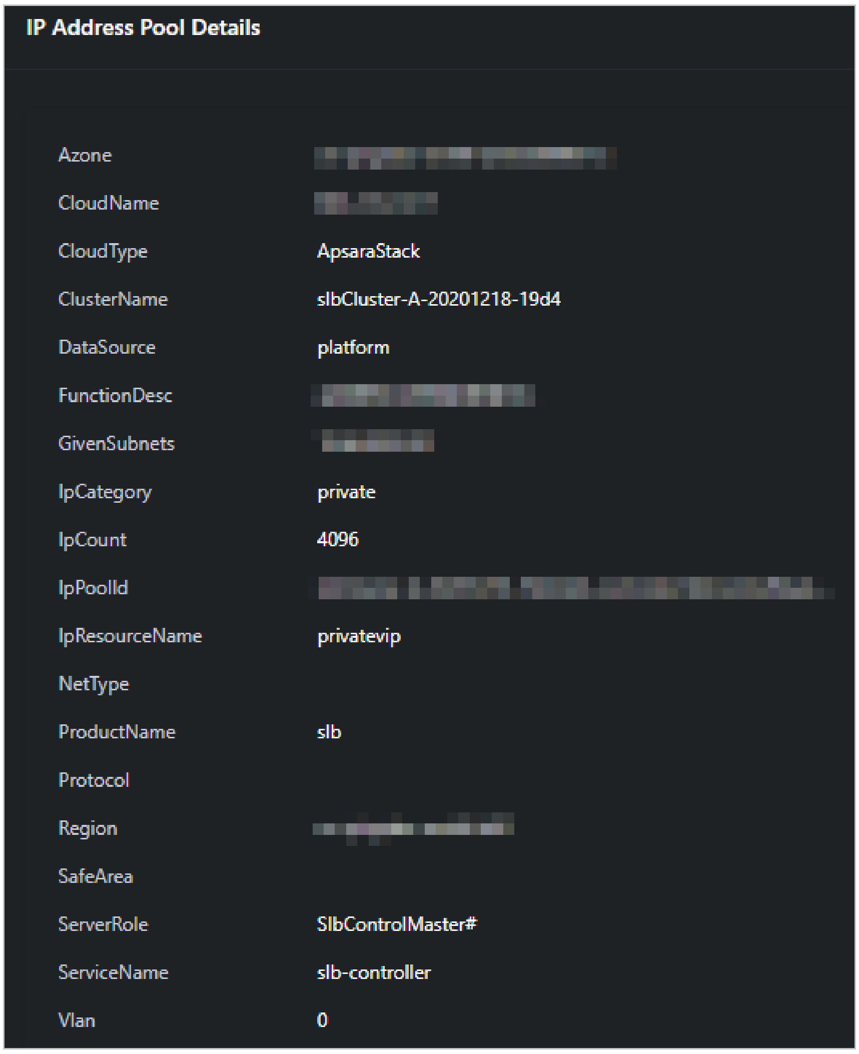
a. Click **Advanced**. Select the required options from the additional **IP Resource Name**, **IP Address Type**, **CIDR Block of the IP Address Pool**, **Protocol**, and **Data Source** drop-down lists, and click **search** to view the information of the IP address pool.



b. (Optional) Click **reset** to clear the filter conditions.

c. (Optional) Click **Fold up** to hide the advanced filter options.

4. Click **Details** in the Actions column to view the details of the IP address pool.



IP Address Pool Details

Azone	[redacted]
CloudName	[redacted]
CloudType	ApsaraStack
ClusterName	slbCluster-A-20201218-19d4
DataSource	platform
FunctionDesc	[redacted]
GivenSubnets	[redacted]
IpCategory	private
IpCount	4096
IpPoolId	[redacted]
IpResourceName	privatevip
NetType	
ProductName	slb
Protocol	
Region	[redacted]
SafeArea	
ServerRole	SlbControlMaster#
ServiceName	slb-controller
Vlan	0

5. Click **Export** to download the information of the IP address pool to your computer.

4.2.3. Network service provider

4.2.3.1. View access gateway instances

You can view the information of access gateway instances, such as the access gateway name, IBGP role, and creation time, on the Instance Management tab.

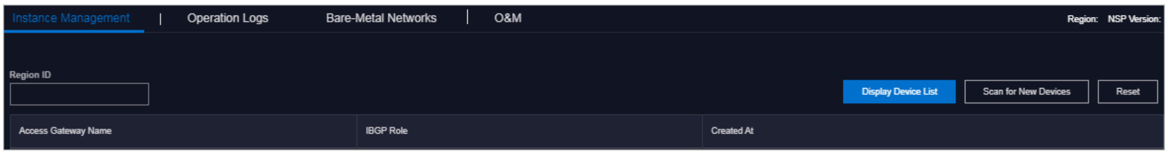
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **Instance Management** tab.
5. Enter the region ID in the upper-left corner.

> **Note** To view the instances in other regions, click **Reset** in the upper-right corner and enter the ID of another region.

6. Click **Display Device List** to view the list of access gateway devices in the current environment.

> **Note** If new devices are added, click **Scan for New Devices** and then click **Display Device List**.



Column	Description
Access Gateway Name	The access gateway name in the current system.
IBGP Role	The role of the access gateway in the environment. Notes: ○ **RR-Active**: indicates that the role of the current gateway device is RR active device. ○ **Client**: indicates that the role of the current gateway is not RR active device.
Management IP Address	The management IP address of the current HSW vSwitch.
Created At	The time when the current vSwitch began to act as an access gateway instance.
Authorization Status	Indicates whether the access gateway instance is authorized.

4.2.3.2. View operation logs

You can view the API operation logs of bare metal instances based on your O&M needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **Operation Logs** tab.
5. Set filter conditions such as vSwitch ID, bare metal instance name, access gateway name, and time range, and click Search to search for the operation logs that meet the filter conditions.

   The following table describes some of the filter conditions.

Filter condition	Description
Vswitch ID	The ID of the vSwitch when the bare metal instance is applied for or released in the VPC.
Bare Metal Name	The name of the bare metal instance that was applied for or released in the VPC. To ensure that the name of the bare metal instance is unique within the region, the serial number of the bare metal instance is used.
Access Gateway Name	The name of the access gateway to query.
Created At	The time range of the API operation to query.

   > **Note** To modify the filter conditions, click **Clear** in the upper-right corner of the tab and set the filter conditions again.

   The following table describes the fields in the query result.

Column	Description
ID	The index of the operation log.
Created At	The time when the operation was performed.

Column	Description
API Operation	The category of the API operation, such as applying for or releasing a bare metal instance in the VPC. Notes: ○ **add** indicates that a bare metal instance is applied for in the VPC. ○ **del** indicates that a bare metal instance is released in the VPC. ○ **del_pc** indicates that a physical connection is deleted. ○ **del_vbr** indicates that a Virtual Border Router (VBR) is deleted. ○ **del_router_intf** indicates that a router interface is deleted. ○ **del_route_entry** indicates that a route table entry is deleted.
Vswitch ID	The ID of the vSwitch when the bare metal instance is applied for or released in the VPC.
Access Gateway Name	The name of the access gateway involved with the current operation.
Port	The port to which the bare metal instance belongs.
Bare Metal Name	The name of the bare metal instance that is applied for or released in the VPC. To ensure that the name of the bare metal instance is unique within the region, the serial number of the bare metal instance is used.
Status	The status of the API operation. **success** indicates that the operation was successful. If the API operation is in progress, the value indicates the real-time status of the API operation. If the API operation is complete but the value is not **success**, you can view the failure information in this column.

6. Find an operation log in the search results and click **View Details** in the **Detail** column to view the details of the API operation.

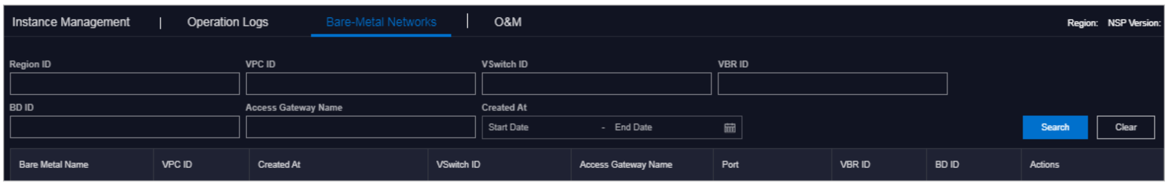
4.2.3.3. View network information of bare metal instances in a VPC

You can view the information of bare metal instancess that are added to a VPC on the Bare-Metal Networks tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **Bare-Metal Networks** tab. By default, the network information of bare metal instances in the current system are displayed by page.

5. Configure the filter conditions such as bare metal instance name, VPC ID, vSwitch ID, VBR ID, BD ID, access gateway name, and time range, and click Search to search for the bare metal instances that meet the filter conditions.



Filter condition	Description
Bare Metal Name	The name of the bare metal instance that was applied for or released in the VPC. To ensure that the name of the bare metal instance is unique within the region, the serial number of the bare metal instance is used.
VPC ID	The ID of the VPC to which the bare metal instance belongs.
Vswitch ID	The ID of the vSwitch to which the bare metal instance belongs.
VBR ID	The VBR ID of the physical connection created on HSW by the VPC to which the bare metal instance belongs.
BD ID	The value of the hardware bridge-domain (BD) to which the bare metal instance is added.
Access Gateway Name	The name of the access gateway to which the bare metal instance belongs.
Created At	The time range within which the bare metal instance is allocated to the VPC.

> **Note** To modify the filter conditions, click **Clear** in the upper-right corner of the tab and configure the filter conditions again.

6. Find a bare metal instance in the search result and click **View Details** in the **Detail** column to view the details of the bare metal instance.

4.2.3.4. O&M configurations

4.2.3.4.1. Apply for a bare metal instance in the VPC

In O&M emergency scenarios, you can use this feature to add the physical port of the access gateway associated with a bare metal instance to the VPC.

Prerequisites

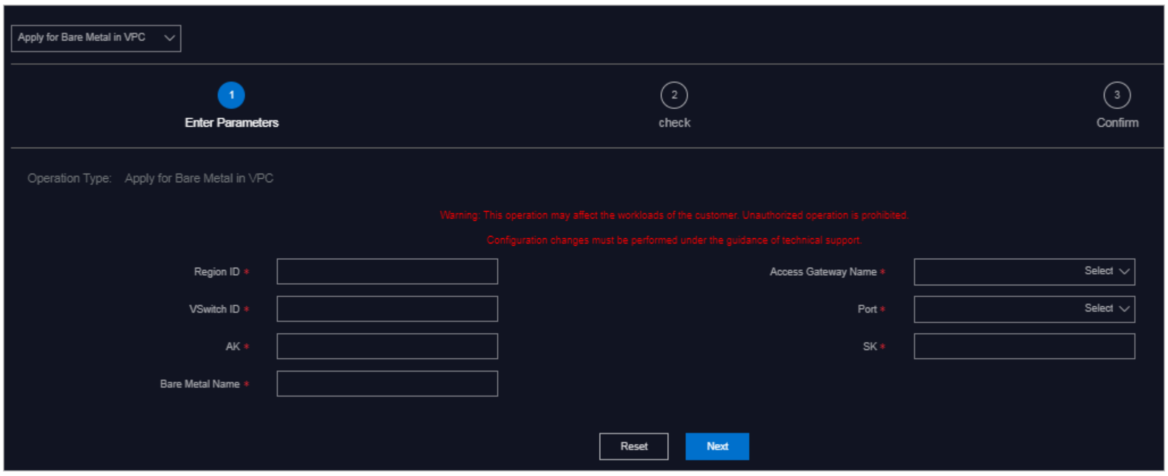
> **Notice** This operation is used only in emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Before you use this feature, take note of the following items:

- Typically, you cannot use this feature to apply for a bare metal instance in the VPC. You can use the bare metal controller to call an API operation to activate the bare metal network.
- This feature can only be used to connect the bare metal instance to the access gateway port but cannot be used to perform operations on the bare metal instance. To configure the network port IP address and routing information of the bare metal instance, contact the corresponding product team for guidance.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **Apply for Bare Metal in VPC** from the drop-down list in the upper-left corner of the tab.



Operation Type: Apply for Bare Metal in VPC

Warning: This operation may affect the workloads of the customer. Unauthorized operation is prohibited.

Configuration changes must be performed under the guidance of technical support.

6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.
Access Gateway Name	Select the name of the access gateway to which the bare metal instance is connected.
Vswitch ID	Enter the ID of the vSwitch to which the bare metal instance is to be added. You can obtain the vSwitch ID from the VPC console.
Port	Select the port of the access gateway to which the bare metal instance is connected.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained from the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VPC belongs.
Bare Metal Name	Enter the name of the bare metal instance. In this case, enter the serial number of the bare metal instance.

> ⓘ **Note** If the specified values are incorrect, click **Reset** in the lower part of the tab and set the parameters again.

7. Click **Next**.
8. Check the information. If the information is correct, click **Confirm**. The svstem starts to push the configurations. After the configurations are pushed, the `Result: Successful` message appears.

   After the configurations are pushed, you can search for the bare metal instance based on the bare metal instance name on the **Bare-Metal Networks** tab. If the bare metal instance is displayed, it is added to the VPC.

4.2.3.4.2. Release a bare metal instance in the VPC

In O&M emergency scenarios, you can use this feature to disconnect the physical port of the bare metal instance from the VPC.

Prerequisites

Before you use this feature, take note of the following items:

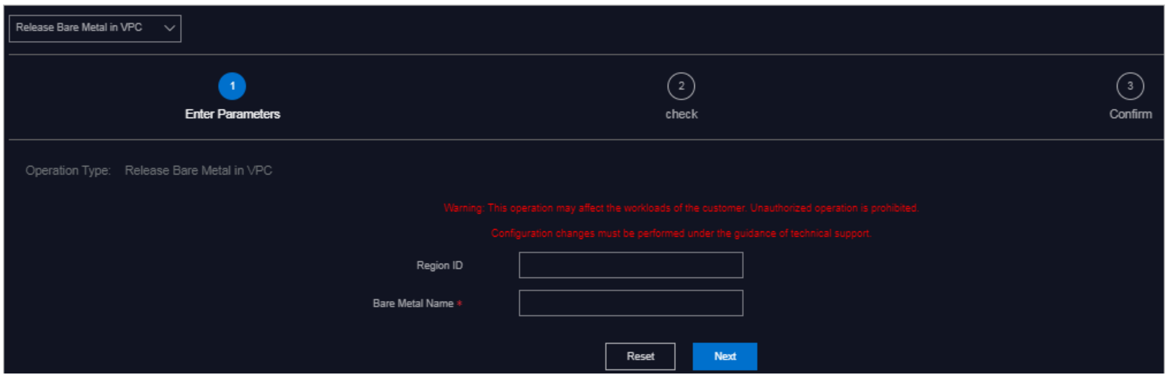
- Typically, you cannot use this feature to release a bare metal instance in the VPC. You can use the bare metal controller to call an API operation to delete the bare metal network.
- This feature can be used only to disconnect the bare metal instance from the access gateway port but cannot be used to perform operations on the bare metal instance. To configure the network port IP address and routing information of the bare metal instance, contact the corresponding product team for guidance.

Context

> **Warning** This operation is used only in emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **Release Bare Metal in VPC** from the drop-down list in the upper-left corner of the tab.



Operation Type: Release Bare Metal in VPC

Warning: This operation may affect the workloads of the customer. Unauthorized operation is prohibited.

Configuration changes must be performed under the guidance of technical support.

Region ID

Bare Metal Name *

6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.
Bare Metal Name	The name of the bare metal instance that you want to release. Enter the serial number of the bare metal instance.

> **Note** If the specified values are incorrect, click **Reset** in the lower part of the tab and set the parameters again.

7. Click **Next**.
8. Check the information. If the information is correct, click **Confirm**. The system starts to push the configurations. After the configurations are pushed, the `Result: Successful` message appears.

   After the configurations are pushed, you can search for the bare metal instance based on the bare metal instance name on the **Bare-Metal Networks** tab. If the bare metal instance is not displayed, it is released.

4.2.3.4.3. Delete a VPC route table entry

In O&M emergency scenarios, you can use the VPC route table entry deletion feature to delete route table entries that point to the bare metal subnet in the VPC.

Prerequisites

Before you use this feature, take note of the following items:

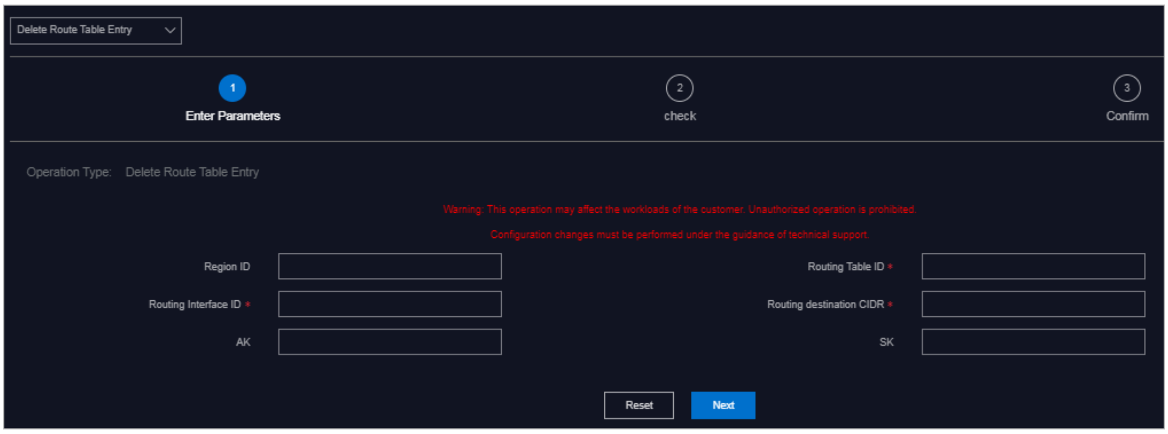
- Typically, you cannot use this feature to delete a VPC route table entry. This operation is used only in emergency situations.
- You can perform this operation to delete only a single route table entry at a time. To delete multiple route table entries, you must perform this operation multiple times.

Context

> **Warning** This operation is used only in emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **Delete Route Table Entry** from the drop-down list in the upper-left corner of the tab.



Operation Type: Delete Route Table Entry

Warning: This operation may affect the workloads of the customer. Unauthorized operation is prohibited.

Configuration changes must be performed under the guidance of technical support.

6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.
Routing Table ID	The VPC route table ID, which can be obtained from the VPC console. For more information about how to obtain the route table ID, see the *VPC User Guide*.
Routing Interface ID	The VPC router interface ID, which can be obtained from the VPC console. For more information about how to obtain the router interface ID, see the *VPC User Guide*.
Routing destination CIDR	The destination CIDR block to which the VPC points, which can be obtained from the VPC console. For more information about how to obtain the routing destination CIDR block, see the *VPC User Guide*.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained from the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VPC belongs.

> Note If the specified values are not correct, click **Reset** in the lower part of the tab and set the parameters again.

7. Click **Next**.
8. Check the information. If the information is correct, click **Confirm**. The system begins to push the configurations. After the configurations have been pushed, the `Result: Successful` message appears.

   After the configurations are pushed, you can log on to the VPC console and view the route table entry of the specified destination CIDR block. If the route table entry is not displayed, it is deleted.
9. (Optional)In actual fault scenarios, if multiple route table entries exist in the VPC route table, repeat Step 3 to Step 6 to delete other route table entries.

4.2.3.4.4. Delete a VBR route table entry

In O&M emergency scenarios, you can use this feature to delete the default route table entry of a VBR.

Context

Warning This operation is only for emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources** > **Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **Delete Route Table Entry** from the drop-down list in the upper-left corner of the tab.
6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.
Routing Table ID	The VBR route table ID. If the bare metal instance involved with the VBR has already been added to the VPC, you can search for the bare metal instance on the **Bare-Metal Networks** tab based on the bare metal instance name, and then click View Details. The VBR Route Table ID in the details is the value of this parameter. If the bare metal instance involved with the VBR is not added to the VPC, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add** on the **Operation Logs** tab. Click **View Details** and the VBR Route Table ID in the details is the value of this parameter.
Routing Interface ID	The VBR router interface ID. If the bare metal instance involved with the VBR has already been added to the VPC, you can search for the bare metal instance on the **Bare-Metal Networks** tab based on the bare metal instance name, and then click View Details. The VBR RI in the details is the value of this parameter. If the bare metal instance involved with the VBR is not added to VPC, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add** on the **Operation Logs** tab. Click View Details and the VBR RI in the details is the value of this parameter.
Routing destination CIDR	Set the value to 0.0.0.0/0.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained from the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VBR belongs.

> Note If the specified values are incorrect, click **Reset** in the lower part of the tab and set the parameters again.

7. Click **Next**.
8. Check the information. If the information is correct, click **Confirm**. The svstem begins to push the configurations. After the configurations are pushed, the `Result: Successful` message appears.

   After the configurations are pushed, you can choose **Products > Product List** in the left-side navigation pane and click **Apsara Network Intelligence**. On the homepage of Apsara Network Intelligence, enter the VBR route table ID and search for the VBR route table. If the route table entry 0.0.0.0/0 does not exist in the VBR route table, the route table entry is deleted.

4.2.3.4.5. Delete a VPC router interface

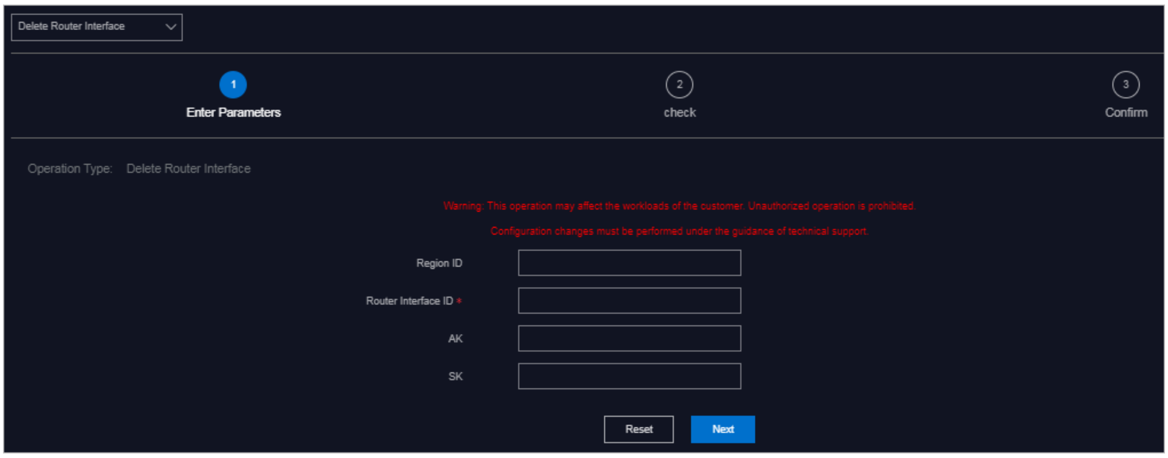
In O&M emergency scenarios, you can use this feature to delete a VPC router interface.

Context

> Warning This operation is only in emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **Delete Router Interface** from the drop-down list in the upper-left corner of the tab.



Operation Type: Delete Router Interface

Warning: This operation may affect the workloads of the customer. Unauthorized operation is prohibited.

Configuration changes must be performed under the guidance of technical support.

Region ID

Router Interface ID *

AK

SK

6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.

Parameter	Description
Router Interface ID	The VPC router interface ID. On the **Operation Logs** tab, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add**. Click **View Details** and the VPC RI in the details is the value of this parameter.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained on the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VPC belongs.

> ⓘ **Note** If the specified values are incorrect, click **Reset** in the lower part of the tab and set the parameters again.

7. Click **Next**.
8. Check the information. If the information is correct, click **Confirm**. The svstem begins to push the configurations. After the configurations are pushed, the `Result: Successful` message appears.

   After the configurations are pushed, you can choose **Products > Product List** in the left-side navigation pane and click **Apsara Network Intelligence**. On the homepage of Apsara Network Intelligence, enter the VPC router interface ID to search for the router interface. If no search result appears, the router interface is deleted.

4.2.3.4.6. Delete a VBR router interface

In O&M emergency scenarios, you can use this feature to delete a VBR router interface.

Context

> **Warning** This operation is only in emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **Delete Router Interface** from the drop-down list in the upper-left corner of the tab.
6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.

Parameter	Description
Router Interface ID	The VBR router interface ID. If the bare metal instance involved with the VBR is added to VPC, you can search for the bare metal instance on the **Bare-Metal Networks** tab based on the bare metal instance name, and then click View Details. The VBR RI in the details is the VBR router interface ID. If the bare metal instance involved with the VBR is not added to VPC, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add** on the **Operation Logs** tab. Click View Details and the VBR RI in the details is the value of this parameter.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained on the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VPC belongs.

> **Note** If the specified values are incorrect, click **Reset** in the lower part of the tab and set the parameters again.

7. Click **Next**.
8. Check the information. If the information is correct, click **Confirm**. The system begins to push the configurations. After the configurations are pushed, the Result: Successful message appears.

   After the configurations are pushed, you can choose **Products** > **Product List** in the left-side navigation pane and click **Apsara Network Intelligence**. On the homepage of Apsara Network Intelligence, enter the VBR router interface ID to search for the router interface. If no search result appears, the router interface is deleted.

4.2.3.4.7. Delete a VBR

In O&M emergency scenarios, you can use the delete VBR feature to delete VBRs.

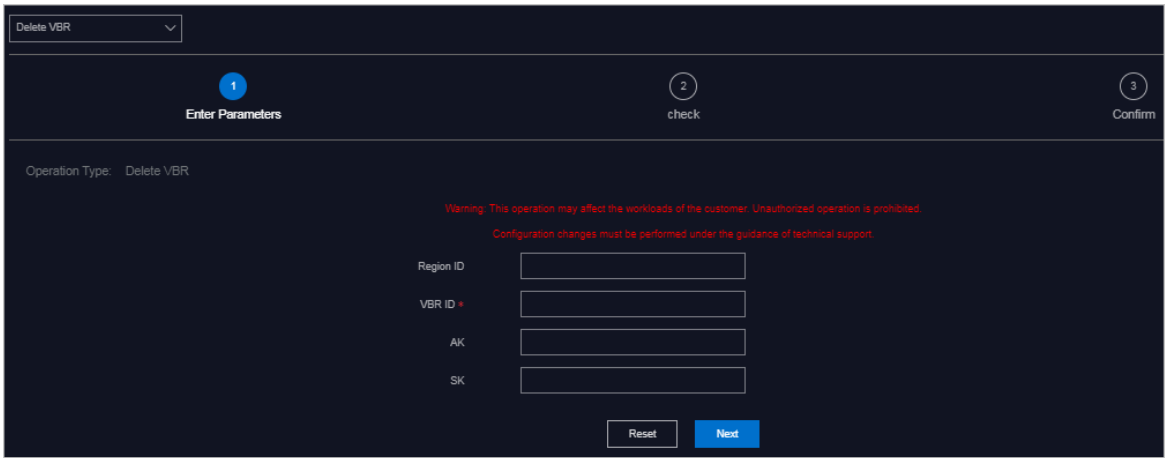
Context

> **Warning** This operation is used only in emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources** > **Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.

5. Select **Delete VBR** from the drop-down list in the upper-left corner of the tab.



Operation Type: Delete VBR

Warning: This operation may affect the workloads of the customer. Unauthorized operation is prohibited.

Configuration changes must be performed under the guidance of technical support.

Region ID

VBR ID *

AK

SK

6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.
VBR ID	The ID of the VBR to delete. On the **Operation Logs** tab, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add**. Click View Details and the VBR ID in the details is the value of this parameter.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained on the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VBR belongs.

> **Note** If the specified values are incorrect, click **Reset** in the lower part of the tab and set the parameters again.

7. Click **Next**.

8. Check the information. If the information is correct, click **Confirm**. The svstem begins to push the configurations. After the configurations are pushed, the `Result: Successful` message appears.

   After the configurations are pushed, you can choose **Products > Product List** in the left-side navigation pane and click **Apsara Network Intelligence**. On the homepage of Apsara Network Intelligence, enter the VBR ID to search for the VBR. If no search result appears, the VBR is deleted.

4.2.3.4.8. Delete a physical connection

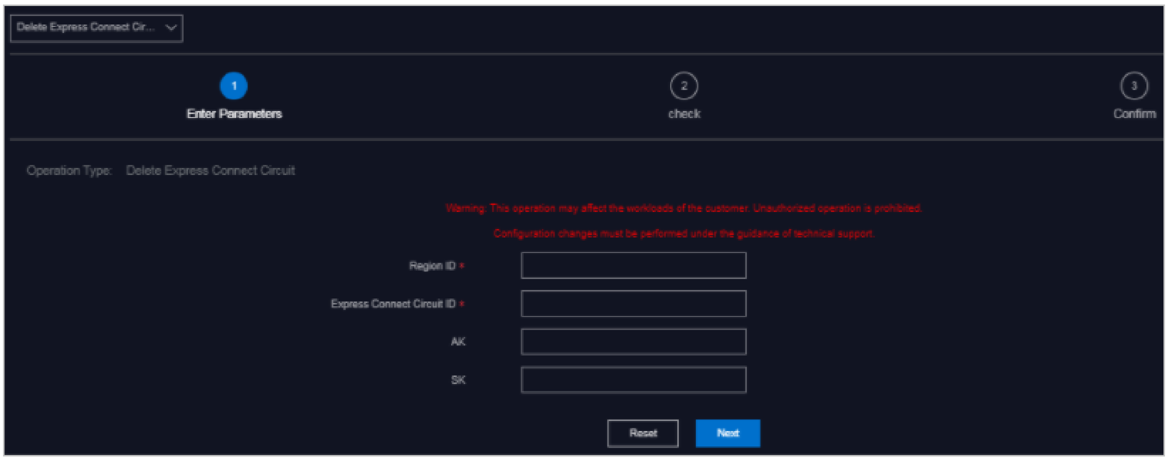
In O&M emergency scenarios, you can use this feature to delete a physical connection.

Context

> **Warning** This operation is used only in emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **Delete Express Connect Circuit** from the drop-down list in the upper-left corner of the tab.



Operation Type: Delete Express Connect Circuit

Warning: This operation may affect the workloads of the customer. Unauthorized operation is prohibited.

Configuration changes must be performed under the guidance of technical support.

6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.
Express Connect Circuit ID	The ID of the physical connection to be deleted. On the **Operation Logs** tab, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add**. Click **View Details** and the Express Connect Circuit ID in the details is the value of this parameter.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained on the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VBR belongs.

> **Note** If the specified values are incorrect, click **Reset** in the lower part of the tab and configure the parameters again.

7. Click **Next**.
8. Check the information. If the information is correct, click **Confirm**. The system begins to push the configurations. After the configurations are pushed, the `Result: Successful` message appears.

   After the configurations are pushed, you can choose **Products > Product List** in the left-side navigation pane and click **Apsara Network Intelligence**. On the homepage of Apsara Network Intelligence, enter the physical connection ID to search for the physical connection. If no search result appears, the physical connection is deleted.

4.2.3.4.9. Delete all resources

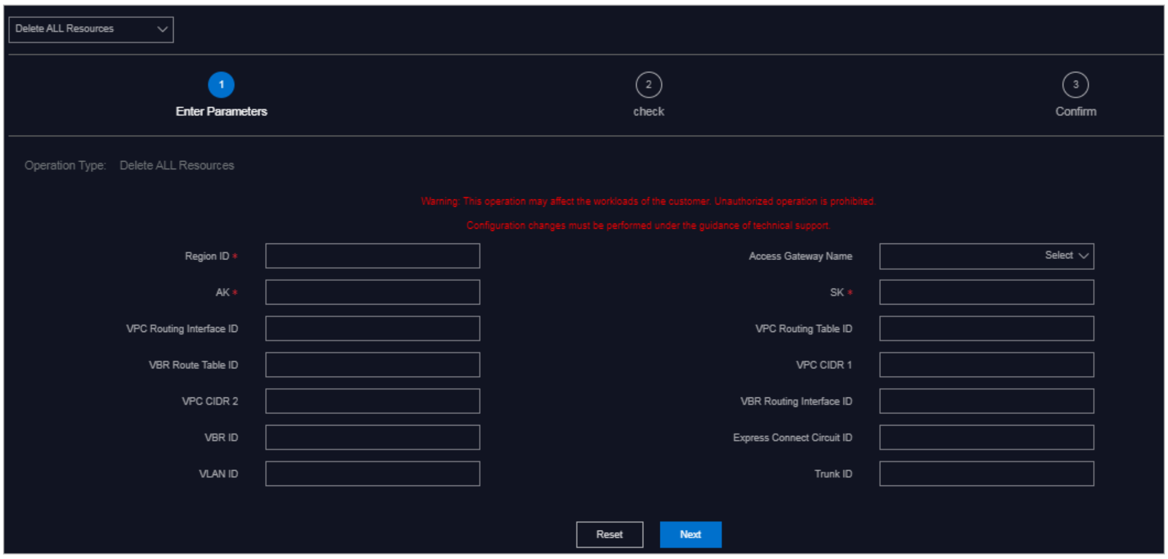
In O&M emergency scenarios, you can use this feature to delete all resources, including the VPC route table entries, VBR route table entries, VPC router interfaces, VBR router interfaces, VBRs, and physical connections.

Context

> **Warning** This operation is only for emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **Delete ALL Resources** from the drop-down list in the upper-left corner of the tab.



Operation Type: Delete ALL Resources

Warning: This operation may affect the workloads of the customer. Unauthorized operation is prohibited.

Configuration changes must be performed under the guidance of technical support.

6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.
Access Gateway Name	The name of the access gateway to which the bare metal instance is connected.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained from the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VBR belongs.

Parameter	Description
VPC Routing Interface ID	The VPC router interface ID, which can be obtained from the VPC console. For more information about how to obtain the VPC router interface ID, see the *VPC User Guide*.
VPC Routing Table ID	The VPC route table ID, which can be obtained from the VPC console. For more information about how to obtain the VPC route table ID, see the *VPC User Guide*.
VBR Route Table ID	The VBR route table ID. If the bare metal instance involved with the VBR has already been added to the VPC, you can search for the bare metal instance on the **Bare-Metal Networks** tab based on the bare metal instance name, and click **View Details**. The VBR Route Table ID in the details is the value of this parameter. If the bare metal instance involved with the VBR is not added to VPC, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add** on the **Operation Logs** tab. Click **View Details** and the VBR Route Table ID in the details is the value of this parameter.
CPC CIDR1	The destination CIDR block 1 to which the VPC points, which can be obtained from the VPC console. For more information about how to obtain the VPC CIDR block 1, see the *VPC User Guide*.
VPC CIDR2	The destination CIDR block 2 to which the VPC points, which can be obtained from the VPC console. For more information about how to obtain the VPC CIDR block 2, see the *VPC User Guide*.
VBR Routing Interface ID	The VBR router interface ID. If the bare metal instance involved with the VBR has already been added to the VPC, you can search for the bare metal instance on the **Bare-Metal Networks** tab based on the bare metal instance name, and then click **View Details**. The VBR RI in the details is the value of this parameter. If the bare metal instance involved with the VBR is not added to VPC, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add** on the **Operation Logs** tab. Click **View Details** and the VBR RI in the details is the value of this parameter.
VBR ID	The ID of the VBR to be deleted. On the **Operation Logs** tab, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add**. Click **View Details** and the VBR ID in the details is the value of this parameter.

Parameter	Description
Express Connect Circuit ID	The ID of the physical connection to be deleted. On the **Operation Logs** tab, specify the bare metal instance name and creation time to search for the operation logs and find an operation log whose **API Operation** is **add**. Click **View Details** and the Express Connect Circuit ID in the details is the value of this parameter.
Trunk ID	This parameter is not required.

> **Note** If the specified values are incorrect, click **Reset** in the lower part of the tab and configure the parameters again.

7. Click **Next**.
8. Check the information. If the information is correct, click **Confirm**. The svstem starts to push the configurations. After the configurations are pushed, the `Result: Successful` message appears.

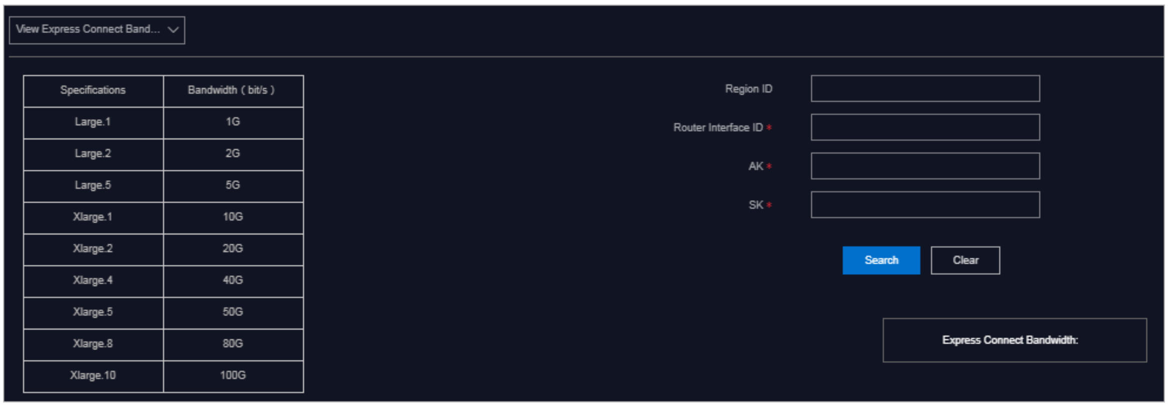
   After the configurations are pushed, use the methods provided in Delete a VPC route table entry, Delete a VBR route table entry, Delete a VPC router interface, Delete a VBR router interface, Delete a VBR, and Delete a physical connection to check whether the VPC route table entries, VBR route table entries, VPC router interfaces, VBR router interfaces, VBRs, and physical connections are deleted.

4.2.3.4.10. View the physical connection bandwidth

You can view the physical connection bandwidth when the access gateway is connected to a VPC in the system based on your O&M needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources** > **Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **View Express Connect Bandwidth** from the drop-down list in the upper-left corner.



Specifications	Bandwidth (bit/s)
Large.1	1G
Large.2	2G
Large.5	5G
Xlarge.1	10G
Xlarge.2	20G
Xlarge.4	40G
Xlarge.5	50G
Xlarge.8	80G
Xlarge.10	100G

6. Configure the filter conditions and click **Search**.

Parameter	Description
Region ID	The name of the region in the current environment.
Router Interface ID	The VBR router interface ID. On the **Bare-Metal Networks** tab, specify the VPC ID and access gateway name, and click View Details. VBR RI is the value of this parameter.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained on the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VBR belongs.

The information of the physical connection bandwidth that meets the filter conditions is displayed.

The bandwidth information describes the specifications of the physical connection bandwidth on the HSW of the current VPC. View the table on the left and obtain the bandwidth (bit/s) based on the specification.

4.2.3.4.11. Modify the physical connection bandwidth

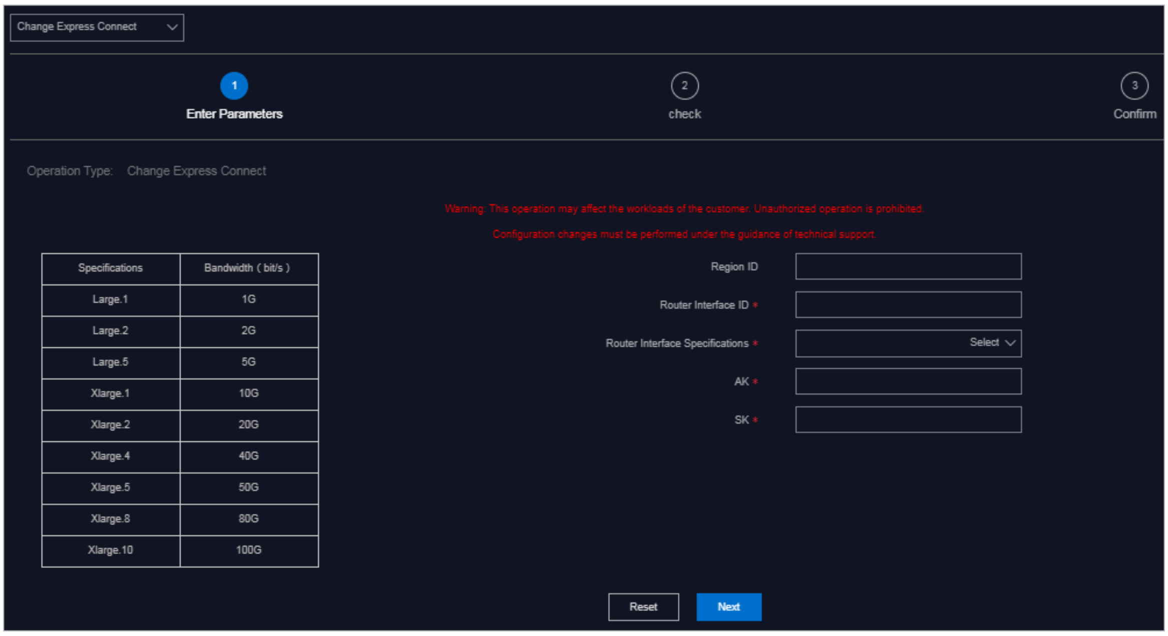
In O&M emergency scenarios, you can use this feature to modify the physical connection bandwidth.

Context

> **Warning** This operation is used only in emergency situations and must be performed under the guidance of technical personnel. Otherwise, normal business operations may be affected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **Change Express Connect** from the drop-down list in the upper-left corner.



Change Express Connect

Operation Type: Change Express Connect

Warning: This operation may affect the workloads of the customer. Unauthorized operation is prohibited.

Configuration changes must be performed under the guidance of technical support.

Specifications	Bandwidth（bit/s）
Large.1	1G
Large.2	2G
Large.5	5G
Xlarge.1	10G
Xlarge.2	20G
Xlarge.4	40G
Xlarge.5	50G
Xlarge.8	80G
Xlarge.10	100G

Region ID

Router Interface ID *

Router Interface Specifications * Select

AK *

SK *

6. Configure the parameters described in the following table.

Parameter	Description
Region ID	The name of the region in the current environment.
Router Interface ID	The ID of the router interface to which the physical connection bandwidth to be modified corresponds. On the **Bare-Metal Networks** tab, specify the VPC ID and access gateway name to search for the bare metal. Click **View Details** and the VBR RI in the details is the value of this parameter.
Router Interface Specifications	The specification of the physical connection bandwidth.
AK and **SK**	The organization AccessKey ID and AccessKey secret, which can be obtained from the **Organizations** page of the Apsara Uni-manager Management Console based on the organization to which the VPC belongs.

> Note If the specified values are incorrect, click **Reset** in the lower part of the tab and configure the parameters again.

7. Click **Next**.

8. Check the information. If the information is correct, click **Confirm**. The svstem starts to push the configurations. After the configurations are pushed, the `Result: Successful` message appears.

   After the configurations are pushed, check whether the physical connection bandwidth has been modified. Form more information, see View the physical connection bandwidth.

4.2.3.4.12. View BD usage

You can view BD usage to learn about the BD configuration distribution in a timely manner.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **View BD Usage** from the drop-down list in the upper-left corner.
6. Configure the filter conditions and click **Search**.

4.2.3.4.13. View BM VPN usage

You can view the information of the BM VPN that is assigned to the access gateway instance.

Procedure

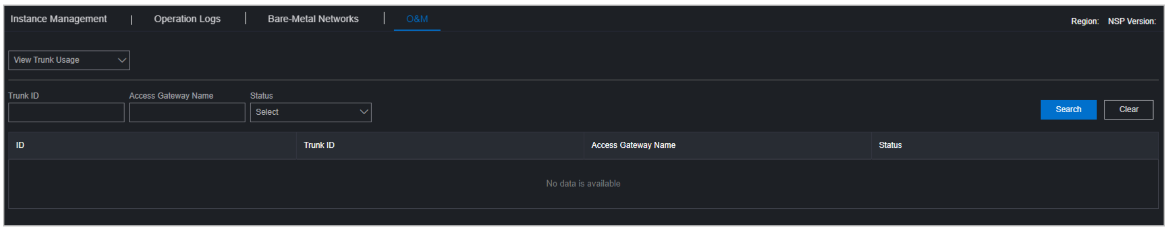
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Specify **Access Gateway Name**, **vxlan id**, and **BM VPN Name**, select a state from the **Status** drop-down list, and then click **Search** to view the BM VPNs assigned to all the HSW vSwitches.

4.2.3.4.14. View trunk usage

You can view trunk usage to learn about the usage of hardware ports in a timely manner.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Network**.
3. In the left-side navigation pane, click **Network Service Provider**.
4. Click the **O&M** tab.
5. Select **View Trunk Usage** from the drop-down list in the upper-left corner.



6. Specify the trunk ID and access gateway name, select a trunk state, and then click **Search**. The Trunk Status options include Idle, Used, Creating, and Deleting.

   Set **Trunk ID** to the last integer of the **Port** value that is obtained from the **Bare-Metal Networks** tab. For example, if the port number is 10GE1/0/40, set **Trunk ID** to 40.

Note To modify the filter conditions, click **Clear** in the upper-right corner and set the filter conditions again.

4.3. Data centers

Operations personnel can monitor and view the physical servers where products are located.

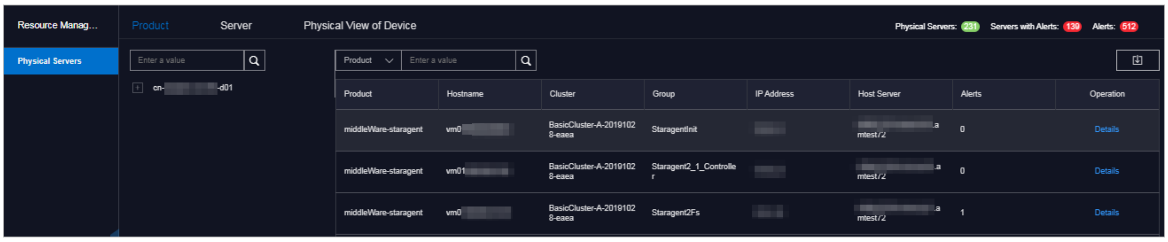
4.3.1. View the physical server information

This topic describes how to view the physical server list and the details of physical servers.

Go to the Data Centers page

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Data Centers**.

   The **Product** tab appears. In the upper-right corner of the tab, the numbers of existing physical servers, servers with alerts, and alerts are displayed.



Physical Servers: 231 Servers with Alerts: 139 Alerts: 512

Product	Hostname	Cluster	Group	IP Address	Host Server	Alerts	Operation
middleWare-staragent	vm0[redacted]	BasicCluster-A-20191028-eaea	StaragentInit	[redacted]	[redacted].a mtest/2	0	Details
middleWare-staragent	vm01[redacted]	BasicCluster-A-20191028-eaea	Staragent2_1_Controller	[redacted]	[redacted].a mtest/2	0	Details
middleWare-staragent	vm0[redacted]	BasicCluster-A-20191028-eaea	Staragent2Fs	[redacted]	[redacted].a mtest/2	1	Details

Product tab

1. On the Product tab, perform the following operations to view the physical server information:
   - Expand the left-side navigation tree by selecting a region, a product, and a cluster in sequence to view the list of physical servers where a cluster of a service is located.
   - In the left-side search box, enter the product name, cluster name, group name, or hostname to search for the corresponding node.
   - In the right-side search box, search for physical servers by product, cluster, group, or hostname, and view the details of a physical server.
   - Select a product and click **Details** in the **Actions** column. On the **Physical Server Details** page, you can view the basic information, monitoring details, and alert information of the physical server to which the product belongs.

     You can switch the tab to view the monitoring details and alert information.

     Monitoring details include the CPU usage, system load, disk usage, memory usage, network throughput, and disk I/O. When you view the monitoring details, you can select a monitoring item in the upper-right corner of each monitoring graph and select a time range to view the monitoring value within the time range.

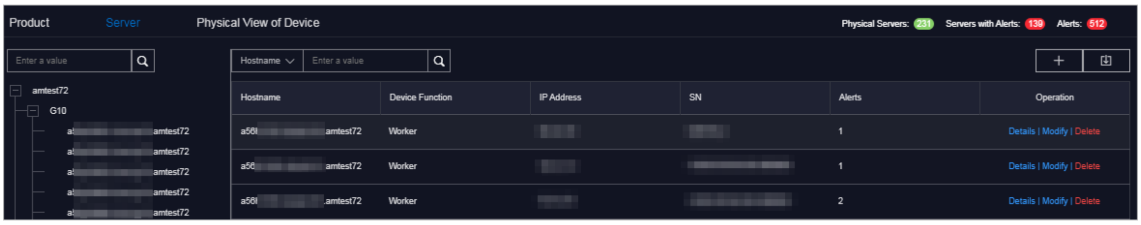
     In the upper-right corner of the CPU usage, system load, disk usage, memory usage, network throughput, and disk I/O sections, you can perform the following operations:

     - Click the ⛶ icon to view the monitoring graph in full screen.

- Click the icon to download the monitoring graph to your computer.
- Click the icon to manually refresh the monitoring data.
- Click the icon. The icon turns green. The system automatically refreshes the monitoring data every 10 seconds. To disable the auto-refresh feature, click the icon again.

Server tab

1. Click the **Server** tab.
2. On the Server tab, perform the following operations to view the physical server list:
    - Expand the left-side navigation tree by selecting an IDC and a rack in sequence to view the physical server list in a rack.
    - Enter a rack name in the left-side search box and press the Enter key or click to search for and view the list of all the physical servers in the rack.



Hostname	Device Function	IP Address	SN	Alerts	Operation
a56[redacted]amtest72	Worker	[redacted]	[redacted]	1	Details | Modify | Delete
a56[redacted]amtest72	Worker	[redacted]	[redacted]	1	Details | Modify | Delete
a56[redacted]amtest72	Worker	[redacted]	[redacted]	2	Details | Modify | Delete

3. To view the details of a physical server, enter the hostname, IP address, device role, or serial number (SN) in the right-side search box and press the Enter key.
4. Find the physical server whose details you want to view and click **Details** in the **Actions** column. On the **Physical Server Details** page, view the basic information, monitoring details, and alert information of the physical server.

    You can switch the tab to view the monitoring details and alert information.

    Monitoring details includes the CPU usage, system load, disk usage, memory usage, network throughput, and disk I/O. When you view the monitoring details, you can select a monitoring item in the upper-right corner of each monitoring graph and then select a time range to view the monitoring value within the time range.

    In the upper-right corner of the CPU usage, system load, disk usage, memory usage, network throughput, and disk I/O sections, you can perform the following operations:

    - Click the icon to view the monitoring graph in full screen.
    - Click the icon to download the monitoring graph to your computer.
    - Click the icon to manually refresh the monitoring data.
    - Click the icon. The icon turns green. The system automatically refreshes the monitoring data in 10 second intervals. To disable the auto-refresh feature, click the icon again.

Physical View of Device tab

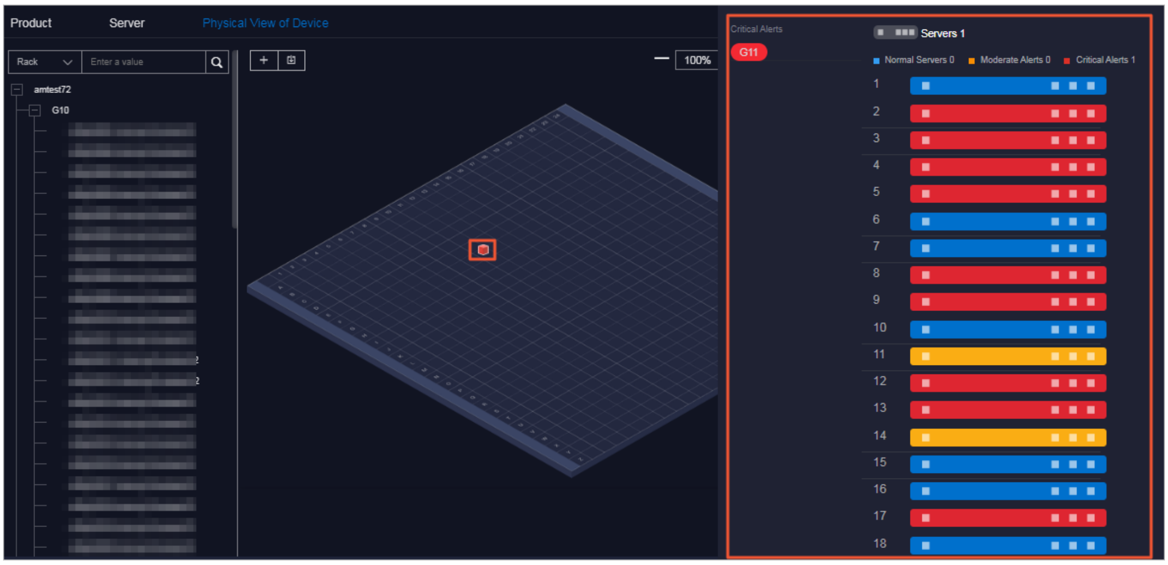
1. Click the **Physical View of Device** tab.

2. On the **Physical View of Device** tab, expand the left-side hierarchy tree by selecting an IDC and a rack in sequence to view the corresponding rack information on the right. In addition, the rack details panel appears on the right side of the tab and shows the server information of the rack.

   Racks and servers are displayed in different colors to indicate the alert condition of servers:

   - Red indicates a critical alert.
   - Orange indicates a moderate alert.
   - Blue indicates that the physical server is normal.

   In the upper-right corner, you can view the alert legend. By default, the check box on the left of the legend is selected, indicating that the information of racks or servers of this alert type is displayed on the rack graph or in the rack details panel. Clear the check box on the left of a legend to hide the information of racks or servers of this alert type on the rack graph or in the rack details panel.

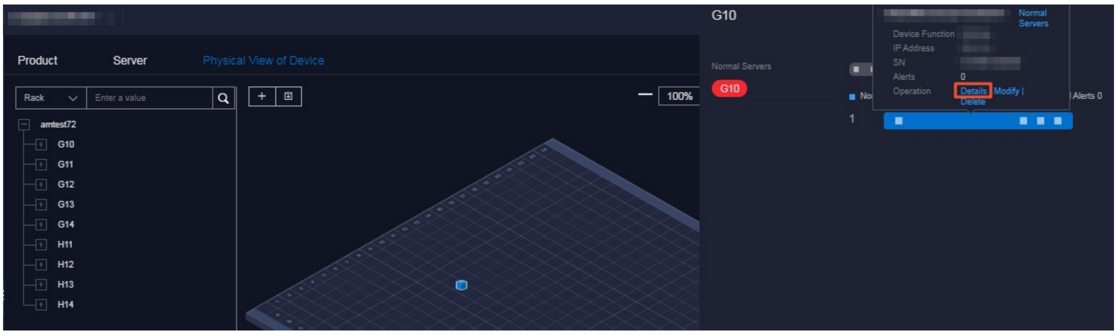


3. To view the details of a physical server, perform the following operations:

   i. Find the physical server whose details you want to view in the left-side navigation tree or rack graph on the right side of the tab.

   ii. In the rack details panel, click the color block of a server to view the basic information of the server.

   iii. Click **Details** in the **Operation** section of the basic information.



iv. On the **Physical Server Details** page, view the basic information, monitoring details, and alert information of the physical server.

You can switch the tab to view the monitoring details and alert information.

Monitoring details includes the CPU usage, system load, disk usage, memory usage, network throughput, and disk I/O. When you view the monitoring details, you can select a monitoring item in the upper-right corner of each monitoring graph and then select a time range to view the monitoring value within the time range.

In the upper-right corner of the CPU usage, system load, disk usage, memory usage, network throughput, and disk I/O sections, you can perform the following operations:

- Click the ⛶ icon to view the monitoring graph in full screen.
- Click the ⤓ icon to download the monitoring graph to your computer.
- Click the ⟳ icon to manually refresh the monitoring data.
- Click the ⟳ icon. The icon turns green. The system automatically refreshes the monitoring data in 10 second intervals. To disable the auto-refresh feature, click the icon again.

4.3.2. Add a physical server

Operations personnel can add the existing physical servers in an environment to the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Data Centers**.
3. Click the **Server** or **Physical View of Device** tab.
4. In the upper-right corner of the **Server** tab or the upper-left corner of the **Physical View of Device** tab, click the + icon.
5. In the **Add Physical Server** pane, configure the parameters.

   The following table describes the parameters.

Parameter	Description
Zone	The zone where to add the physical server.
Data Center	The data center where to add the physical server.
Rack	The rack where to add the physical server.
Room	The room where to add the physical server.
Physical Server Name	The name of the physical server.
Memory	The memory size of the physical server.

Parameter	Description
Disk Size	The disk size of the physical server.
CPU Cores	The number of CPU cores of the physical server.
Rack Group	The rack group to which the physical server belongs.
Server Type	The type of the physical server.
Server Role	The feature or purpose of the physical server.
Serial Number	The serial number (SN) of the physical server.
Operating System Template	The template used by the operating system of the physical server.
IP Address	The IP address of the physical server.

6. Click **OK**.

4.3.3. Modify a physical server

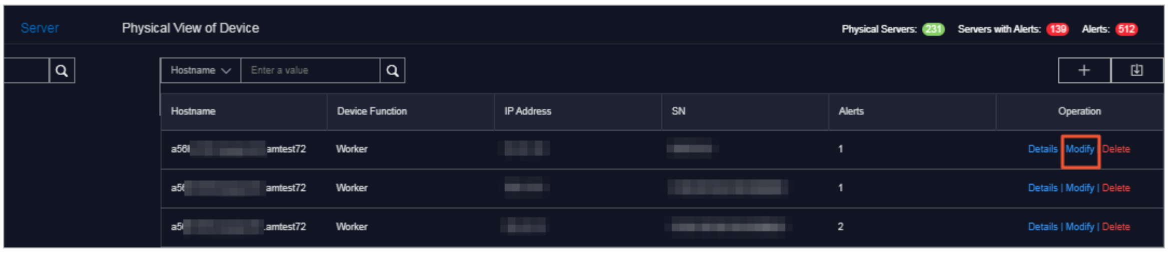
You can modify the physical server information in the Apsara Uni-manager Management Console when the information is changed in the Apsara Stack environment.

Go to the Data Centers page

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Data Centers**.

Server tab

1. Click the **Server** tab.
2. (Optional)In the right-side search box, search for the physical server that you want to modify by hostname, IP address, device role, or serial number (SN).
3. Find the physical server and click **Modify** in the **Operation** column.



Hostname	Device Function	IP Address	SN	Alerts	Operation
a56[redacted]amtest72	Worker	[redacted]	[redacted]	1	Details Modify Delete
a5[redacted]amtest72	Worker	[redacted]	[redacted]	1	Details | Modify | Delete
a5[redacted]amtest72	Worker	[redacted]	[redacted]	2	Details | Modify | Delete

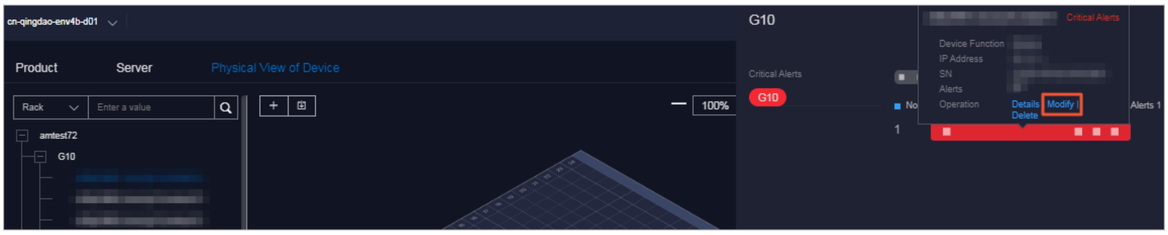
4. In the **Modify Physical Server** panel, modify the physical server information. You can modify the following physical server information: zone, data center, rack, room, physical server name, memory size, disk size, number of CPU cores, rack group, server type, server role, serial number, operating system template, and IP address.
5. Click **OK**.

Physical View of Device tab

1. Click the **Physical View of Device** tab.
2. Expand the left-side navigation tree by selecting an IDC and a rack in sequence to find the physical server that you want to modify.

   > **Note** In the left-side search box, you can also search for the physical server by rack, hostname, IP address, device role, SN, or IDC.

3. In the rack details panel, click the color block of a server to view the basic information of the server.
4. Click **Modify** in the **Operation** row of the basic information.



5. In the **Modify Physical Server** panel, modify the physical server information. You can modify the following physical server information: zone, data center, rack, room, physical server name, memory size, disk size, number of CPU cores, rack group, server type, server role, serial number, operating system template, and IP address.
6. Click **OK**.

4.3.4. Export server information

You can export the information of all physical servers within the system for offline viewing.

Go to the Data Centers page

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources** > **Data Centers**.

Product tab

The physical server information exported from the **Product** tab includes the zone, hostname, disk size, number of CPU cores, memory size, information about the data center (data center, rack, room, and rack group), model, device role, serial number, operating system template, IP address, out-of-band IP address, CPU architecture, host server, alerts, region, product, cluster, service role group, and capacity and performance usage (CPU usage, system load, disk usage, memory usage, network throughput, and disk I/O).

1. In the upper-right corner of the tab, click the icon to export the information of all the physical servers of all services to your computer.

Server or Physical View of Device tab

The physical server information exported from the **Server** or **Physical View of Device** tab includes the zone, hostname, disk size, number of CPU cores, memory size, information about the data center (data center, rack, room, and rack group), model, device role, serial number, operating system template, IP address, out-of-band IP address, CPU architecture, alerts, and capacity and performance usage (CPU usage, system load, disk usage, memory usage, network throughput, and disk I/O).

1. Click the **Server** or **Physical View of Device** tab.
2. In the upper-right corner of the **Server** tab, click the ⊡ icon to export all the information of physical servers to your computer.
3. In the upper part of the **Physical View of Device** tab, click the ⊡ icon to export all the information of physical servers to your computer.

4.3.5. Delete a physical server

This topic describes how to delete physical servers that no longer need to be monitored.

Go to the Data Centers page

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Data Centers**.

Server tab

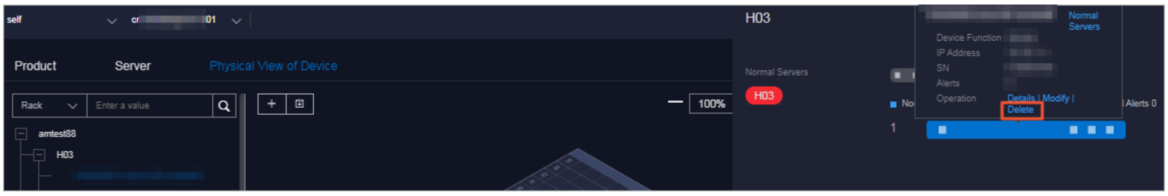
1. Click the **Server** tab.
2. (Optional)In the right-side search box, search for the physical server that you want to delete by hostname, IP address, device role, or serial number (SN).
3. Find the physical server and click **Delete** in the **Operation** column.
4. In the message that appears, click **OK**.

Physical View of Device tab

1. Click the **Physical View of Device** tab.
2. Expand the left-side hierarchy tree tree by selecting an IDC and a rack in sequence to find the physical server that you want to delete.

> **Note** In the left-side search box, you can also search for the physical server that you want to delete by rack, hostname, IP address, device role, SN, or IDC.

3. In the rack details panel that appears, click the color block of a server to view the basic information of the server.
4. Click **Delete** in the **Operation** section of the basic information.



5. In the message that appears, click **OK**.

4.4. Full stack

The Full Stack Monitoring module allows you to perform aggregate queries for system alert events. You can query all end-to-end alert data by host IP address, instance ID, and time range, as well as view the end-to-end topology.

4.4.1. SLA

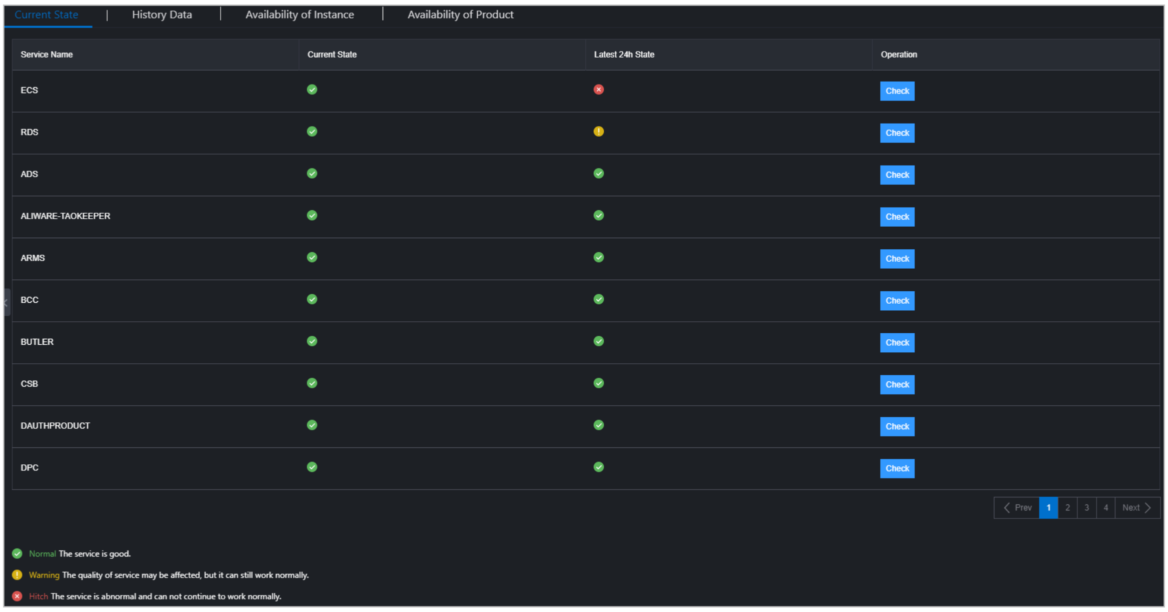
The **SLA** module allows you to view the current state, historical data, instance availability, and product availability of each cloud product. You can view the current status and historical data of a product to obtain the SLA values and unavailability events of product instances for a period of time.

4.4.1.1. View the current status of a cloud service

You can view the current status of a cloud service and the details of exception events on the Current State tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Full Stack**.
3. The **Current State** tab appears.



Service Name	Current State	Latest 24h State	Operation
ECS	✓	✗	Check
RDS	✓	!	Check
ADS	✓	✓	Check
ALIWARE-TAOKEEPER	✓	✓	Check
ARMS	✓	✓	Check
BCC	✓	✓	Check
BUTLER	✓	✓	Check
CSB	✓	✓	Check
DAUTHPRODUCT	✓	✓	Check
DPC	✓	✓	Check

✓ Normal The service is good.

! Warning The quality of service may be affected, but it can still work normally.

✗ Hitch The service is abnormal and can not continue to work normally.

The current status and the statuses within the last 24 hours of each cloud service are displayed on this tab. Services in different states are displayed in different colors:

- Green: normal. The service is running normally.
- Yellow: warning. The service has some latency, but can still run normally.
- Red: faulty. The service is temporarily interrupted and cannot run normally.

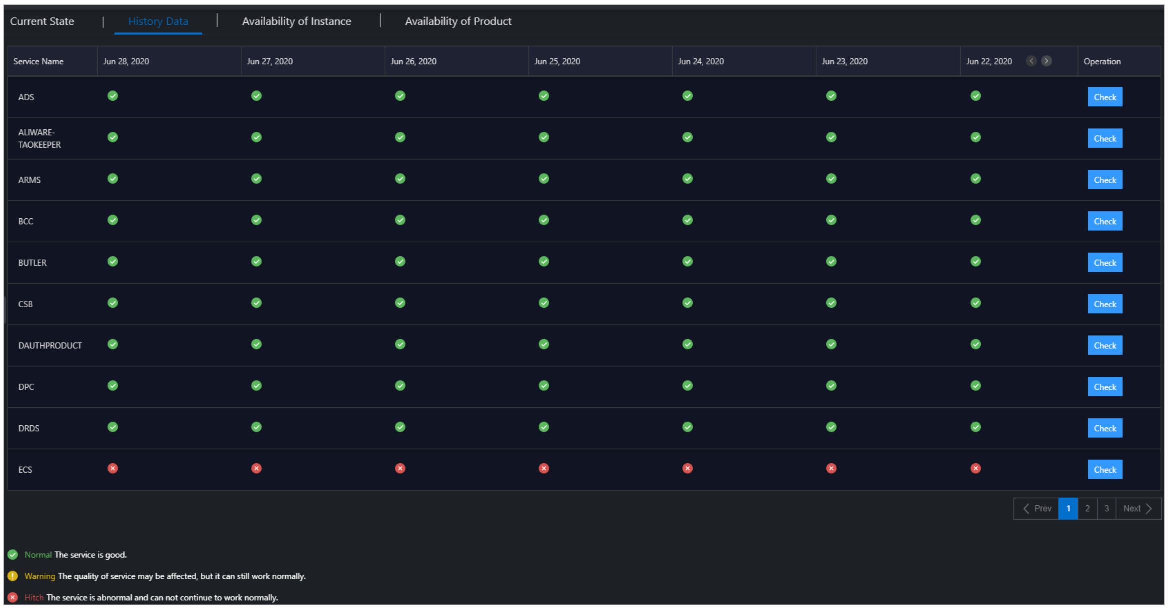
4. Find the service whose running status you want to view, and click **Check** in the Operation column.
   - The **Overall Availability** section shows the availability of the service. You can view the availability by minute, hour, or day.
   - The **Related Events** section shows the current exception events. Click **Show Details** corresponding to an event to view the event details.

4.4.1.2. View the history data of a cloud service

On the History Data tab, you can view the history status of a cloud service and the details of exception events.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Full Stack**.
3. Click the **History Data** tab.



Service Name	Jun 28, 2020	Jun 27, 2020	Jun 26, 2020	Jun 25, 2020	Jun 24, 2020	Jun 23, 2020	Jun 22, 2020	Operation
ADS	✓	✓	✓	✓	✓	✓	✓	Check
ALIWARE-TAOKEEPER	✓	✓	✓	✓	✓	✓	✓	Check
ARMS	✓	✓	✓	✓	✓	✓	✓	Check
BCC	✓	✓	✓	✓	✓	✓	✓	Check
BUTLER	✓	✓	✓	✓	✓	✓	✓	Check
CSB	✓	✓	✓	✓	✓	✓	✓	Check
DAUTHPRODUCT	✓	✓	✓	✓	✓	✓	✓	Check
DPC	✓	✓	✓	✓	✓	✓	✓	Check
DRDS	✓	✓	✓	✓	✓	✓	✓	Check
ECS	✗	✗	✗	✗	✗	✗	✗	Check

✓ Normal The service is good.

! Warning The quality of service may be affected, but it can still work normally.

✗ Hitch The service is abnormal and can not continue to work normally.

The service availability of each service in the last two weeks is displayed on this tab. Services in different states are displayed in different colors:

- Green: normal. The service is running normally.
- Yellow: warning. The service has some latency, but still can work normally.
- Red: faulty. The service is temporarily interrupted and cannot work normally.

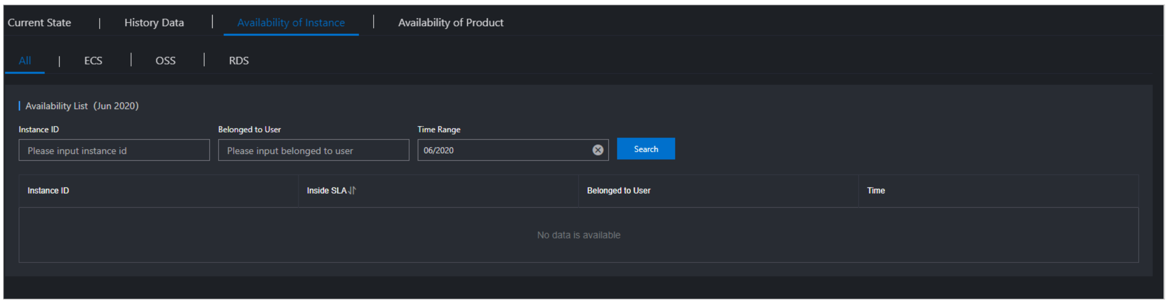
4. Find the service whose history status you want to view and click **Check** in the Operation column.
   - The **Overall Availability** section shows the historical availability of the service. You can view the availability by minute, hour, or day.
   - The **Related Events** section shows the historical exception events. Click **Show Details** corresponding to an event to view the event details.

4.4.1.3. View the availability of an instance

You can view the instance availability ratio of a cloud service to know the instance damages.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Full Stack**.
3. Click the **Availability of Instance** tab.



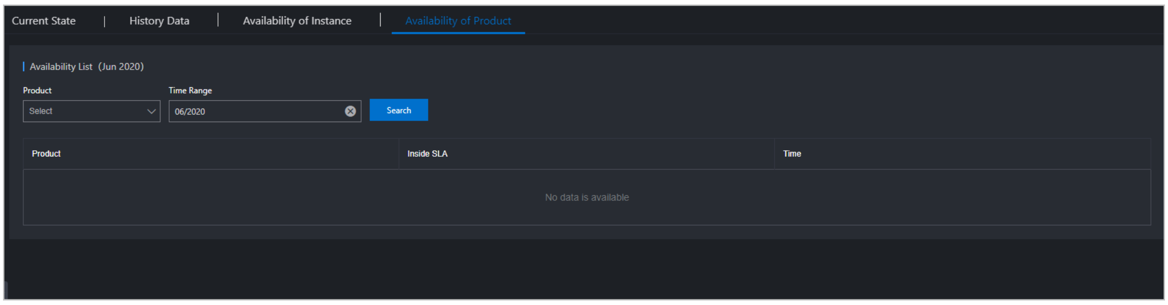
4. Specify **Instance ID**, **Belonged to User**, or **Time Range**. Then, click **Search**.
5. Click an **Instance ID** to view the following information of the instance:
   - **Basic Information**: the instance ID and the user to whom the instance belongs.
   - **Availability**: the availability ratio of the instance.
   - **Damage Event** : the exception event list.

4.4.1.4. View the availability of a service

You can view the availability ratio of a cloud service to understand its monthly availability.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources** > **Full Stack**.
3. Click the **Availability of Product** tab.
4. Specify **Product** and **Time Range**, and click **Search** to view the availability ratio of the product. For example, if the availability ratio of Elastic Compute Service (ECS) is 100.00%, ECS runs normally this month without faults.



4.4.2. Full stack log monitoring

The Full Stack Log Monitoring module allows you to search for logs of ECS-, SLB-, and All in ECS-related applications.

Context

- You can search for the logs of a variety of product components on the ECS tab, such as pop, OpenAPI, pync, and OpsApi.
- If the ilogtail reporting feature is enabled on each SLB service node, you can search for logs of pop, slb-yaochi, and slb-control-master on the SLB tab.
- You can search for vm_adapter logs, all in ECS-Apsara Infrastructure Management Framework

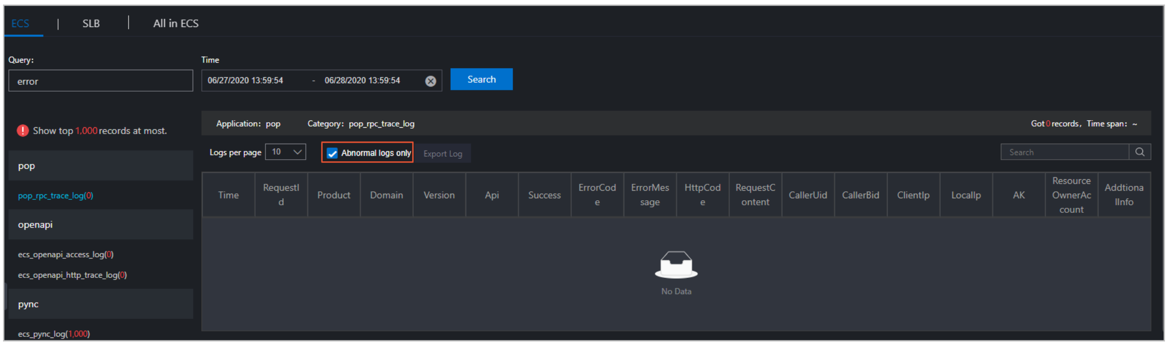
adaption layer logs, and all the other ECS operations logs on the All in ECS tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, choose **Resources > Full Stack**.
3. In the left-side navigation pane, click **Full Stack Log Monitoring**.
4. Click the **ECS**, **SLB**, or **All in ECS** tab.
5. Enter a keyword in the **Query** search box, select a time range in **Time**, and then click **Search**.

   > **Note** You can enter a string in the Query search box as the filter condition, such as the instance ID, request ID, or the keyword **error**.

6. The search results are displayed. Click an application log.

   Query: error

   Time: 06/27/2020 13:59:54 - 06/28/2020 13:59:54

   Show top 1,000 records at most.

   pop
   pop_rpc_trace_log(0)
   openapi
   ecs_openapi_access_log(0)
   ecs_openapi_http_trace_log(0)
   pync
   ecs_pync_log(1,000)

   Application: pop Category: pop_rpc_trace_log Got 0 records, Time span: ~

   Logs per page 10

   ☑ Abnormal logs only

Time	RequestId	Product	Domain	Version	Api	Success	ErrorCode	ErrorMessage	HttpCode	RequestContent	CallerUid	CallerBid	ClientIp	LocalIp	AK	ResourceOwnerAccount	AddtionalInfo

7. Select **Abnormal logs only** to view only the exceptional logs.

   If `code != 200`, `success=false`, or `error` exists in a log, the log is an abnormal log.

8. Enter a keyword in the search box to search for the related information in the search results.
9. (Optional)After the search is complete, click **Export Log** to export the search results to your computer.

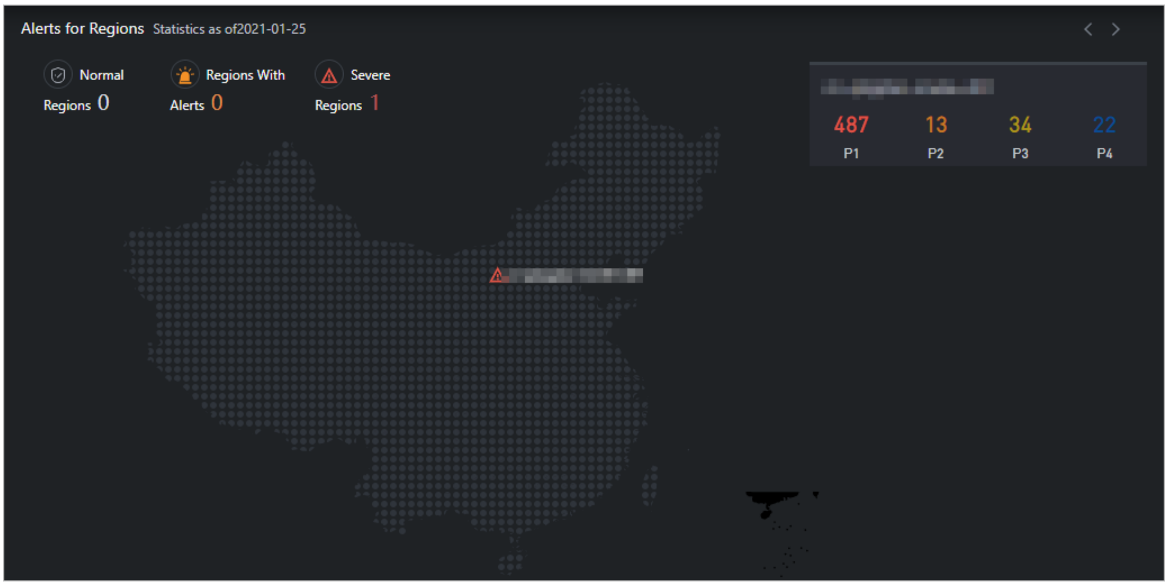
5.Alerts

5.1. Dashboard

This topic describes how to view alerts within each region of a multi-region scenario.

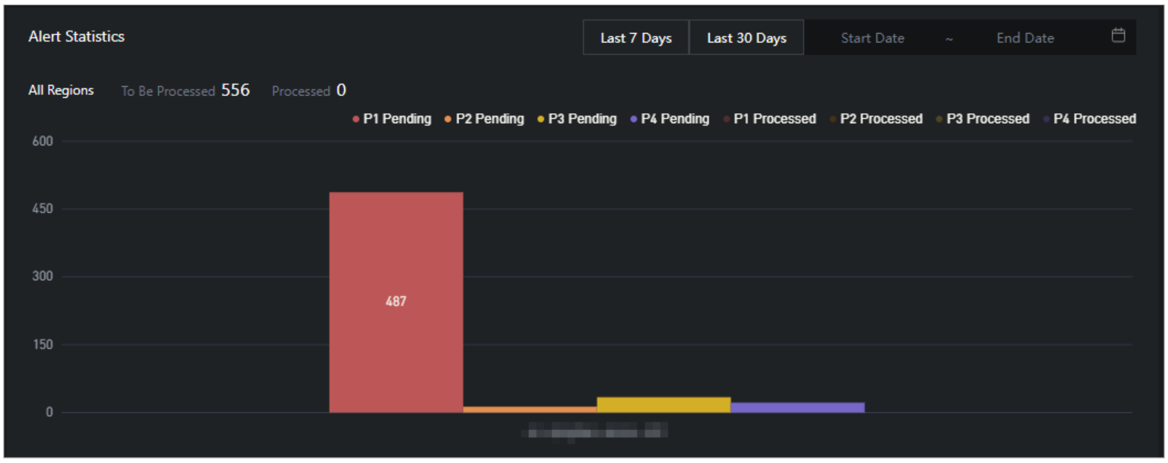
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Alerts**.
3. In the **Alerts for Regions** section, view the distribution of alerts in different regions. Move the pointer over a region with alerts, and the system displays the specific number of alerts.



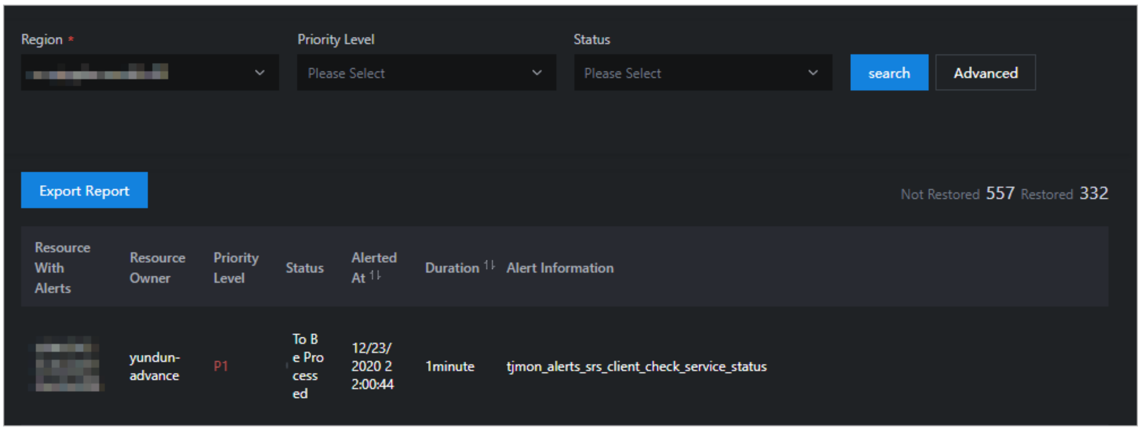
> **Note** P1, P2, P3, and P4 have the following meanings:
>
> - P1: an urgent alert
> - P2: a major alert
> - P3: a minor alert
> - P4: a reminder alert

4. In the **Alert Statistics** section, view the statistical data of alerts in the region.



[redacted]

- Click **Last 7 Days**, **Last 30 Days**, or specify **Start Date** and **End Date** to view the statistical data of alert handling within the period.
- Move the pointer over a column chart, and the corresponding statistical data is displayed.
- Select the required options from the **Region**, **Priority Level**, and **Status** drop-down lists, and click **search** to view the alert details.

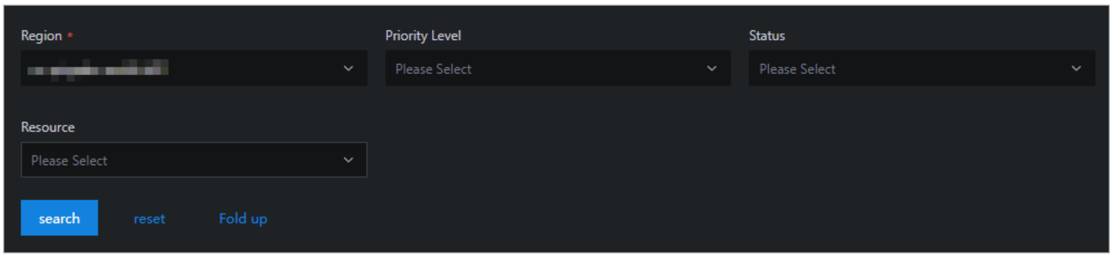


Region *: [redacted]

Not Restored 557 Restored 332

Resource With Alerts	Resource Owner	Priority Level	Status	Alerted At ↑↓	Duration ↑↓	Alert Information
[redacted]	yundun-advance	P1	To Be Processed	12/23/2020 22:00:44	1minute	tjmon_alerts_srs_client_check_service_status

- Specify more filter conditions to query alerts.
  - Click **Advanced**. Select the required options from the **Region**, **Priority Level**, **Status**, and **Resource** drop-down lists, and click **search** to view the alert details.



Region *: [redacted]

  - (Optional) Click **reset** to clear the filter conditions.
  - (Optional) Click **Fold up** to hide the **Resource** option.

5. Click **Export Report** to download the alert details to your computer.

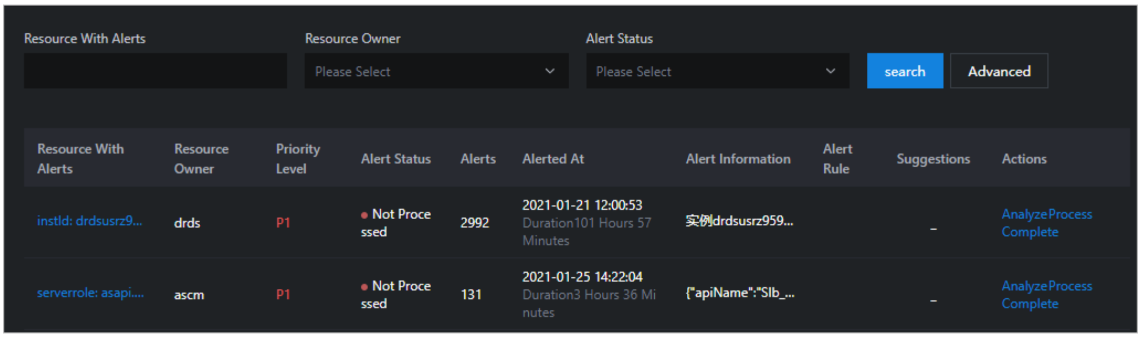
5.2. View alerts

This topic describes how to view the alerts for each cloud service, basic service, and hardware in the system.

Procedure

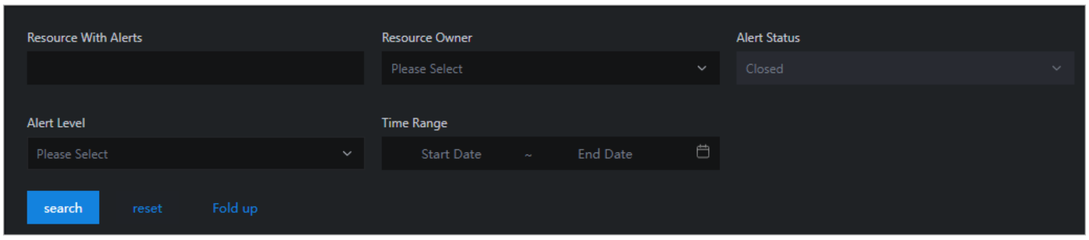
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Alerts**.
3. In the left-side navigation pane, click **Alerts** to view the distribution of alerts in the services.
   - Click the **Critical Alerts**, **Existing Alerts**, and **Alert History** tabs to view the information about different types of alerts.
   - The different colors of alerts indicate different ranges of quantities.
   - Drag the scroll bar to view more alerts.
   - Move the pointer over a color block, and alerts of the corresponding service are displayed.
4. View alerts.
   - Enter an alert resource ID in the **Resource With Alerts** search box, select the required options from the **Resource Owner** and **Alert Status** drop-down lists, and then click **search** to view the alerts.

     Move the pointer over an alert resource or a piece of alert information, and the full description of the alert information is displayed.

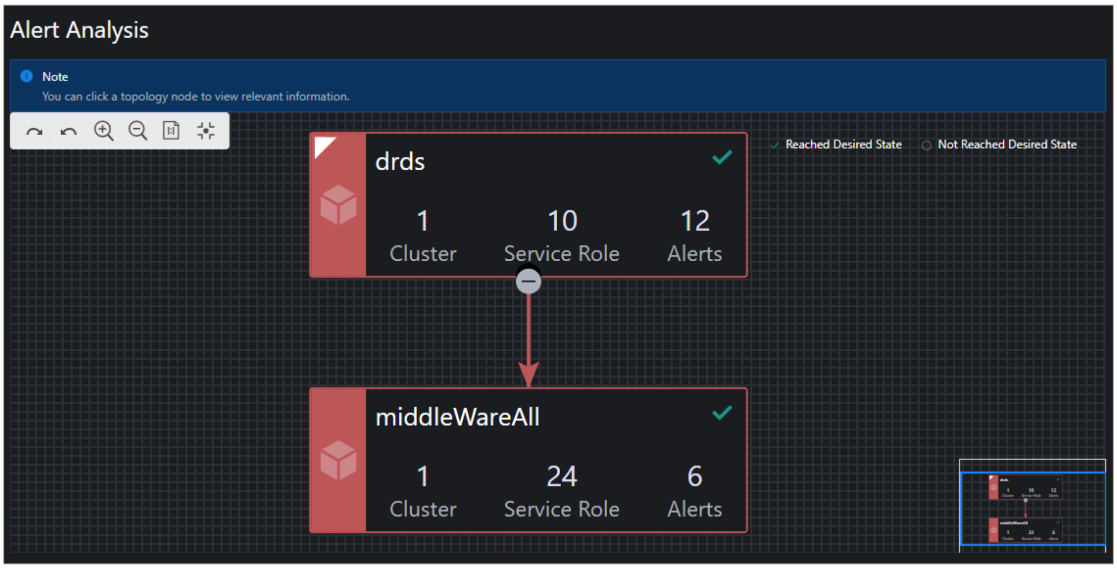
Resource With Alerts	Resource Owner	Priority Level	Alert Status	Alerts	Alerted At	Alert Information	Alert Rule	Suggestions	Actions
instId: drdsusrz9...	drds	P1	● Not Processed	2992	2021-01-21 12:00:53 Duration101 Hours 57 Minutes	实例drdsusrz959...		-	AnalyzeProcess Complete
serverrole: asapi....	ascm	P1	● Not Processed	131	2021-01-25 14:22:04 Duration3 Hours 36 Minutes	{"apiName":"Slb_...		-	AnalyzeProcess Complete

   - Specify more filter conditions to view the alerts.
     a. Click **Advanced**. Enter an alert resource ID in the **Resource With Alerts** search box, select the required options from the **Resource Owner**, **Alert Status**, and **Alert Level** drop-down lists, and then select a start date and an end date to specify **Time Range**. Then, click **search** to view the alert information.

     b. (Optional) Click **reset** to clear the filter conditions.
     c. (Optional) Click **Fold up** to hide the **Alert Level** and **Time Range** options.
5. Analyze the alert information.

i. Click **Analyze** in the Actions column corresponding to the alert information. On the **Alert Analysis** page, view the service role to which the alert belongs, the dependency link diagram of the service, or the logical topology of the server.



Alert Analysis

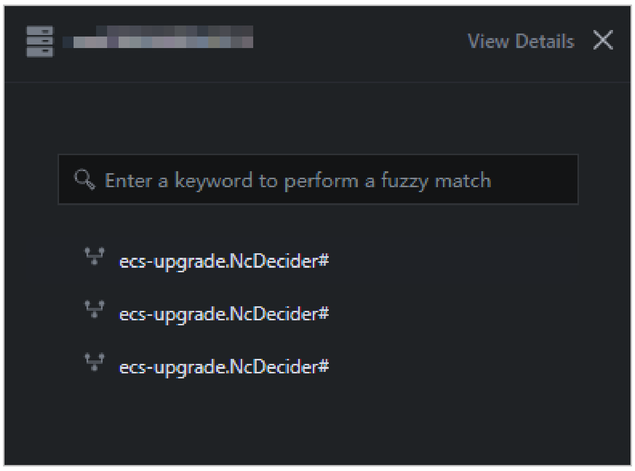
Note

You can click a topology node to view relevant information.

Note Icons:

- : indicates the server.
- : indicates the cluster.
- : indicates the service.
- : indicates the server role.

ii. Click a node in the topology. The details panel of the node appears on the right. The panel displays the elements related to this node. You can search for the elements by entering a keyword in the search box.



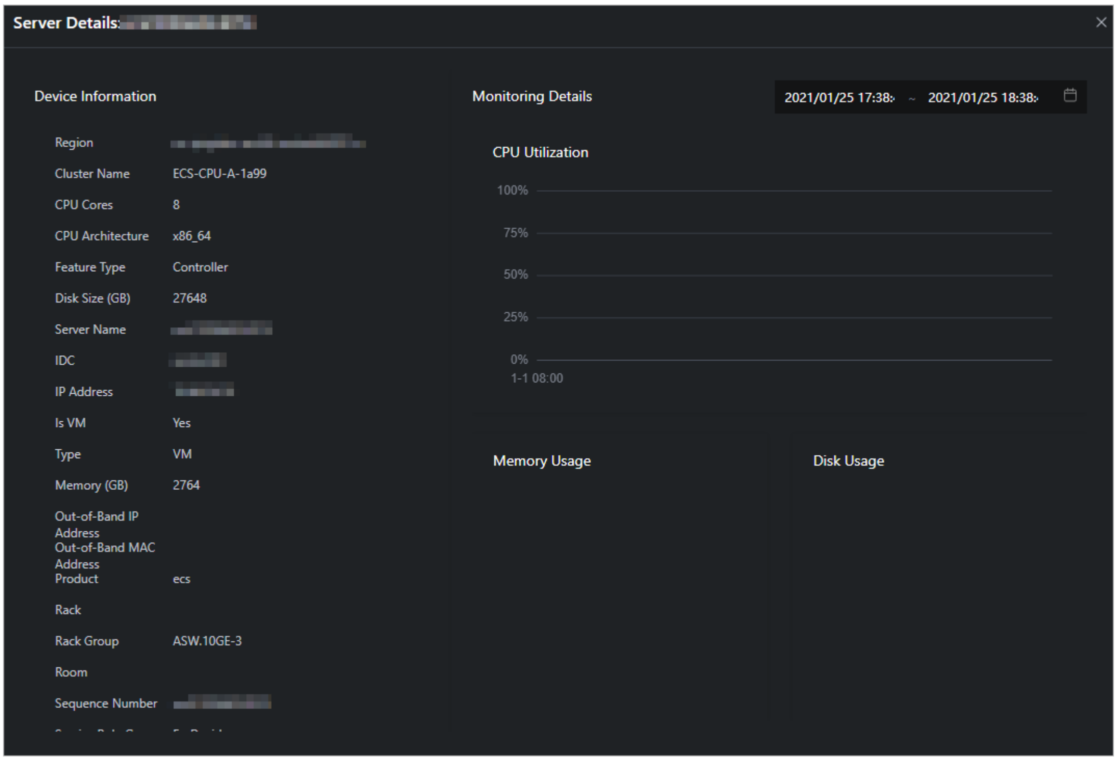
[redacted]

ecs-upgrade.NcDecider#

ecs-upgrade.NcDecider#

ecs-upgrade.NcDecider#

iii. Click **View Details** in the upper-right corner to view the details of the node. Select a start time and an end time to view the monitoring details within the time range.



Server Details:[redacted]

Device Information

Region	[redacted]
Cluster Name	ECS-CPU-A-1a99
CPU Cores	8
CPU Architecture	x86_64
Feature Type	Controller
Disk Size (GB)	27648
Server Name	[redacted]
IDC	[redacted]
IP Address	[redacted]
Is VM	Yes
Type	VM
Memory (GB)	2764
Out-of-Band IP Address	
Out-of-Band MAC Address	
Product	ecs
Rack	
Rack Group	ASW.10GE-3
Room	
Sequence Number	[redacted]

Monitoring Details 2021/01/25 17:38: ~ 2021/01/25 18:38:

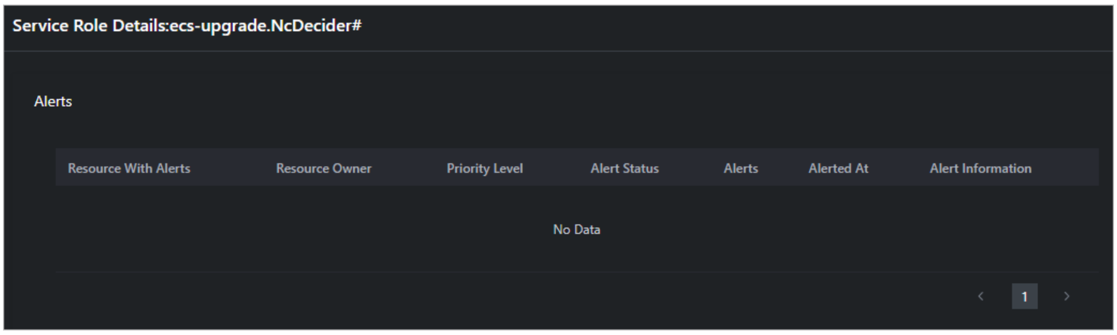
CPU Utilization

Memory Usage

Disk Usage

iv. In the node details panel, click an element related to this node to view the details of this element.

> **Note** In this example, the node is a server and the element related to the node is service role.



Service Role Details:ecs-upgrade.NcDecider#

Alerts

Resource With Alerts	Resource Owner	Priority Level	Alert Status	Alerts	Alerted At	Alert Information
No Data						

6. Click **Treatment** in the Actions column corresponding to the alert information. In the message that appears, click **OK** to mark the alert as being processed.
7. Click **Complete** in the Actions column corresponding to the alert information. In the message that appears, click **OK** to mark the alert as processed.

5.3. Alert settings

5.3.1. Policy management

The Policy Management module allows you to manage contacts and contact groups, and configure static parameters.

5.3.1.1. Alert contacts

You can query, add, modify, or delete alert contacts to suit your business needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Alerts**.
3. In the left-side navigation pane, choose **Alert Settings > Policy Management**.
4. On the Contacts tab, perform the following operations:
    - Query alert contacts

      In the upper-left corner of the tab, specify the product name, contact name, and phone number, and click **Search**. The alert contacts that meet the filter conditions are displayed in the list.
    - Add an alert contact

      In the upper-left corner of the tab, click **Add**. In the **Add Contact** panel, configure the parameters. Then, click **OK**.
    - Modify an alert contact

      Find the alert contact whose information you want to modify and click **Modify** in the **Actions** column. In the **Modify Contact** panel, modify the relevant information and click **OK**.
    - Delete an alert contact

      Find the alert contact that you want to delete and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

5.3.1.2. Alert contact groups

You can query, add, modify, or delete alert contact groups based on your business needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Alerts**.
3. In the left-side navigation pane, choose **Alert Settings > Policy Management**.
4. Click the **Contact Groups** tab.
5. Perform the following operations:
    - Query an alert contact group

      In the upper-left corner of the tab, enter a group name in the search box and click **Search**. The information of the alert contact group that meets the filter conditions is displayed.
    - Add an alert contact group

      In the upper-left corner of the tab, click **Add**. In the **Add Contact Group** panel, enter a group name and select the contacts to be added to the contact group. Then, click **OK**.
    - Modify an alert contact group

Find the contact group that you want to modify and click **Modify** in the **Actions** column. In the **Modify Contact Group** panel, modify the group name, description, contacts, and notification method. Then, click **OK**.

- Delete one or more alert contact groups

  Find the contact group that you want to delete and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

  Select one or more contact groups that you want to delete and click **Delete All** in the upper part of the tab. In the message that appears, click **OK**.

5.3.1.3. Configure static parameters

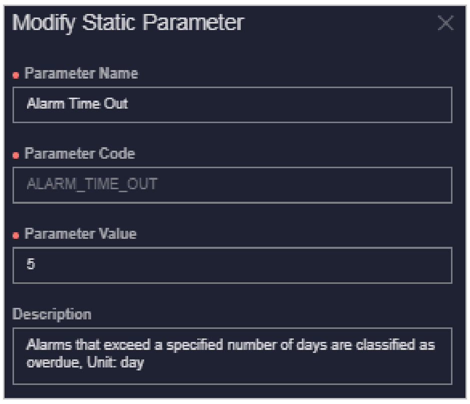
You can configure alert-related static parameters to suit your business needs. Only parameters related to timeout alerts can be configured.

Context

You cannot add new alert configurations in the current version. You can modify the default parameter configurations for timeout alerts.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Alerts**.
3. In the left-side navigation pane, choose **Alert Settings > Policy Management**.
4. Click the **Static Parameter Settings** tab.
5. (Optional)In the upper-left corner of the tab, enter a parameter name in the search box and click **Search** to query static parameter configurations.
6. Find the static parameter that you want to modify and click **Modify** in the **Actions** column.
7. In the **Modify Static Parameter** panel, modify the parameters described in the following table.



Modify Static Parameter

- Parameter Name: Alarm Time Out
- Parameter Code: ALARM_TIME_OUT
- Parameter Value: 5
- Description: Alarms that exceed a specified number of days are classified as overdue, Unit: day

Parameter	Description
Parameter Name	Enter a parameter name related to the configuration.

Parameter	Description
Parameter Value	Enter a parameter value. The default value is 5, indicating five days. After you complete the configurations, you can choose **Alert Monitoring > Alert Events** and then click the **Timeout Alert** tab to view the alert events that meet the condition specified by this parameter value. For example, if the parameter value is 5, you can choose **Alert Monitoring > Alert Events** and then click the **Timeout Alert** tab to view the alert events that are retained more than five days.
Description	Enter a description related to the configuration.

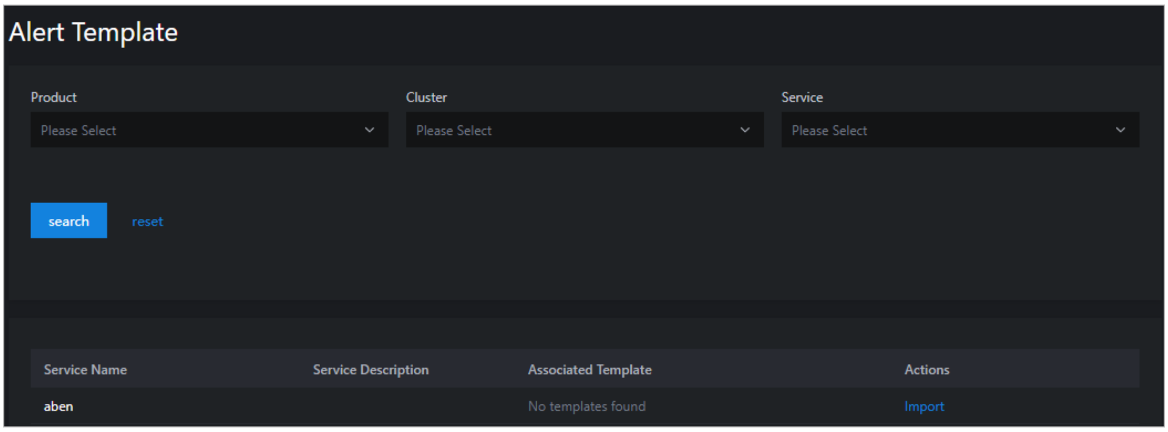
8. Click **OK**.

5.3.2. Alert templates

For Ant Financial Service products deployed on the PaaS platform, you can upload alert templates to configure or adjust the rules that trigger alerts.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Alerts**.
3. In the left-side navigation pane, choose **Alert Settings > Alert Template**.
4. On the **Alert Template** page, select the required options from the **Product**, **Cluster**, and **Service** drop-down lists, and click **search** to view the details of the service.



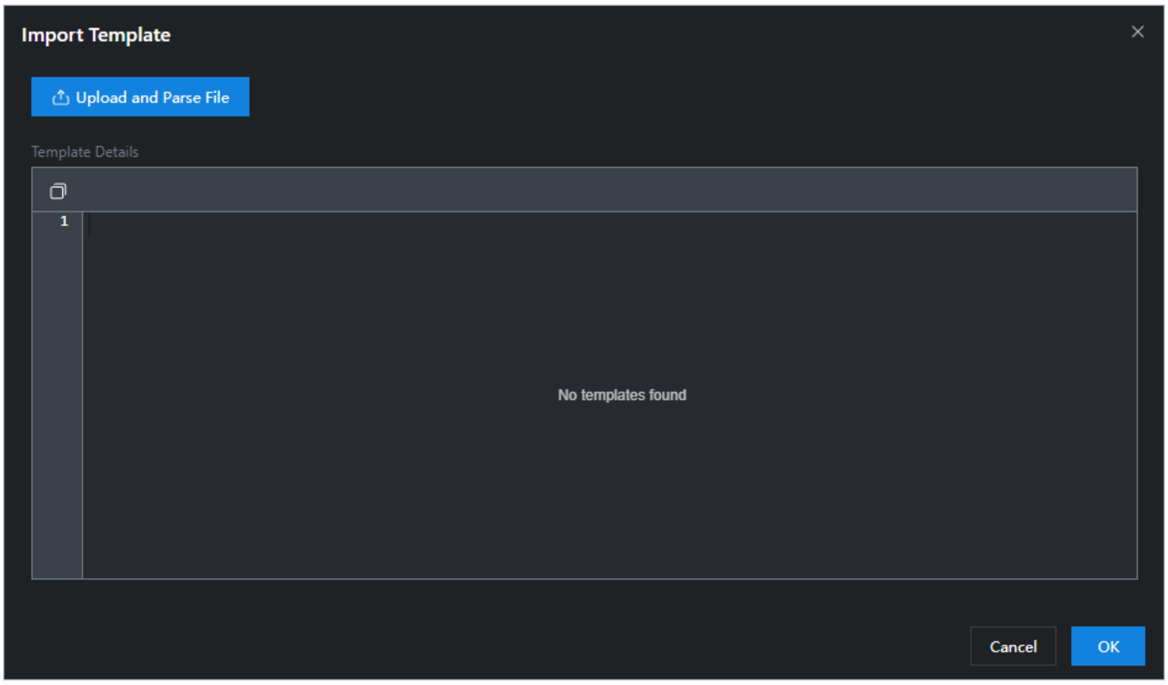
Service Name	Service Description	Associated Template	Actions
aben		No templates found	Import

5. (Optional) Click **reset** to clear the filter conditions.
6. Download Alert Templates.

> **Note** For Ant Financial Service products deployed on the PaaS platform, use the simple_template.json template.

7. Click **Import** in the Actions column corresponding to an entry. In the **Import Template** dialog box,

click **Upload and Parse File**. Select the template and click **Open**. After the template is uploaded, click **OK** to import the template.

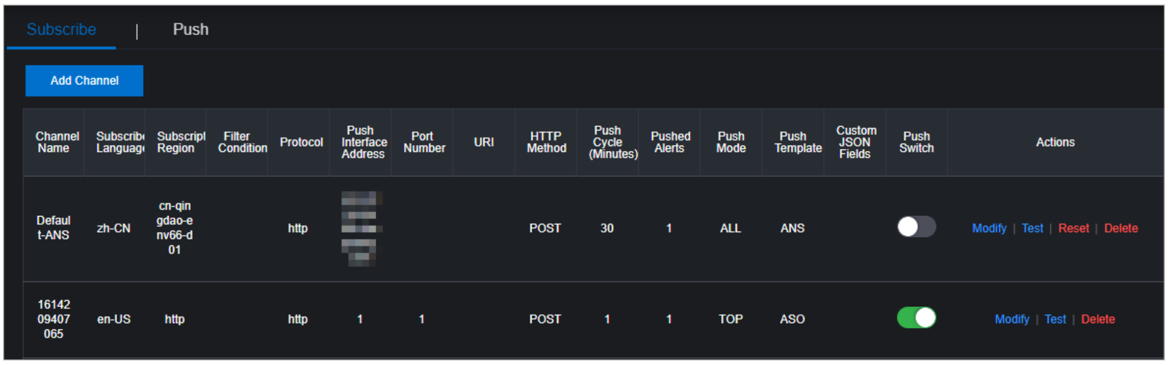


5.3.3. Notification management

The notification management feature allows you to configure alert notification channels and then push alerts to O&M engineers.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Alerts**.
3. In the left-side navigation pane, choose **Alert Settings > Notification Management**.



Channel Name	Subscrib Languag	Subscript Region	Filter Condition	Protocol	Push Interface Address	Port Number	URI	HTTP Method	Push Cycle (Minutes)	Pushed Alerts	Push Mode	Push Template	Custom JSON Fields	Push Switch	Actions
Default-ANS	zh-CN	cn-qingdao-env66-d01		http	[redacted]			POST	30	1	ALL	ANS		○	Modify | Test | Reset | Delete
1614209407065	en-US	http		http	1	1		POST	1	1	TOP	ASO		●	Modify | Test | Delete

4. On the **Subscribe** tab, click **Add Channel**.
5. In the **Add Subscription** panel, configure the parameters described in the following table.

Parameter	Description
Channel Name	The name of the subscription channel.

Parameter	Description
Subscribed Language	The subscription language. Valid values: Chinese and English.
Subscription Region	The region where the subscription is located.
Filter Condition	The filter conditions used to filter alerts. Valid values: ○ **Basic** ○ **Critical** ○ **Important** ○ **Minor** ○ Custom filter
Protocol	The protocol used to push alerts. Only HTTP is supported.
Push Interface Address	The IP address of the push interface.
Port Number	The port number of the push interface.
URI	The URI of the push interface.
HTTP Method	The request method used to push alerts. Only the POST method is supported.
Push Cycle (Minutes)	The interval at which to push alerts. Unit: minutes.
Pushed Alerts	The number of alerts pushed each time.
Push Mode	The mode used to push alerts. Valid values: ○ **ALL**: All alerts are pushed in each push cycle. ○ **TOP**: Only high priority alerts are pushed in each push cycle.
Push Template	The template used to push alerts. Valid values: ○ ASO: the default template. ○ ANS: Select this template to push alerts by DingTalk, short messages, or emails. You can configure only one channel of this type. **Note** A preset ANS template exists if the system is already connected to ANS. To restore the initial configurations of the template, click **Reset** in the **Actions** column corresponding to the channel.

Parameter	Description
Custom JSON Fields	The push receiver can use this field to customize an identifier. The field must be in the JSON format.
Push Switch	Specifies whether to push alerts. If the switch in this panel is not turned on, you can enable the push feature in the **Push Switch** column after you configure the subscription channel.

6. Click **OK**. To modify or delete a channel, click **Modify** or **Delete** in the **Actions** column corresponding to the channel.
7. (Optional)The newly added channel is displayed in the list. Click **Test** in the **Actions** column to test the connectivity of the push channel.

   > ? **Note** For an ANS push channel, you must enter the mobile phone number, email address, or DingTalk to which the alerts are pushed after you click **Test** in the Actions column.

8. After you configure the push channel and turn on the push switch, you can click the **Push** tab to view the push records.

5.3.4. Alert masking

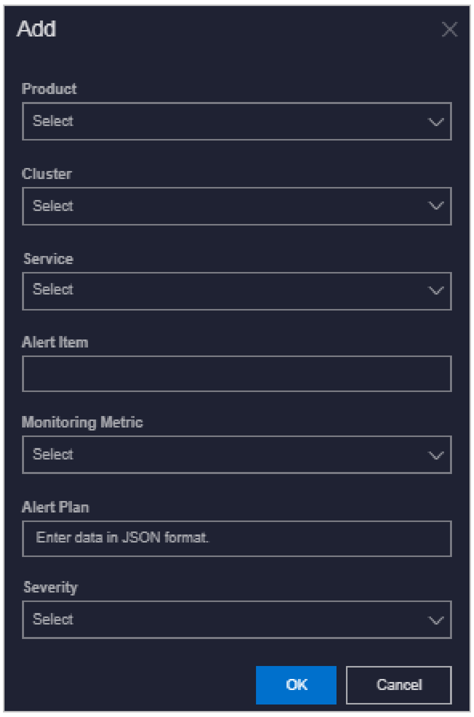
The Alert Masking module allows you to mask a type of alerts and remove masking as needed.

5.3.4.1. Add masking rules

Masking rules allow you to mask alerts that are no longer needed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Alerts**.
3. In the left-side navigation pane, choose **Alert Settings > Alert Masking**.
4. In the upper part of the page, click **Add**.
5. In the **Add** panel, configure the parameters to filter the alerts to be masked.


Add

Product

Select

Cluster

Select

Service

Select

Alert Item

Monitoring Metric

Select

Alert Plan

Enter data in JSON format.

Severity

Select

Parameter	Description
Product	Optional. The product to which the alerts to be masked belong.
Cluster	Optional. The cluster to which the alerts to be masked belong.
Service	Optional. The service to which the alerts to be masked belong.
Alert Item	Optional. The name of the alerts to be masked. **Note** When you configure **Alert Item**, you may need to wait a few minutes if the number of alerts is large.
Monitoring Metric	Optional. The monitoring metric to which the alerts to be masked belong.
Alert Plan	Optional. Details of the alerts to be masked. Example: `{"serverrole":"ecs-yaochi.ServiceTest#","machine":"vm01001******","level":"error"}`

Parameter	Description
Severity	Optional. The severity level of the alerts. Valid values: ○ **P0**: indicates the alerts that have been cleared, corresponding to alerts whose **Alert Level** is **Restored** in **Monitoring > Alert History** of Apsara Infrastructure Management Framework. ○ **P1**: indicates critical alerts, corresponding to alerts whose **Alert Level** is **P1** in **Monitoring > Alert History** of Apsara Infrastructure Management Framework. ○ **P2**: indicates major alerts, corresponding to alerts whose **Alert Level** is **P2** in **Monitoring > Alert History** of Apsara Infrastructure Management Framework. ○ **P3**: indicates minor alerts, corresponding to alerts whose **Alert Level** is **P3** in **Monitoring > Alert History** of Apsara Infrastructure Management Framework. ○ **P4**: indicates reminder alerts, corresponding to alerts whose **Alert Level** is **P4** in **Monitoring > Alert History** of Apsara Infrastructure Management Framework. ○ **P5**: indicates system alerts.

6. Click **OK**.

Result

The added masking rule is displayed in the alert masking list.

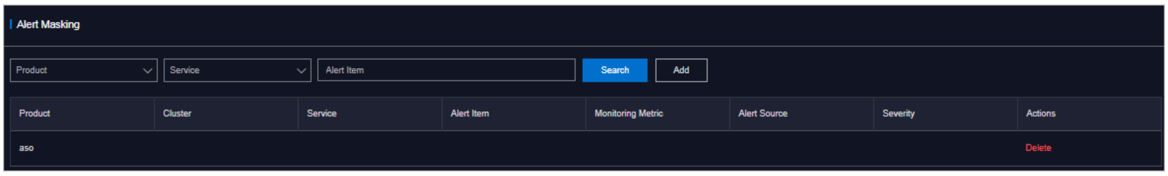
After a masking rule is added, alerts that meet the conditions in the masking rule are not displayed in **Alerts > Alerts**.

5.3.4.2. Disable masking

You can disable masking for masked alerts.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Alerts**.
3. In the left-side navigation pane, choose **Alert Settings > Alert Masking**.
4. (Optional)Specify a product, service, or an alert item. Then, click **Search**.
5. Find the alert masking rule for which you want to disable and click **Delete** in the **Actions** column.



Product	Cluster	Service	Alert Item	Monitoring Metric	Alert Source	Severity	Actions
aso							Delete

6. In the message that appears, click **OK**.

Result

After masking is disabled, the unmasked alerts are displayed in **Alerts > Alerts**.

6.O&M

6.1. Automated O&M

The automated O&M feature automates O&M for data centers. A web-based method is provided to implement O&M operations for resources at scale, simplify O&M management of IT resources, and support full-stack automated O&M of the infrastructure, the Apsara Stack environment, operating systems, and the application layer.

6.1.1. View host resources

You can view the information about hosts such as physical machines or Docker virtual machines.

Context

Before you execute a script or an O&M job on a host, you can view the specific information about the host to ensure that the script or job can be effectively executed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Host Resources**.
4. On the **Host Resources** page, enter a hostname, project name, or cluster name in the upper-left search box and click **search**. Fuzzy match is supported. You can view the information about the hosts that meet the filter condition, including the hostname, IP address, project name, cluster name, operating system, and IDC.
5. (Optional) Click **reset** to clear the filter conditions.

6.1.2. View Docker resources

You can view the information about Docker containers.

Context

Before you execute a script or an O&M job on a Docker container, you can view the specific information about the Docker container to ensure that the script or job can be effectively executed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Docker Resources**.
4. On the **Docker Resources** page, enter a server role name, project name, cluster name, or service name in the upper-left search box and click **search**. Fuzzy match is supported. You can view the information about the Docker containers that meet the filter conditions, including the server role name, type, hostname, host IP address, project name, cluster name, and service name.
5. (Optional) Click **reset** to clear the filter conditions.

6.1.3. Manage scripts

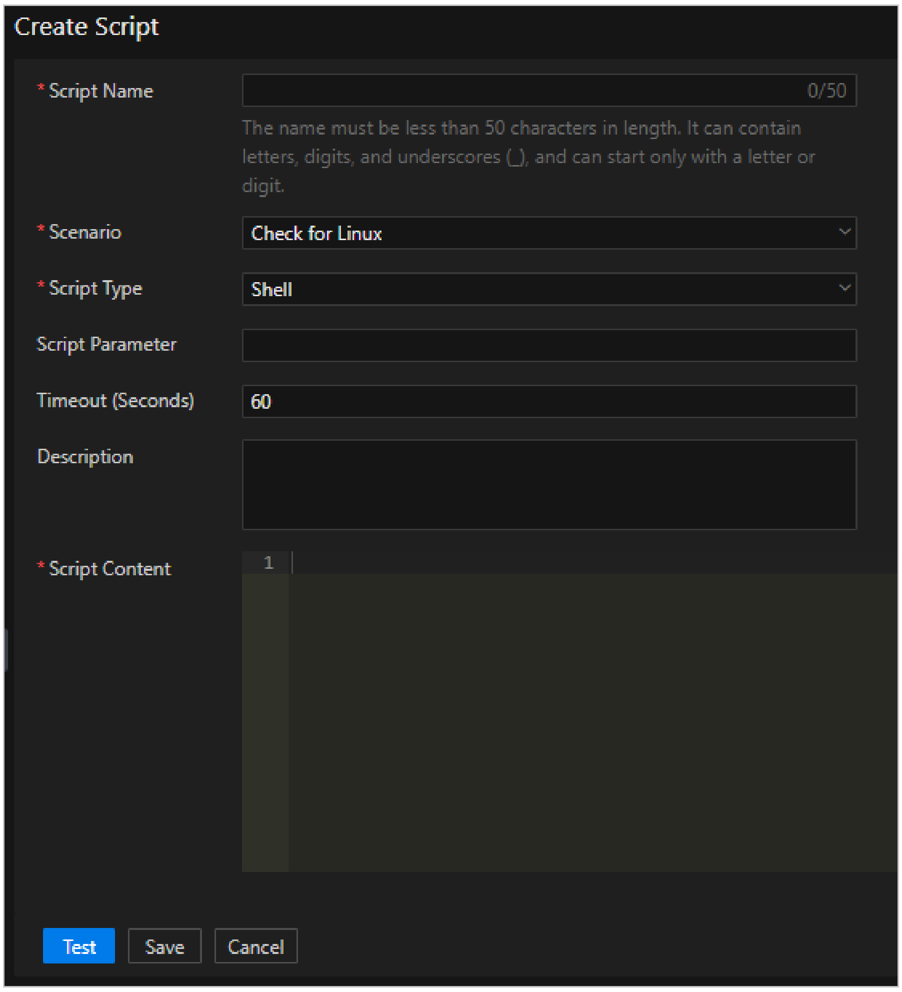
The script library is used to store scripts for implementing various features and is the basis for automated O&M. All O&M commands are run by using scripts. The system provides some common built-in default scripts and supports custom scripting. You can create, import, view, modify, export, and delete scripts.

6.1.3.1. Create a script

You can create a script and test whether it can be properly executed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Script Library**.
4. Click **Create Script**.
5. Configure the parameters for the script.



Create Script

* Script Name: 0/50

The name must be less than 50 characters in length. It can contain letters, digits, and underscores (_), and can start only with a letter or digit.

* Scenario: Check for Linux

* Script Type: Shell

Script Parameter:

Timeout (Seconds): 60

Description:

* Script Content:

The following table describes the parameters.

Parameter	Description
Script Name	The name of the script.
Scenario	The application scenario of the script. Valid values: **Check for Linux**, **Run Command**, and **Install Software**.
Script Type	The type of the script. Valid values: Shell and Python.
Script Parameter	The parameters passed in when the script is executed. Separate multiple parameters with spaces.
Timeout (Seconds)	The timeout period for script execution. After the specified number of seconds, the script stops executing and the execution timeout result is returned.
Description	The description of the script.
Script Content	The content of the script. When you write a script, you must add a script interpreter. For example, for a Shell script, you must enter `#!/bin/bash`. For a Python script, you must enter `#!/usr/bin/python`. The path of the interpreter may vary with the execution resources and environments.

6. Click **Test** to test whether the script can be properly executed. If you confirm that the script can be executed, you can directly click **Save**.
   i. After you click **Save** or **Test**, the system checks the script content. If the **The script has high-risk commands. Do you want to continue?** message appears, check whether the script content is correct.
      - Correct: Click **OK**.
      - Incorrect: Modify the script and test again.
   ii. After you click **Test**, click **Host Resources** or **Docker Resources** in the **Script Test** dialog box, select one or more host resources or Docker resources, and then click **Execute**.

      > **Note** The SSH protocol is used to copy files to the host or Docker container. Therefore, the test execution process may be slow.

   iii. In the **Test Results** dialog box, view the test result of the script.
      - Click **OK** to exit the dialog box and click **Save** to save the script.
      - Click **Re-select Resources** to select another host or Docker container to test the script.

6.1.3.2. Import a script

You can import a script on your computer to the script library.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Script Library**.
4. Click **Import Script**.
5. In the **Upload Script File** dialog box, click **Click Here to Upload** to upload a script on your computer to the script library.

   > **Note** Only JSON files can be uploaded. The file to be uploaded cannot exceed 500 KB in size.

6.1.3.3. View scripts

You can view scripts in the script library.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Script Library**.
4. In the **Script Name** search box, enter the name of the script that you want to view and click **search**. Fuzzy match is supported. You can view the information about the scripts that meet the filter conditions, including the script name, script type, scenario, parameter, modification time, description, user who updates the script, and whether the script is a default script.
5. (Optional) Click **reset** to clear the filter conditions.

6.1.3.4. Modify a script

After a script is created or imported, you can modify the script to suit your requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Script Library**.
4. Find the script that you want to modify and click **Edit** in the **Actions** column.
5. Modify the parameters and click **Test** to test whether the script can be executed. If you confirm that the script can be executed, you can click **Save**.

   i. After you click **Save** or **Test**, the system checks the script content. If the **The script has high-risk commands. Do you want to continue?** message appears, check whether the content of the script is correct.

      - Correct: Click **OK**.
      - Incorrect: Modify the script and test again.

ii. After you click **Test**, click **Host Resources** or **Docker Resources** in the **Script Test** dialog box, select one or more host resources or Docker resources, and then click **Execute**.

> ⓘ **Note** The SSH protocol is used to copy files to the host or Docker container, which may result in slow execution speeds.

iii. In the **Test Results** dialog box, view the test result of the script.

- Click **OK** to exit the dialog box and click **Save** to save the script.
- Click **Re-select Resources** to select another host or Docker container to test the script.

6.1.3.5. Export a script

You can export a script to your computer.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Script Library**.
4. Select one or more scripts that you want to export and click **Export Script** to export the scripts to your computer.

> ⓘ **Note** If you export multiple scripts at a time, the content of the scripts is stored as a single JSON file.

6.1.3.6. Delete a script

You can delete scripts that are no longer needed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Script Library**.
4. Select one or more scripts that you want to delete and click **Delete Script** in the lower part of the page, or click **Delete** in the **Actions** column.
5. In the message that appears, click **OK**.

6.1.4. Manage software

The software repository is used to manage software, including uploading, viewing, downloading, and deleting software. The term software used in this topic is in its broad sense, including compressed packages, JAR packages, images, and files. Only software uploaded to the software repository can be used in subsequent jobs.

6.1.4.1. Upload software

You can upload software to the software repository.

Context

When an O&M job is executed in an on-site environment, software is downloaded from the software repository and deployed on the host or Docker container. You must upload the software to the software repository before you can use it in subsequent jobs.

> ? **Note** Delete software that is no longer needed to free up storage space.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Software Repository**.
4. Click **Upload Software**.
5. In the **Upload Software** dialog box, enter a software name in the **Software Name** field and click **Click Here to Upload** to upload a file. If you do not enter a software name, the software name is the same as the file name.

   > ? **Note** The file to be uploaded cannot exceed 500 MB in size.

6.1.4.2. View software

You can view software in the software repository.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Software Repository**.
4. In the **Software Name** search box, enter the name of the software that you want to view and click **search**. Fuzzy match is supported. You can view information about software that meets the filter conditions, including the software name, file name, file size, upload time, and upload user.
5. (Optional) Click **reset** to clear the filter conditions.

6.1.4.3. Download software

You can download software from the software repository to your computer.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Software Repository**.

4. Select the software that you want to download and click **Download** in the **Actions** column.

6.1.4.4. Delete software

To save storage space, you can delete software that is no longer needed after O&M jobs are executed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Software Repository**.
4. Select one or more software that you want to delete and click **Delete Software** in the lower part of the page, or click **Delete** in the **Actions** column.
5. In the message that appears, click **OK**.

6.1.5. Manage processes

Process orchestration is one of the core features of automated O&M. It is used to manage processes, including creating, importing, viewing, exporting, modifying, running, and deleting processes. You can define a process to combine a series of logical actions into a task and automate O&M.

6.1.5.1. Create a process

You can create a process to visually orchestrate the O&M process and automate O&M.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Process Orchestration**.
4. Click **Create Process**.
5. On the **Create Process** page, click **Process Settings**.
6. In the **Process Settings** dialog box, configure the following parameters:
    - **Process Name**: Enter a name for the process.
    - **Process Description**: Enter a description for the process.
    - **Trigger Method**: Select **Manual** or **Scheduled**.
        - **Manual**: The process must be manually triggered.
        - **Scheduled**: The process is triggered at the specified time.
    - **Timing Rule**: This parameter is available only when **Trigger Method** is set to **Scheduled**. Set the time to trigger the process.
        - **Once**: The process is triggered only once at the specified time. Select a date and time to trigger the process.

- **Daily**: The process is triggered once at the specified time every day. Select a time to trigger the process every day.
- **Monthly**: The process is triggered at the specified date and time every month. Select a date and time to trigger the process. For example, if you set **Days** to 10 and **Time** to 09:00:00, the process is triggered at 09:00:00 on the tenth day of every month.

7. Click **OK**.
8. Drag nodes on the left side to the right side and add lines between the nodes. The nodes that can be added to a process include the Start, Task, Judgement, Manual, Wait, and Notification nodes.

   - ▶: the Start node. Each process has only one Start node, which represents the start of the process. The Start node has no parameters and can have only one line to connect to another node.
   - ▣: the Task node. The Task node is the major node for process execution and can execute one script or job. Click the Task node and configure the following parameters in the **Node Properties** dialog box.

Tab	Parameter	Description
Specify Node	**Node Name**	The name of the node.
	Description	The description of the node.
Specify Parameters	**Input Parameters**	Input parameters are the output parameters of the previous node. If a previous node has no output parameters, the current node has no input parameters. Input parameters follow a script in sequence when the script is executed. Example: `./test.sh params1 params2`. **Note** If you set Operation to **Execute Job** on the Select Operation tab, you do not need to specify the input parameters.

Tab	Parameter	Description
	Output Parameters	Output parameters take effect when only one script and execution resource is selected for the node. Output parameters come from the execution result of the script. Therefore, the script must return a fixed result. For example, if the execution result is `echo "CPU=22,MEM=30"`, click **Add** to configure the output parameters. Specify **Output Parameter Name** and enter CPU and MEM in the **Parsed Key Value** field. **Note** If you set Operation to **Execute Job** on the Select Operation tab, you do not need to specify the output parameters.
Select Operation	**Operation**	Select **Script** or **Execute Job** and select a script from the Script drop-down list, or select an execute job from the Execute Job drop-down list.

Tab	Parameter	Description
	Resource Type	Select **Host** or **Docker**. - **Host**: Click **Select Host**. In the **Select Host** dialog box, select one or more hosts and click **OK**. You can also enter a hostname, project name, or cluster name in the **Host** search box and press the Enter key to search for the hosts that you want to select. Fuzzy match is supported. - **Docker**: Click **Select Docker**. In the **Select Docker** dialog box, select one or more Docker containers and click **OK**. You can also enter a service role name, project name, or cluster name in the **Docker** search box and press the Enter key to search for the Docker containers that you want to select. Fuzzy match is supported. You can click the 🗑 icon to delete the specified host or Docker container.
		Select **None**, **Automatically Executed**, or **Stop Waiting**. - **None**: The scripts or jobs are executed on all the selected hosts or Docker containers in one batch.

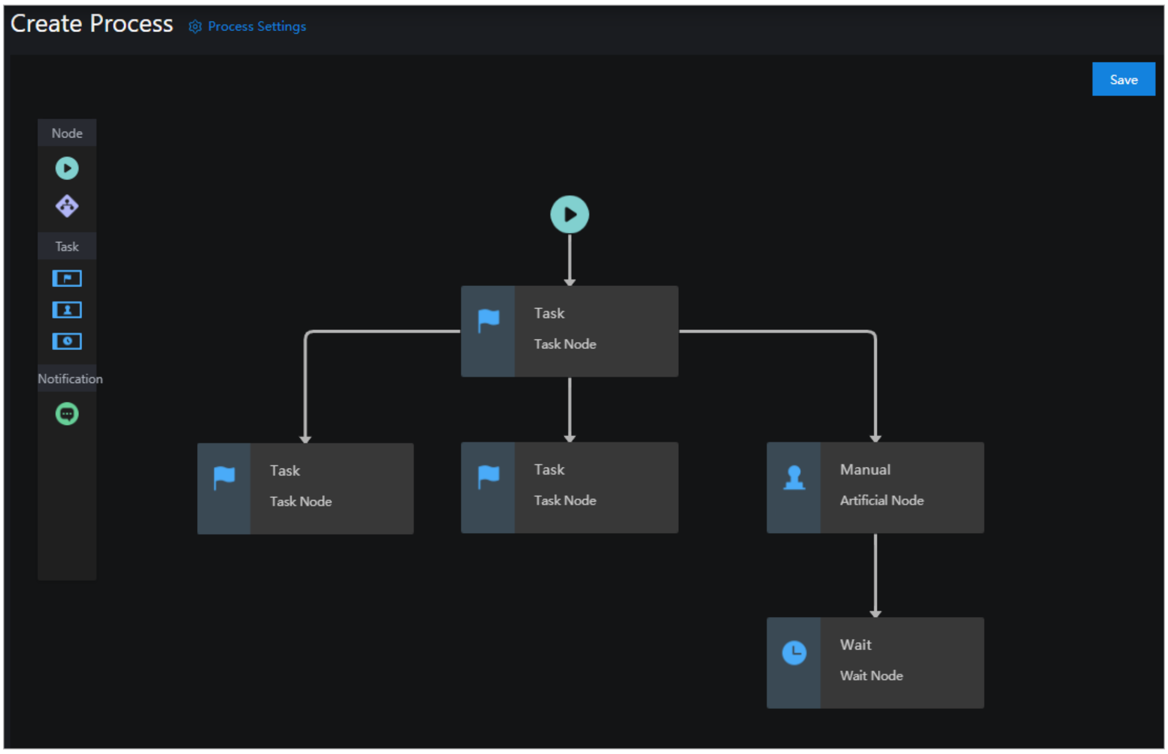
Tab	Parameter	Description
Select Execution Resources	**Phased Execution Settings**	■ **Automatically Executed**: The scripts or jobs are executed in two batches on the selected hosts or Docker containers. One batch is executed at a time. After the first batch is executed, the second batch starts to be executed. If the first batch fails to be executed, the second batch is not executed. **Note** If you set Resource Type to Docker, the selected Docker containers are automatically divided into batches based on the service role name such that Docker containers with the same service role are in different batches. ■ **Stop Waiting**: The scripts or jobs are executed in two batches on the selected hosts or Docker containers. The first batch is executed first. After the first batch is executed, a process approval is sent. The approver can click **Passed** or **Stop** in **Process Review**. When the approval is passed, the second batch starts to be executed. If the first batch fails to be executed, the execution stops and no process approval is sent. **Note** If you set Resource Type to Docker, the selected Docker containers are automatically divided into batches based on the service role name such that Docker containers with the same service role are in different batches.

Tab	Parameter	Description

- ◈: the Judgement node, which is used to judge the process routes of different directions. The previous node of the Judgement node must be a Task node that has output. Otherwise, the Judgement node is of no use. Click the Judgement node. In the **Node Properties** dialog box, configure the following parameters.
  - **Node Name**: Enter a name for the node.
  - **Description**: Enter a description for the node.
  - **Judgement Condition**: Click **Add**. In the **Add** dialog box, set **Output Parameter Name** of the previous node and set the judgement condition by specifying **Judge** and **Value**. Click **OK** to save the judgement condition.
  - **Judgement Type**: If you set multiple judgement conditions, you must select **Or** or **And**.
    - **Or**: The judgement result is yes if one judgement condition is met. The judgement result is no if no judgement conditions are met.
    - **And**: The judgement result is no if one judgement condition is not met. The judgement result is yes if all the judgement conditions are met.

  You must click the lines coming out from the Judgement node and set **Yes** or **No** to define the execution of the subsequent process.
- ▣: the Manual node. When the process is executed to this node, the process is suspended for manual approval. If the approval is passed, the process continues execution. If the approval is not passed, the subsequent process is not executed. If a timeout period is specified and manual approval is not performed after this period expires, the subsequent process is automatically stopped.
- ▣: the Wait node. When the process is executed to this node, the process waits a specified period of time before the subsequent process is executed. For example, the previous node executed the script for service startup, but usually the service startup takes some time. In this case, you can wait 1 minute and then check whether the service is normal in the next node.
- ●: the Notification node. Notifications are sent by email. Select **Email** from the **Notification Type** drop-down list. Then, set Recipient, Notification Title, and Notification Content. Separate multiple email addresses with commas (,).

9. Click **Save** in the upper-right corner.



6.1.5.2. Import a process

You can import existing processes.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Process Orchestration**.
4. Click **Import Process**.
5. In the **Upload Process** dialog box, click **Click Here to Upload** to upload an existing process.

> **Note** Only JSON files can be uploaded. The file to be uploaded cannot exceed 500 KB in size.

6.1.5.3. View processes

You can view existing processes.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Process Orchestration**.

4. In the **Name** search box, enter the name of the process that you want to view and click **search**. Fuzzy match is supported. You can view the information of processes that meet the filter conditions, including the process name, description, execution method, modification time, execution history, latest execution time, and latest execution status.
5. (Optional) Click **reset** to clear the filter conditions.
6. Click the process name to go to the **Process Details** page. On the **Process Details** page, you can perform the following operations:
   - Click the **Process Details** tab to view the structure of the process.
   - Click the **Execution History** tab to view the execution history of the process. You can also click **View Details** to view the details of the execution history, including the node name, node type, start time, end time, task status, and execution information.
   - Click **Run** in the upper-right corner to manually run the process.
   - Click **Modify** in the upper-right corner to modify the process.
   - Click **Delete** in the upper-right corner to delete the process.

6.1.5.4. Export a process

You can export processes to your computer.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Process Orchestration**.
4. Select one or more processes that you want to export and click **Export Process** to export the processes to your computer.

> **Note** If you export multiple processes at a time, the content of the processes is stored in one JSON file.

6.1.5.5. Modify a process

After you have created or imported a process, you can modify the process to suit your requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Process Orchestration**.
4. Select the process that you want to modify and click **Modify** in the **Actions** column.
5. Modify the process and click **Save** in the upper-right corner.

6.1.5.6. Run a process

You can manually trigger processes.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Process Orchestration**.
4. Select the process that you want to run and click **Run** in the **Actions** column.
5. In the message that appears, click **OK**.

6.1.5.7. Delete a process

You can delete processes that are no longer needed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > Process Orchestration**.
4. Select the process that you want to delete and click **Delete** in the **Actions** column.
5. In the message that appears, click **OK**.

6.1.6. Manage O&M jobs

O&M jobs is one of the core features of automated O&M and can be used to independently complete O&M tasks such as software distribution, patch upgrade, and program update. You can create, import, view, export, modify, run, and delete O&M jobs.

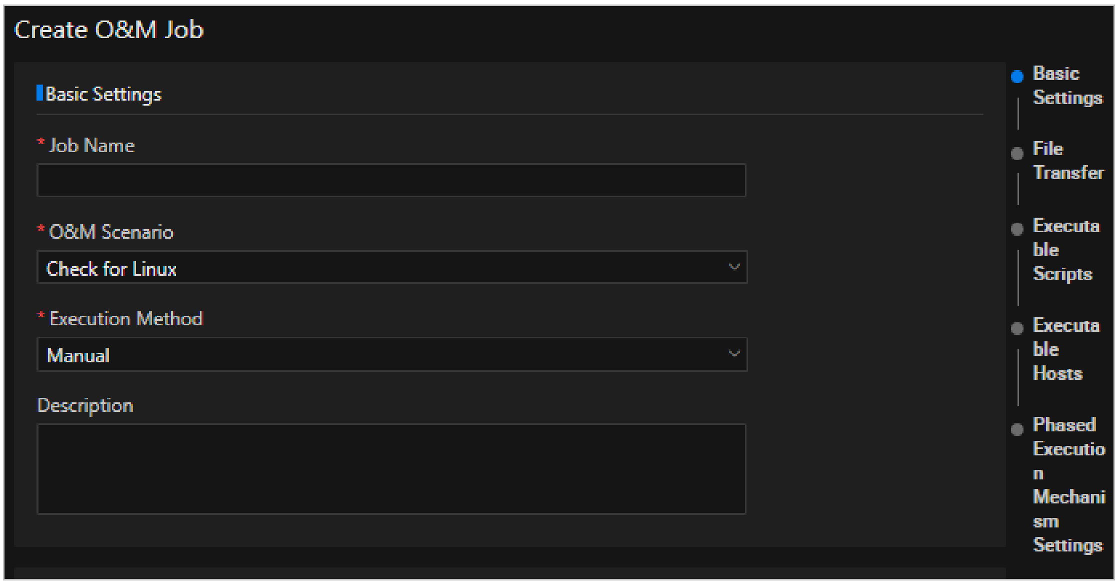
Each O&M job is a collection of features for O&M resources, software, and scripts. Scripts are used to implement features and are executed on different hosts or Docker instances in a specified order to reduce the workloads of O&M personnel.

6.1.6.1. Create an O&M job

You can create an O&M job to independently complete an O&M task to automate O&M.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > O&M Jobs**.
4. Click **Create O&M Job**.
5. On the **Create O&M Job** page, configure the parameters described in the following table.


Create O&M Job

Basic Settings

* Job Name

* O&M Scenario: Check for Linux

* Execution Method: Manual

Description

Parameter	Description
Job Name	The name of the O&M job.
O&M Scenario	The scenario of the O&M job. You can select **Check for Linux**, **Run Command**, or **Install Software**.
Execution Method	Select **Manual** or **Scheduled**. ○ **Manual**: The O&M job must be manually executed. ○ **Scheduled**: The O&M job is executed at the specified time.
Timing Rule	This option is available only when **Execution Method** is set to **Scheduled Execution**. Set the time to execute the O&M job. ○ **Once**: The O&M job is executed only once at the specified time. Select a date and time to execute the O&M job. ○ **Daily**: The O&M job is executed once at the specified time every day. Select a time to execute the O&M job every day. ○ **Monthly**: The O&M job is executed at the specified date and time every month. Select a date and time to execute the O&M job. For example, if you set **Days** to 10 and **Time** to 09:00:00, the O&M job is executed at 09:00:00 on the tenth day of every month.
Description	The description of the O&M job.

Parameter	Description
File Transfer	Click **Add File**. In the **Add File** dialog box, select the file that you want to transmit to the host or Docker container, enter an absolute path in the Transmission Path field, and then click **OK**. You can add multiple files or click the 🗑 icon to delete the files that are no longer needed. **Note** The files that you can select all come from the software repository.
Execution Scripts	Add one or more scripts that you want to execute on the host or Docker container, and the system executes them in sequence. Click **Add Executable Script** and select a script from the script library, or click **Add Script** to create a script. You can click the ✎ icon to modify the script. The modification does not change the original script content in the script library. You can click the ⇧ or ⇩ icon to change the order of execution of the script. You can also click the 🗑 icon to delete the scripts that are no longer needed.
Executable Hosts	Set **Resource Type** to **Host** or **docker**. Click **Add Host resources** or **Add Docker Resources** to add one or more hosts or Docker containers. These hosts or Docker containers are where all files are transferred to and where the scripts are executed. **Note** You can specify only one resource type. You cannot add both host and Docker resources at the same time.
	You can select the following options to set the phased execution rules: ○ **None (You do not need to specify this parameter, and all target hosts are executed directly.)**: The script is executed on all the selected hosts or Docker containers in a single batch. You can select this option if you are selecting only a few hosts or Docker containers, or if you have confirmed that you

Parameter	Description
Phased Execution Rules	do not have problem with script execution. ○ **Automatically Execute (You do not need to specify batches. The system executes jobs in two batches. After the execution of the first batch is complete, the second batch is automatically executed.)**: The script is executed in two batches on the selected hosts or Docker containers. The first batch is executed first. If the first batch is executed, the second batch start to be executed. If the first batch fails to be executed, the second batch is not executed. **Note** If you set Resource Type to docker, the selected Docker containers are automatically divided into batches based on the service role name so that Docker containers with the same service role are in different batches. ○ **Stop Waiting (You do not need to specify batches. The system executes jobs in two batches. After the execution of the first batch is complete, the process suspends. The second batch is executed after confirmation.)**: The script is executed in two batches on the selected hosts or Docker containers. The first batch is executed first. If the first batch is executed, a job approval is sent. The approver clicks **Passed** or **Stop** in **Job Review**. When the approval is passed, the second batch is executed. If the first batch fails to be executed, the execution is stopped and no job approval is sent. **Note** If you set Resource type to docker, the selected Docker containers are automatically divided into batches based on the service role name such that Docker containers with the same service role are in different batches. ○ **Phased execution rules apply to physical servers by default but are not applicable to VMs or Docker containers. (The default phased execution rule is a cluster-based algorithm and is executed automatically on multiple hosts in parallel.)**: This option is applicable only to physical machines, but not to VMs or Docker containers. The script is executed in batches based on the phased execution rules provided in Apsara Infrastructure Management Framework. After a batch is executed, a job approval is sent. The approver clicks **Passed** or **Stop** in **Job**

Parameter	Description
	Review. When the approval is passed, the next batch is executed. If the batch fails to be executed, the execution is stopped and no job approval is sent. Jobs are executed by cluster based on the following rules on the machines in each cluster: ■ For clusters in SLB, VPC, Apsara Infrastructure Management Framework, ApsaraDB RDS, MiniRDS, OSS, and Blink, the job is executed machine by machine. ■ For clusters other than the preceding ones and that contain 10 or fewer machines, the job is executed on the machines in the following order: 1 machine, 1 machine, 2 machines, 3 machines, and then the remaining machines. ■ For clusters other than the preceding ones and that contain more than 10 machines, the job is executed on the machines in the following order: 1 machine, 3 machines, 5 machines, N/3-1 (rounded down) machines, and N/3-1 machines until the job is executed on all the machines. N is the number of machines in the cluster. **Note** If a cluster contains both physical machines and VMs, the job is executed on all the VMs in the last batch. ○ **Custom**: You can set the batches on your own to execute the job. In the **Batch Settings** drop-down list, select the hosts or Docker containers to add. You can click the ⊕ icon to add batches or click the ⊖ icon to delete batches. You can add up to three batches. Set **Phased Execution Condition** to **Automatic Execution per Batch** or **Waiting for Review and Confirmation**. ■ **Automatic Execution per Batch**: A batch is executed first. If the batch is executed, the next batch start to be executed. If the batch fails to be executed, the next batch stops execution. ■ **Waiting for Review and Confirmation**: A batch is executed first. If the batch is executed, a job approval is sent. The approver clicks **Passed** or **Stop** in **Job Review**. When the approval is passed, the next batch starts execution. If the batch fails to be executed, the execution is stopped and no job approval is sent.

Parameter	Description

6. Click **Create**.

6.1.6.2. Import an O&M job

You can import existing O&M jobs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > O&M Jobs**.
4. Click **Import O&M Job**.
5. In the **Upload O&M Job** dialog box, click **Click Here to Upload** to upload an existing O&M Job.

   > **Note**
   >
   > - Only JSON files can be uploaded. The file to be uploaded cannot exceed 500 KB in size.
   > - An imported O&M job cannot be directly executed. You must select a host before you can execute the job.

6.1.6.3. View O&M jobs

You can view existing O&M jobs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > O&M Jobs**.
4. In the **O&M Job Name** search box, enter the name of the O&M job that you want to view and click **search**. Fuzzy match is supported. You can view information of the O&M job that meets the filter conditions, including the job name, O&M scenario, description, execution method, modification time, execution history, latest execution time, latest execution status, update user, and whether the job is set to default.
5. (Optional) Click **reset** to clear the filter conditions.
6. Click the number in the **Execution History** column to view the execution history of the job, including the start time, end time, execution method, execution result, and job information.
7. On the **Execution History** page, you can perform the following operations:
   - Click **View** in the **Details** column to view the execution details of each step on each host or Docker container.
   - Click **Snapshot Records** in the **Details** column to view the job history snapshot.
   - Click **Proceed** in the **Details** column to continue to execute the job.

> ⓘ **Note** If an O&M job is executed based on the phased execution rules and if you want to execute a subsequent batch when the previous batch fails to be executed, you can click **Proceed**.

- Select one or more execution history entries and click **Delete Execution History** above the list, or click **Delete** in the **Details** column corresponding to the entries. In the message that appears, click **OK**.

6.1.6.4. Export an O&M job

You can export existing O&M jobs to your computer.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > O&M Jobs**.
4. Select one or more O&M jobs that you want to export and click **Export O&M Job** to export the O&M jobs to your computer.

   > ⓘ **Note** If you export multiple O&M jobs at a time, the content of the jobs is stored in a single JSON file.

6.1.6.5. Modify an O&M job

After an O&M job is created or imported, you can modify the O&M job to suit your needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > O&M Jobs**.
4. Find the O&M job that you want to modify and click **Modify** in the **Actions** column.
5. On the Modify O&M Job page, modify the settings and click **Save**.

6.1.6.6. Execute an O&M job

You can manually execute O&M jobs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > O&M Jobs**.
4. Select the O&M job that you want to execute and click **Execute** in the **Actions** column.
5. In the Execute O&M Job message, click **OK**.

6.1.6.7. Delete an O&M job

You can delete O&M jobs that are no longer needed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > O&M Resources > O&M Jobs**.
4. Select one or more O&M jobs that you want to delete and click **Delete Job** in the lower part of the page, or click **Delete** in the **Actions** column.
5. In the message that appears, click **OK**.

6.1.7. Review jobs

If an O&M job is executed based on the phased execution rules, the system enables job review. After a batch is executed, the next batch does not start to be executed until the previous batch passes the review. You can pass or stop an O&M job.

Context

During the execution of an O&M job, the system can only judge whether the O&M job is executed, but cannot know the execution result. If the O&M personnel want to confirm the execution results of one batch before they execute the next batch, the O&M personnel can set **Phased Execution Rules** to **Stop Waiting (You do not need to specify batches. The system executes jobs in two batches. After the execution of the first batch is complete, the process suspends. The second batch is executed after confirmation.)** to review the O&M jobs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > Audit Management > Job Review**.
4. Select the O&M job that you want to review and click **Passed** in the **Actions** column to execute the next batch, or click **Stop** to stop the execution of the next batch.
5. In the message that appears, click **OK**.

6.1.8. Review processes

If a Manual node or a Task node for which **Phased Execution Settings** is set to **Stop Waiting** is available when a process is running, the system initiates process review. You can pass or stop the process.

Context

When a process is running, the system can judge whether the task is complete but cannot determine whether the task is correctly executed. If a Manual node or a Task node for which **Phased Execution Settings** is set to **Stop Waiting** is available in a process, the O&M personnel can view the task execution result to determine whether to pass or stop the process.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > Audit Management > Process Review**.
4. Select the process that you want to review and perform the following operations in the **Actions** column:
   - Click **Passed** to pass the process or run the next batch.
   - Click **Stop** to stop the process or stop the execution of the next batch.
5. In the message that appears, click **OK**.

6.1.9. View O&M logs

You can view the logs of various automated O&M operations.

Context

You can view the type, time, user, and details of automated O&M operations to help you perform subsequent audits.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Automated O&M > Audit Management > O&M Logs**.
4. Select an O&M operation type from the **Type** drop-down list, select the start time and end time of the O&M operation, and then click **search**. You can view the operation logs that meet the filter conditions, including the type, time, user, and details of the operation.
5. (Optional) Click **reset** to clear the filter conditions.

6.2. Network Operation Center

The Network Operation Center (NOC) is a comprehensive operations tool platform that covers the entire network (virtual and physical).

NOC provides operations capabilities such as the visualization of network-wide monitoring, automated implementation, automated fault location, and network traffic analysis to enhance the efficiency of network operations engineers, reduce operations risks, and improve the quality of Apsara Stack services.

6.2.1. Dashboard

6.2.1.1. View the dashboard

You can view the status of the current devices, network, and traffic on the Dashboard tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.

2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Dashboard**.
4. On the **Dashboard** tab, view the dashboard information.

Item		Description
Device Management	**Device Overview**	The model distribution of the network devices in use.
	Ports Usage	○ **Ports Utilization**: the proportion of the number of ports in use to the total number of ports in the network devices. ○ **Error Packets by Port Top 5**: the total number of error packets generated by the device ports within a specified time range, of which the top 5 are displayed.
	Configuration Management	○ **Automatic Backup**: shows the proportions of **Backup Completed**, **Connection Failed**, and **Out-of-Scope** data sources. Move the pointer over the corresponding section and the details are displayed. ○ **Configuration Sync**: shows the proportions of **Configuration Synchronized**, **Connection Failed**, and **Out-of-Scope** data sources. Move the pointer over the corresponding section and the details are displayed.
Network Monitoring	**Alerts**	The total number of alerts generated by network devices.
	Alerting Devices	The number of network devices that generate alerts and the total number of network devices.
	Alarm Details	The details of the alert.
Traffic Dashboard	**SLB Overview**	The bandwidth utilization of SLB clusters.
	XGW Overview	The bandwidth utilization of XGW clusters.

6.2.1.2. View the network topology

You can view the physical network topology on the **Network Topology** tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.

3. In the left-side navigation pane, choose **Network Operations Center > Dashboard**.
4. Click the **Network Topology** tab.
5. On the **Network Topology** tab, view the physical network topology of a physical data center.

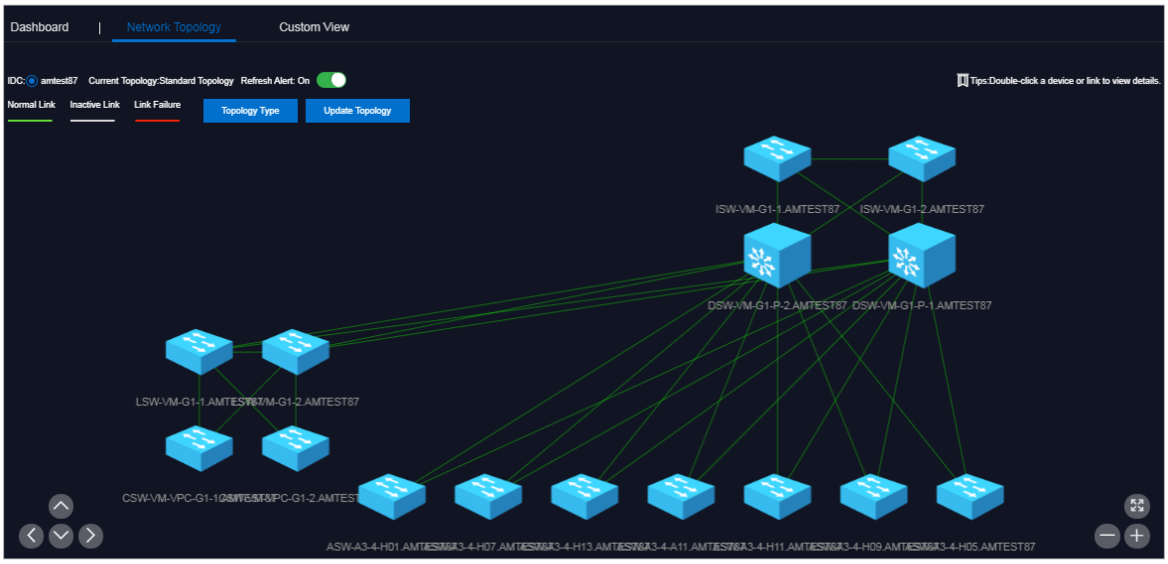
   You can set **Topology Type** to **Standard Topology** or **Dynamic Topology**.

   If an offset exists between the dynamic topology and the standard topology, a message appears when you go to the **Network Topology** tab in the upper-right corner of the tab and disappears after a few seconds. You can click **Update Topology** to update the standard topology.

   > **Note**
   >
   > The colors of connections between network devices indicate the connectivity between the network devices:
   >
   > - Green: The connection works normally.
   > - Red: The connection has an error.
   > - Grey: The connection is inactive.

   By default, if **Topology Type** is set to **Standard Topology**, the **Refresh Alert** switch is turned on. You can turn off **Refresh Alert** to stop receiving new alerts that are triggered for the devices or connection statuses within the topology.

   If **Topology Type** is set to **Dynamic Topology**, **Refresh Alert** is turned off.



Dashboard | Network Topology | Custom View

IDC: ● amtest87 Current Topology:Standard Topology Refresh Alert: On

Tips:Double-click a device or link to view details.

Normal Link Inactive Link Link Failure

Topology Type

Update Topology

6. In the topology, double-click a connection between two devices to view the connection and alerts between the two devices.
7. In the topology, double-click a physical network device to view the basic information and node alerts of the device on the right.

6.2.1.3. Manage custom views

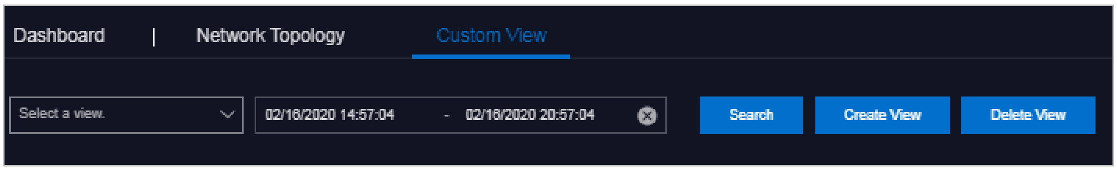
You can create a custom view to configure how to show the independent monitoring data set. You can configure the content and rules to display in the view to summarize and demonstrate the monitoring data and graph information you are interested in.

Go to the Dashboard page

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Dashboard**.

Create a view

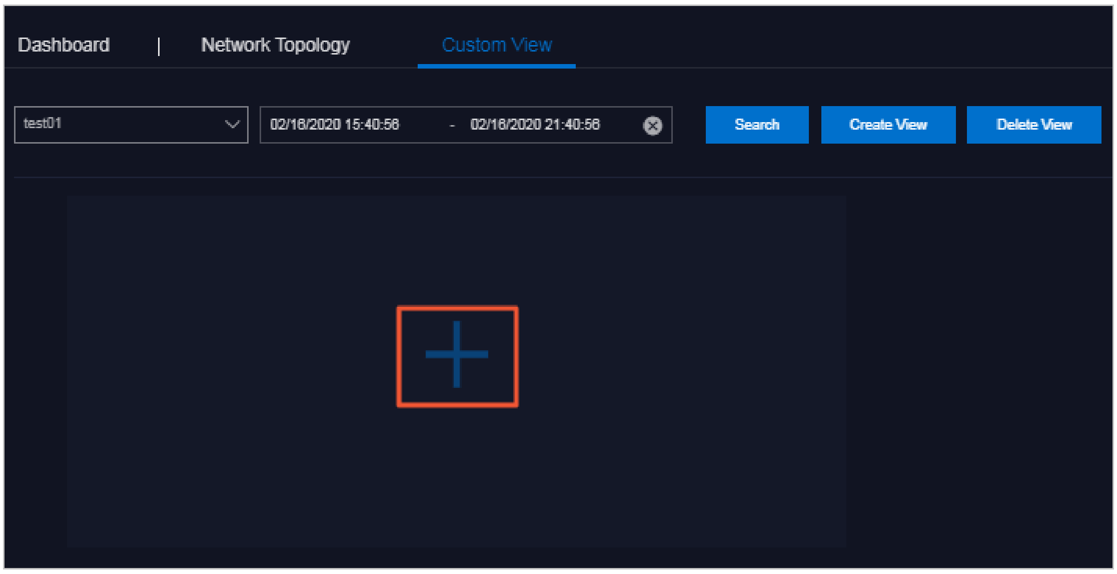
1. Click the **Custom View** tab.
2. Create a view.
   i. In the upper part of the tab, click **Create View**.



   ii. In the dialog box that appears, set View Name and Description and click **OK**.

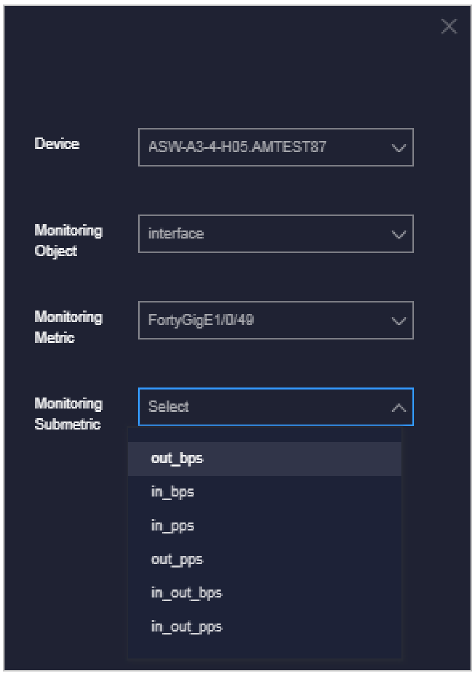
   The view name cannot be the same as the name of an existing view. If the **A view with the same name already exists** message appears, you must change the view name to a unique one and then click **OK**.

3. Add a subview. By default, no subviews exist in a view after you create the view.
   i. Select the created view from the drop-down list in the upper part of the page, select a start time and an end time, and then click **Search**.



   ii. Click the + icon.

iii. In the panel that appears, configure the parameters described in the following table.



Device: ASW-A3-4-H05.AMTEST87

Monitoring Object: interface

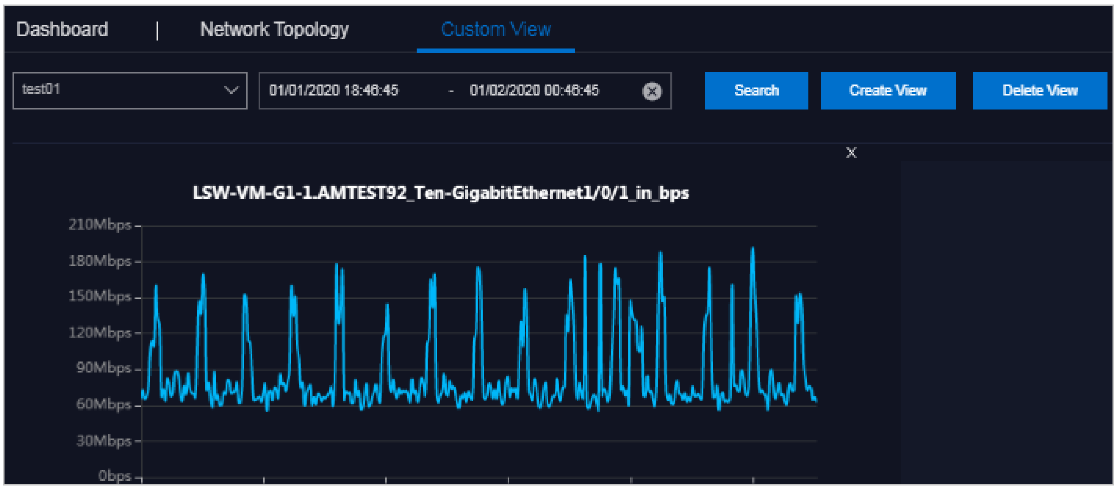
Monitoring Metric: FortyGigE1/0/49

Monitoring Submetric: Select

Parameter	Description
Device	Required. Select the device to be monitored from the drop-down list.
Monitoring Object	Required. Select the monitoring object from the drop-down list. - **interface**: the switch interface, including the water level, packet error, and packet loss of the interface. - **hardware**: the switch hardware, including the memory usage and CPU usage. - **capacity**: others, which is not supported.
Monitoring Metric	Required. Select the corresponding monitoring metric from the drop-down list.
Monitoring Submetric	Optional. Select the corresponding monitoring submetric from the drop-down list.

iv. Click **OK**.

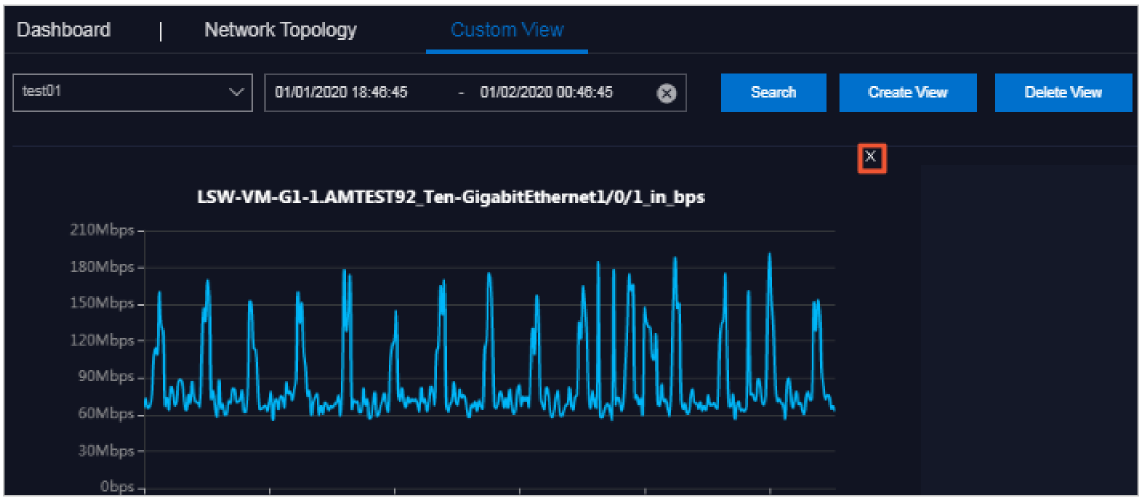
After the subview is added, the system automatically shows the subview on the view to which the subview belongs.



v. You can add other subviews.

Delete a subview

1. Click the **Custom View** tab.
2. Select the view to which the subview that you want to delete belongs from the drop-down list in the upper part of the page, select a start time and an end time, and then click **Search**.
3. Click the x icon in the upper-right corner of the subview.



4. In the message that appears, click **OK**.

Delete a view

Notice If you delete a view, all subviews of the view are also deleted. Proceed with caution.

1. Click the **Custom View** tab.
2. Select the view that you want to delete from the drop-down list in the upper part of the page, select a start time and an end time, and then click **Search**.

3. Click **Delete View** in the upper part of the tab.
4. In the message that appears, click **OK**.

6.2.2. Network element management

Network elements are network devices such as vSwitches and routers. The Network Element Management module shows the basic information and running status of physical network devices. The module also provides configuration management operations for physical network devices, including device management, password management, and configuration comparsion.

6.2.2.1. Device management

The Device Management module shows the basic information, running status, traffic monitoring information, and logs of physical network element devices. The module also allows you to configure the collection settings of network devices.

6.2.2.1.1. View the network monitoring information

The Network Monitoring tab allows you to view the basic information, running status, and traffic monitoring information of Apsara Stack physical network devices and check the health status of network devices in a timely manner.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Network Element Management**.
4. On the **Device Management** tab, click the **Network Monitoring** tab.
5. In the upper part of the tab, select an IDC and perform the following operations:
   - View the basic information, ping status, and SNMP status of Apsara Stack physical network devices.

     > **Note** You can also click **Export to CSV** to export network device information to your computer.

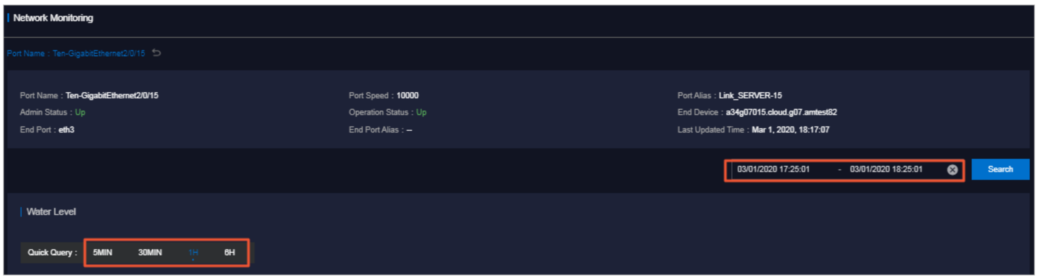
     If a device has a business connectivity or gateway connectivity problem, the value in the Ping Status or SNMP Status column turns from green to red. The O&M personnel must troubleshoot the problem.
   - In the upper-right corner of the tab, enter the device name or IP address in the search box to search for the monitoring information of a specific device.
   - View the port information, CPU utilization, memory usage, aggregation port information, and alert information of a device.
     a. Click a device name, or click **View** in the **Details** column corresponding to a device.

b. On the **Port** tab, view the ports, port operation status, and other link information of the device.

   a. In the upper-right corner of the **Port** tab, search for the port that you are about to view by using the search box. Click **View** in the **Details** column corresponding to the port.

   b. Select a time range on the right and click **Search** to view the traffic in the selected time range.

      You can select 5MIN, 30MIN, 1H, 6H for **Quick Query** to view the traffic within the last 5 minutes, 30 minutes, 1 hour, or 6 hours.

      Network Monitoring

      Port Name : Ten-GigabitEthernet2/0/15

Port Name : Ten-GigabitEthernet2/0/15	Port Speed : 10000	Port Alias : Link_SERVER-15
Admin Status : Up	Operation Status : Up	End Device : a34g07015.cloud.g07.amtest82
End Port : eth3	End Port Alias : --	Last Updated Time : Mar 1, 2020, 18:17:07

      03/01/2020 17:25:01 - 03/01/2020 18:25:01

c. On the **CPU Utilization** tab, view all the CPU utilization information of the device.

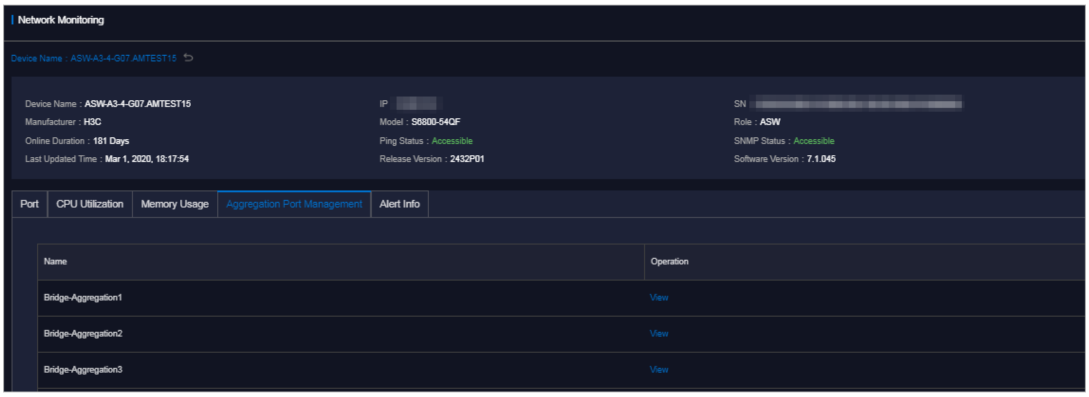
d. On the **Memory Usage** tab, view all the memory usage information of the device.

e. On the **Aggregation Port Management** tab, view all the aggregation port information of the device. You can click **View** in the **Operation** column corresponding to a port to view the usage of the aggregation port.

f. On the **Alert Info** tab, view the alert information of the device.

   During routine O&M, you must closely monitor the alert list of the device. Typically, if no data is displayed on the **Alert Info** tab, the device is operating normally.

   If alert events occur, unrecovered alert events are displayed in the list. You must handle these exceptions in a timely manner. When exceptions are handled, their corresponding alerts are automatically cleared from the list.

   Network Monitoring

   Device Name : ASW-A3-4-G07.AMTEST15

Device Name : ASW-A3-4-G07.AMTEST15	IP [redacted]	SN [redacted]
Manufacturer : H3C	Model : S6800-54QF	Role : ASW
Online Duration : 181 Days	Ping Status : Accessible	SNMP Status : Accessible
Last Updated Time : Mar 1, 2020, 18:17:54	Release Version : 2432P01	Software Version : 7.1.045

Name	Operation
Bridge-Aggregation1	View
Bridge-Aggregation2	View
Bridge-Aggregation3	View

6.2.2.1.2. View logs

The Syslogs tab allows you to view logs of physical network element devices and provides necessary data for fault location and diagnosis information collection.

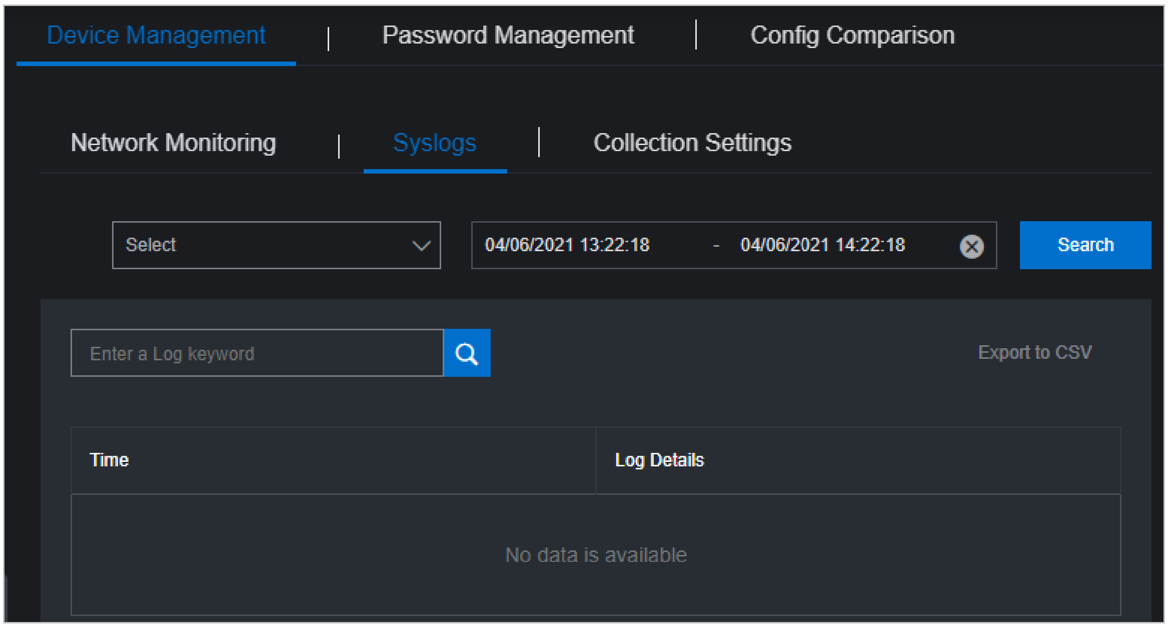
Context

During the daily inspection, you can search for logs generated by a specific network device during a specific time range on the **Syslogs** tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Network Element Management**.
4. On the **Device Management** tab, click the **Syslogs** tab.
5. In the upper-right corner of the tab, select a device name from the drop-down list, select a time range, and then click **Search** to check for system logs generated by the device within the specified time range.

   If the device has a configuration exception or does not have any generated logs for the specified time range, no search results are returned.



Time	Log Details
No data is available	

6. (Optional)You can filter the search results based on log keywords.
7. (Optional)Click **Export to CSV** in the upper-right corner to export the search results to your computer.

6.2.2.1.3. Collection settings

The Collection Settings tab allows you to set the collection interval of physical network element devices and manage OOB network segments.

6.2.2.1.3.1. Configure the collection interval

Before you collect network device information, you must configure a collection interval.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.

2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Network Element Management**.
4. On the **Device Management** tab, click the **Collection Settings** tab.
5. In the **Collection Interval Settings** section, configure the auto scan interval, device scan interval, port scan interval, and link scan interval.

   If you have no special requirements, we recommend that you use the initial default value.
6. Click **Submit**. Then, the system collects the device information based on your configurations.

6.2.2.1.3.2. Modify the collection interval

This topic describes how to modify the interval at which network device information is collected.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Network Element Management**.
4. On the **Device Management** tab, click the **Collection Settings** tab.
5. In the **Collection Interval Settings** section, modify the parameter values.

   > ? **Note** To cancel your modification before you submit it, click **Reset** in the upper-right corner to reset the collection interval to the previous version.
6. Click **Submit**. The modified collection interval of the network device information takes effect after 1 minute.

6.2.2.1.3.3. Add an OOB network segment

If this is the first time you are using the Network Elements feature of Network Operations Center (NOC), you must add the device loopback network segment planned by the current Apsara Stack network device, which is typically the network segment of the netdev.loopback field in the IP address planning list.

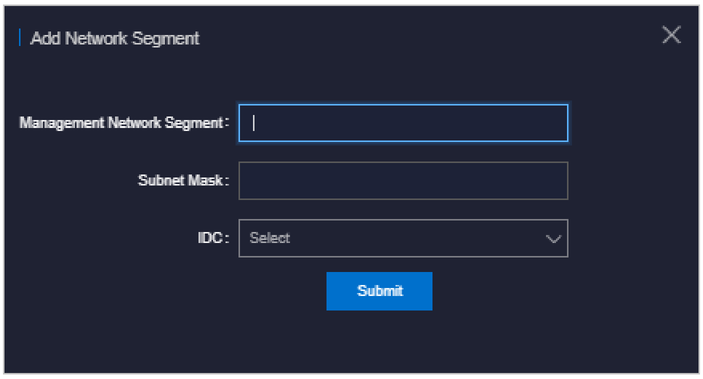
Context

The OOB Network Segments section is used to configure the management scope of a physical network element device. Typically, O&M engineers must add the loopback network segment in which the network device to be managed resides.

In the Apsara Stack scenario, a loopback network segment is used to configure the management scope of a physical network element device. To expand the network and the loopback network segment, you must add the network segment involved in the expansion to the management scope. The procedure to add an expanded network segment is the same as that used to add the loopback network segment for the first time. Then, you can search for the network segment of the managed device on this page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the left-side navigation pane, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Network Element Management**.
4. On the **Device Management** tab, click the **Collection Settings** tab.
5. In the lower part of the **OOB Network Segments** section, click **Add Network Segment**.
6. In the Add Network Segment dialog box, enter the network segment that contains the mask information and a subnet mask and select an IDC.



7. Click **Submit**. The initial data entry is complete.

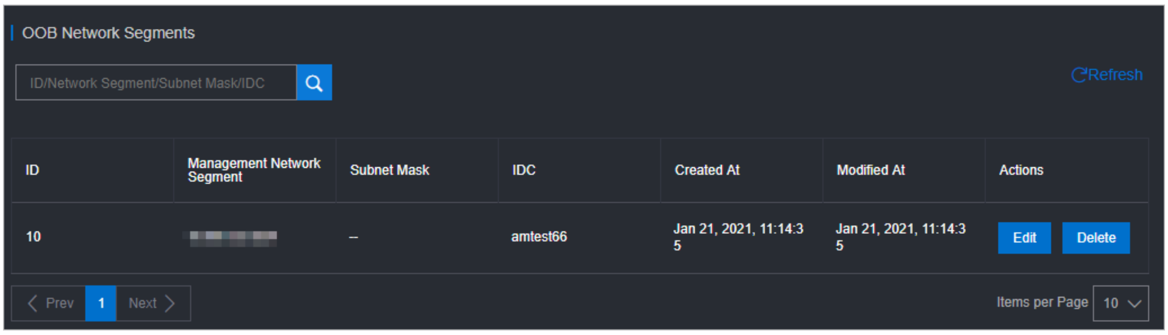
   To modify or delete an OOB network segment, find it in the list and click **Edit** or **Delete** in the **Actions** column.

6.2.2.1.3.4. View the OOB network segment information

You can search for and view the network segment information of your managed devices.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Network Element Management**.
4. On the **Device Management** tab, click the **Collection Settings** tab.
5. In the **OOB Network Management** section, click **Refresh** in the upper-right corner of the section.



ID	Management Network Segment	Subnet Mask	IDC	Created At	Modified At	Actions
10	[redacted]	–	amtest66	Jan 21, 2021, 11:14:35	Jan 21, 2021, 11:14:35	Edit Delete

6. In the list, view the network segment information of your managed devices.

> ⓘ **Note** You can search for the information of a specific network segment by entering keywords in the search box.

6.2.2.2. Modify the device password

You can modify the passwords of physical network devices.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Network Element Management**.
4. Click the **Password Management** tab.
5. (Optional)Enter the name of the device for which you want to modify the password in the search box of the **Devices on Live Network** section and click **Search**. To search for another device, you can click **Reset** to reset the previous search conditions.
6. Select one or more devices and click **Add**. The selected devices are displayed in the **Target Devices** section on the right.

   > ⓘ **Note** To remove a device from the **Target Devices** section, choose **Manage > Delete** in the **Actions** column corresponding to the device. You can also click **Clear** in the upper-right corner to remove all the devices from the Target Devices section.

7. The system must verify the old password before you modify it. Enter **Username** and **Old Password** in the lower-right corner and click **Verify**. You must verify the old passwords for all the devices in the **Target Devices** section.
8. After the verification is passed, you can modify the password for one or more devices.
   - Modify the password of a device

     Choose **Manage > Set Username and Password** in the **Actions** column corresponding to a device. In the dialog box that appears, enter the username and password and click **OK**.
   - Modify the passwords of all devices
     a. In the lower part of the **Target Devices** section, click **Modify**.
     b. In the dialog box that appears, enter and confirm the new password, and then click **OK**. The passwords of all the devices that are added to the **Target Devices** section are modified.

6.2.2.3. Compare device configurations

You can compare the current configuration of a device with its configuration on startup and check whether they are consistent.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.

3. In the left-side navigation pane, choose **Network Operations Center > Network Element Management**.
4. Click the **Config Comparison** tab.
5. (Optional)Enter the name of the device whose configurations you want to compare in the **Device Name** search box and click **Search**. To search for more devices, you can click **Reset** to reset the configured search condition.
6. Select devices and click **Compare Configuration**. After you compare the configurations, click **Refresh** and click **Export Results**.

6.2.3. SLB management

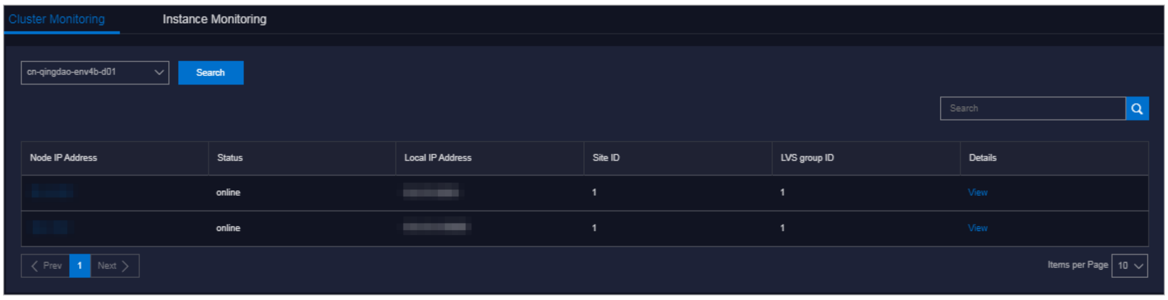
The SLB Management module contains the Cluster Monitoring and Instance Monitoring tabs and shows the basic information, running status, and usage of SLB network products.

6.2.3.1. View cluster monitoring information

The Cluster Monitoring tab allows you to view the basic information, inbound limit (bit/s), outbound limit (bit/s), inbound limit (PPS), outbound limit (PPS), active connection limit, inactive connection limit, and usage of a single device node in a cluster.

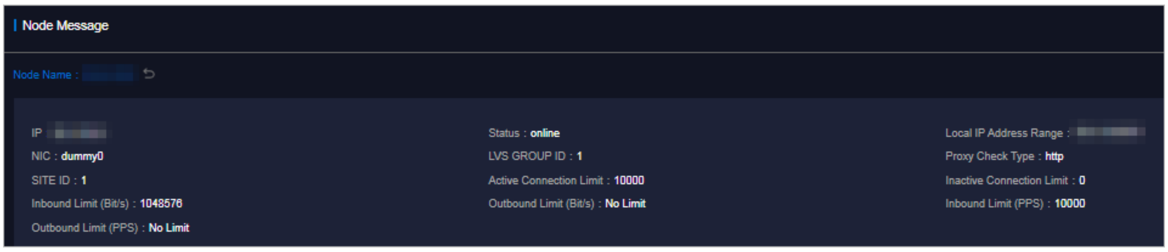
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > SLB Management**.
4. The **Cluster Monitoring** tab appears.
5. Select the cluster that you want to view from the drop-down list and click **Search**. Information of all the device nodes in the cluster is displayed.



Node IP Address	Status	Local IP Address	Site ID	LVS group ID	Details
[redacted]	online	[redacted]	1	1	View
[redacted]	online	[redacted]	1	1	View

6. Find a device node and click **View** in the **Details** column.
7. On the **Node Message** page, view the basic information, inbound limit (bit/s), outbound limit (bit/s), inbound limit (PPS), outbound limit (PPS), active connection limit, and inactive connection limit of the device node.



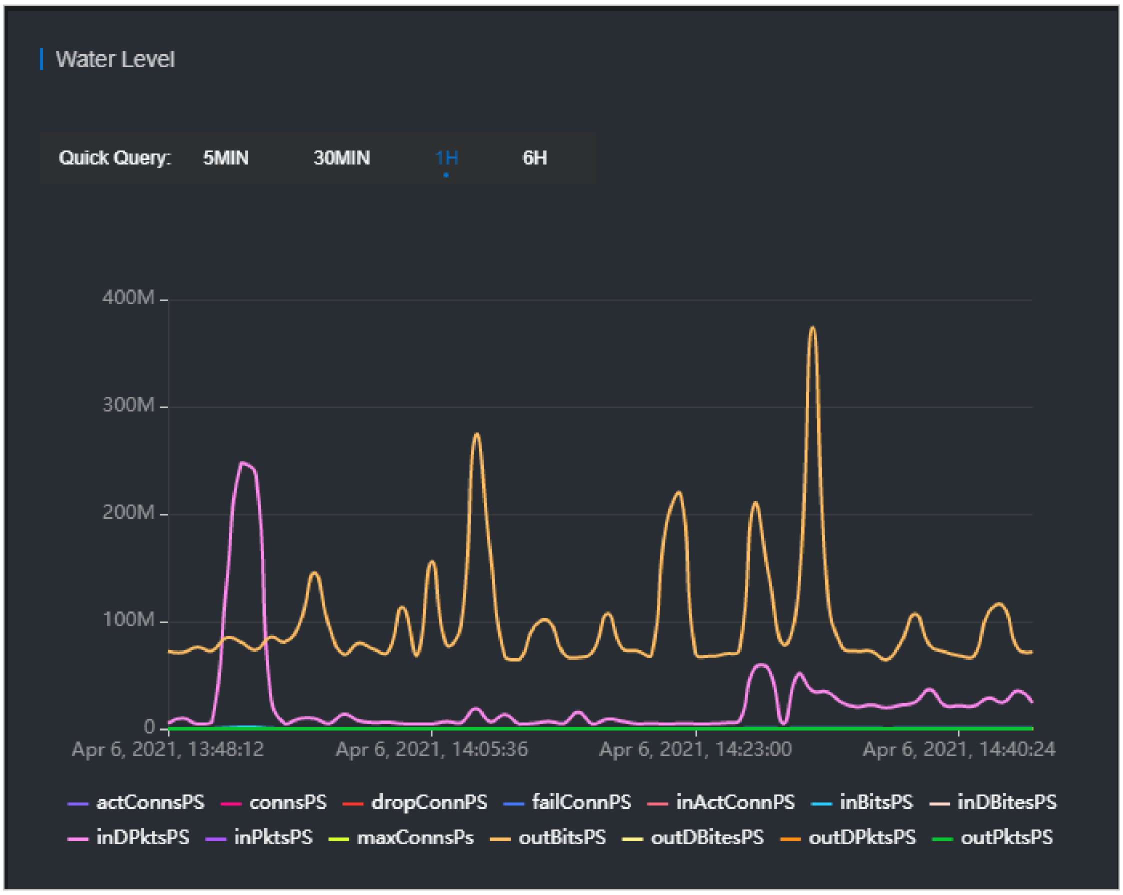
Node Name : [redacted]

IP [redacted]
NIC : dummy0
SITE ID : 1
Inbound Limit (Bit/s) : 1048576
Outbound Limit (PPS) : No Limit

Status : online
LVS GROUP ID : 1
Active Connection Limit : 10000
Outbound Limit (Bit/s) : No Limit

Local IP Address Range : [redacted]
Proxy Check Type : http
Inactive Connection Limit : 0
Inbound Limit (PPS) : 10000

8. On the **Node Message** page, view the usage information of the device node.



- In the upper-right corner, you can set the start and end time and click **Search** to view the usage data within the specified time range.
- You can also click **5MIN**, **30MIN**, **1H**, or **6H** in the upper-left corner to query the usage data within the corresponding time range.
- Click a metric in the lower part of the chart, and the curve corresponding to the metric disappears from the chart. Click the metric again, the curve appears.
- Move the pointer over a point in time to display the values of all metrics for that point in time.

Metric	Description	Example
actConnsPS	The number of active connections.	0
connsPS	The number of new connections.	1
dropConnsPS	The number of connections dropped per second.	0
failConnPS	The number of connections failed per second.	0
inActConnPS	The number of inactive connections.	1

Metric	Description	Example
inBitsPS	The amount of inbound data per second.	248
inDBitesPS	The amount of inbound data dropped per second.	0
inDPktsPS	The number of inbound packets dropped per second.	0
inPktsPS	The number of inbound packets per second.	1
maxConnsPs	The total number of connections.	1
outBitsPS	The amount of outbound data per second.	208
outDBitesPS	The amount of outbound data dropped per second.	0
outDPktsPS	The number of outbound packets dropped per second.	0
outPktsPS	The number of outbound packets per second.	1

6.2.3.2. View the instance monitoring information

The Instance Monitoring tab allows you to view the basic information and usage of an instance, including the BPS and PPS.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > SLB Management**.
4. Click the **Instance Monitoring** tab.
5. Select the cluster where the instance that you want to view is located from the Cluster drop-down list. Enter the ID or VIP address of the instance that you want to query in the search box and click **Search**.
6. In the query result, view the monitoring information of the instance.
    - The first section shows the basic information of the SLB instance, which allows O&M engineers to troubleshoot problems and confirm the owner of a device.
    - The second section shows the operating graph of the instance. Select a time range and click **Search**, or select 5MIM, 30MIN, 1H, or 6H in the Quick Query section to view the operating graph of the instance in a specific time range, including the detailed BPS and PPS.

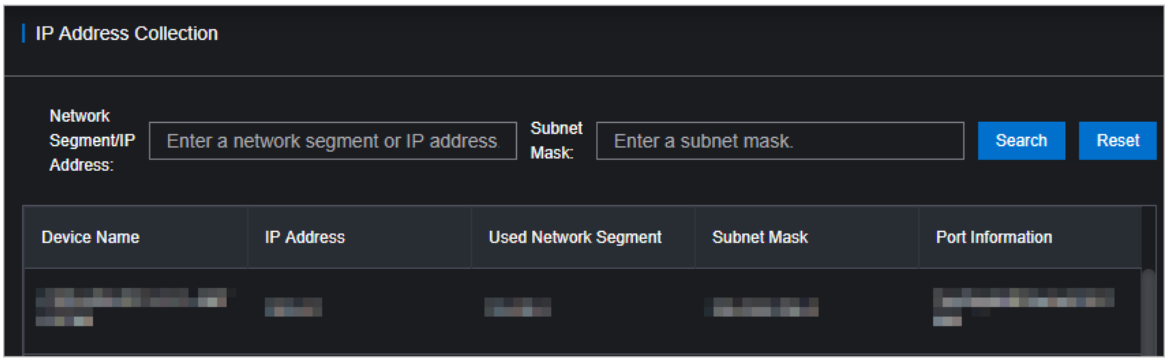
6.2.4. Collect IP addresses

The system routinely collects the IP addresses of all physical networks within the current Apsara Stack environment at a specified collection interval. You can use a CIDR block or IP address, and subnet mask to search for the information of corresponding devices and ports.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > IP Address Collection**.
4. Enter the CIDR block or IP address and subnet mask in the corresponding search boxes, and then click **Search**. If the CIDR block you are searching for belongs to a CIDR block in the current Apsara Stack environment, the system shows the information of devices and ports to which the specified CIDR block belongs.

   > **Note** If you enter an IP address in the search box and then click Search, the system calculates the corresponding CIDR block based on the IP address and subnet mask.



IP Address Collection

Network Segment/IP Address: Enter a network segment or IP address

Subnet Mask: Enter a subnet mask.

Device Name	IP Address	Used Network Segment	Subnet Mask	Port Information
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

6.2.5. IP address range management

The IP Address Ranges module allows you to manage planning information in the Apsara Stack environment, including the network architecture and address planning. You can modify, import, and export the planning information.

6.2.5.1. Import the planning file

No data is imported at the time the system is initialized. You must import the planning file to obtain the IP address allocation information of the current Apsara Stack environment. You can also import a new planning file for a change in the environment.

Prerequisites

The IP address allocation table is obtained from the Apsara Stack deployment planner. If you have not obtained the allocation table, contact your account manager or submit a Apsara Stack ticket.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.

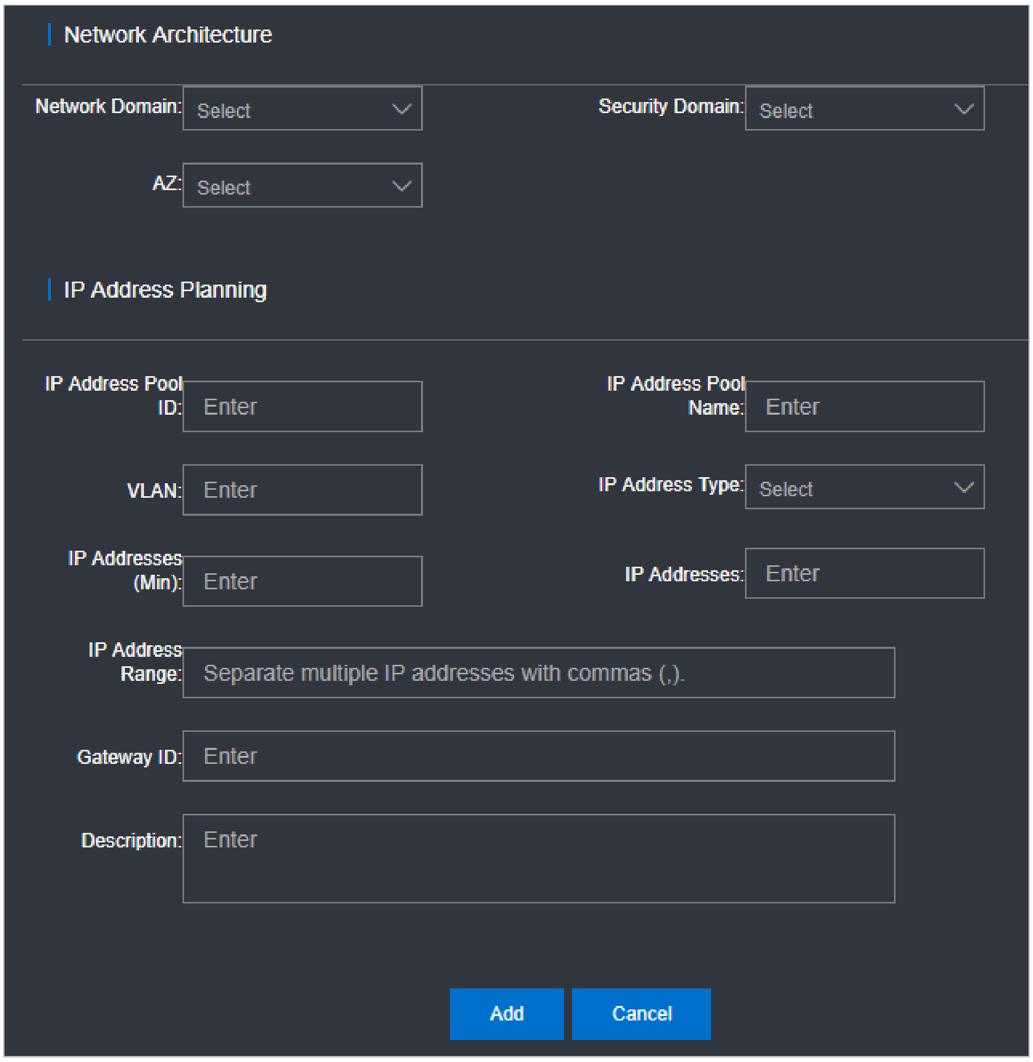
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > IP Address Ranges**.
4. Click **Import** in the upper-right corner.
5. In the dialog box that appears, click **Select a file to upload** or **Browse** and select the IP address allocation list.
6. Click **Import**.

6.2.5.2. Manually add the IP address pool information

You can also manually add new IP address pool information to the Apsara Uni-manager Operations Console for centralized management.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Console > IP Address Ranges**.
4. Click **Add**.
5. In the dialog box that appears, configure the IP address pool information.



6. Click **Add**.

6.2.5.3. Modify the IP address pool information

If an IP address range is changed, you can modify the IP address pool information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > IP Address Ranges**.
4. (Optional)On the **IP Address Ranges** page, configure the search conditions and click **Search**.

> **Note** To reset the search conditions, you can click **Reset** to clear your configurations with one click.

5. Find the IP address pool for which you want to modify the configurations and choose **Manage > Modify** in the **Actions** column.
6. In the dialog box that appears, modify the network architecture and IP address planning.

7. Click **Edit**.

6.2.5.4. Export the IP address pool information

You can export the IP address pool information to your computer and then view the information offline.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > IP Address Ranges**.
4. Select IP address pools that you want to export and click **Export**.

6.2.5.5. Delete an IP address pool

You can delete IP address pools that are no longer needed.

Procedure

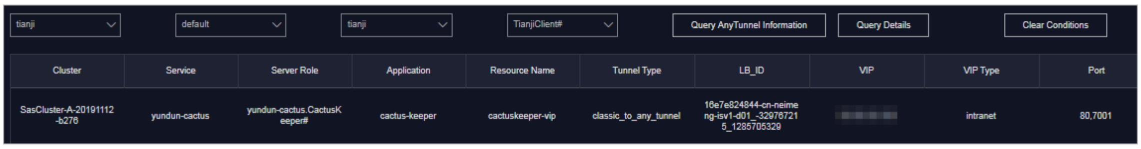
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > IP Address Ranges**.
4. Find the IP address pool that you want to delete and choose **Manage > Delete** in the **Actions** column.

6.2.6. View Anytunnel information

You can view the Anytunnel information to see the Anytunnel resources registered by projects within the current environment or whether a project has Anytunnel registered. The system allows you to query the registration information of Anytunnel resources based on the project, cluster, service instance, and server role. You can use the global query feature to query the usage of all the Anytunnel resources in the current environment.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Anytunnel Management**.
4. Query all information or specific information. Perform the following steps:
    - In the upper part of the page, click **Query Details** to view all the Anytunnel information in the environment.



tianji | default | tianji | TianjiClient#

Cluster	Service	Server Role	Application	Resource Name	Tunnel Type	LB_ID	VIP	VIP Type	Port
SasCluster-A-20191112-b276	yundun-cactus	yundun-cactus.CactusKeeper#	cactus-keeper	cactuskeeper-vip	classic_to_any_tunnel	16e7e824844-cn-neimeng-isv1-d01_-329767215_1285705329	[redacted]	intranet	80,7001

    - In the upper part of the page, select the project, cluster, service instance, or service role, and then click **Query AnyTunnel Information** to view the AnyTunnel information that meets the search conditions.

> ? **Note** You can click **Clear Conditions** and modify the search conditions.

6.2.7. XGW management

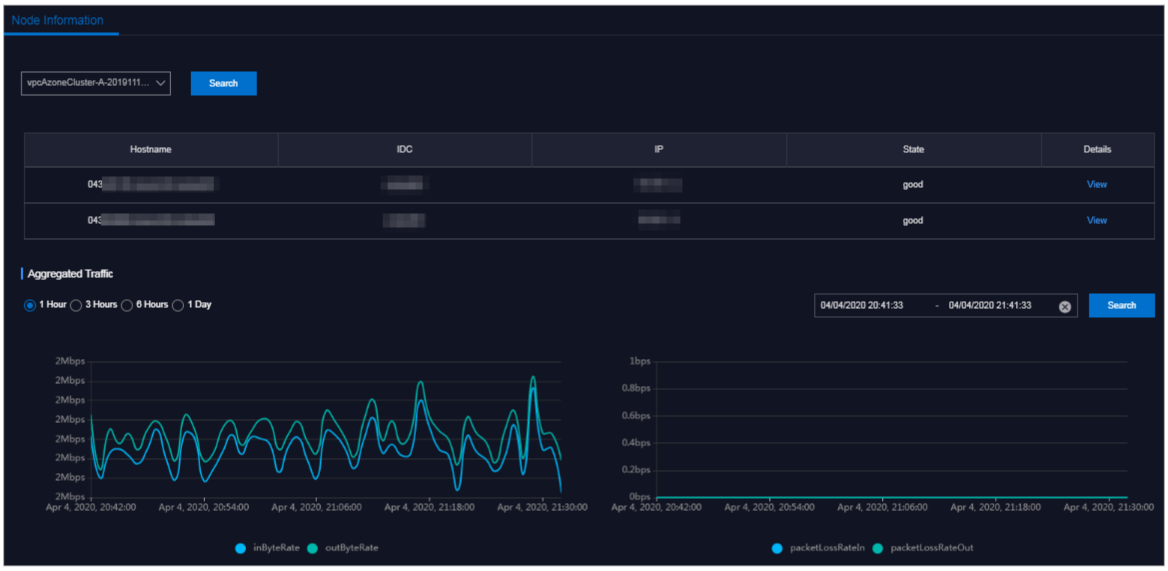
The XGW Management module allows you to manage VPC gateways and view the usage information of device nodes and service instances.

6.2.7.1. View node information

The XGW Management module allows you to view the basic information, running status, aggregated traffic, and usage of each device node of XGW network products.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > XGW Management**.
4. Select the cluster that you want to view from the drop-down list and click **Search**. The system shows the basic information and usage information of aggregated traffic of all device nodes within the selected cluster. By default, the usage information of the last one hour is displayed. You can select 1 hour, 3 hours, 6 hours, or one day as the time range, or customize the time range to search for the usage information.



Node Information

vpcAzoneCluster-A-2019111... Search

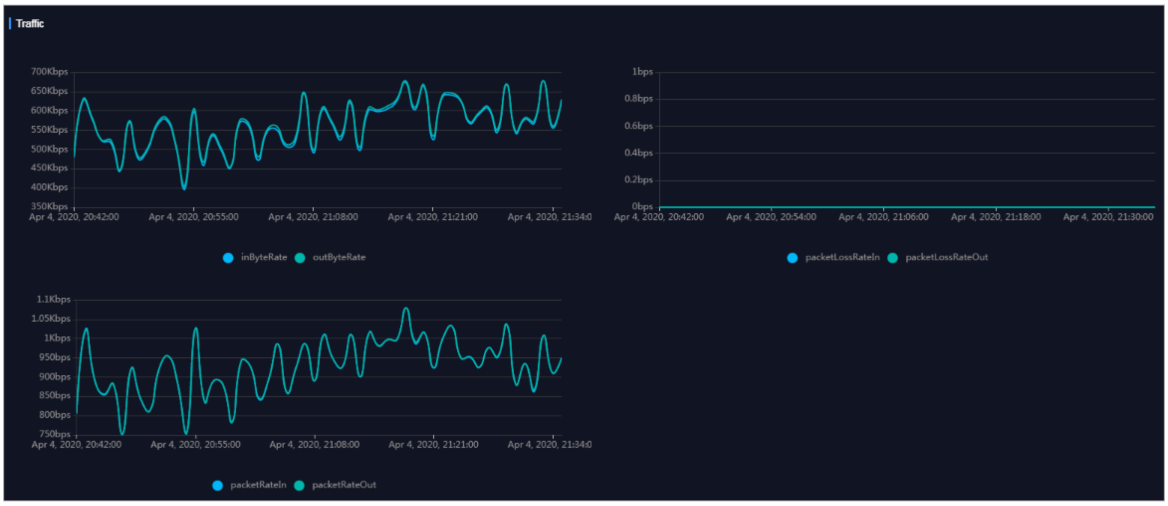
Hostname	IDC	IP	State	Details
043[redacted]	[redacted]	[redacted]	good	View
043[redacted]	[redacted]	[redacted]	good	View

Aggregated Traffic

● 1 Hour ○ 3 Hours ○ 6 Hours ○ 1 Day

04/04/2020 20:41:33 - 04/04/2020 21:41:33 Search

5. Find a device node and click **View** in the **Details** column.
6. On the page that appears, view the traffic usage information of the device node.



6.2.7.2. View the instance monitoring information

The Instance Monitoring tab allows you to view information such as bps, pps, drop_speed, fin_speed, ratelimit_drop_speed, rst_speed, and syn_ack_speed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > XGW Management**.
4. Click the **Instance Monitoring** tab.
5. Select the cluster where the instance you want to view is located from the drop-down list, enter the instance ID (EIP address) in the search box, and then click **Search**. By default, the data information within the last one hour is displayed. You can select a time range such as 5 minutes, 30 minutes, 1 hour, or 6 hours.

Item	Description
in_bps	The data receiving rate. Unit: bit/s.
in_drop_speed	The inbound packet loss rate. Unit: PPS.
in_fin_speed	The inbound Fin packet forwarding rate. Unit: PPS.
in_pps	The inbound packet forwarding rate. Unit: PPS.
in_ratelimit_drop_speed	The inbound throttling packet loss rate. Unit: PPS.
in_rst_speed	The inbound RST packet forwarding rate. Unit: PPS.
in_syn_ack_speed	The inbound SYN/ACK packet forwarding rate. Unit: PPS.
out_bps	The data sending rate. Unit: bit/s.
out_drop_speed	The outbound packet loss rate. Unit: PPS.

Item	Description
out_fin_speed	The outbound FIN packet forwarding rate. Unit: PPS.
out_pps	The outbound packet forwarding rate. Unit: PPS.
out_ratelimit_drop_speed	The outbound throttling packet loss rate. Unit: PPS.
out_rst_speed	The outbound RST packet forwarding rate. Unit: PPS.
out_syn_ack_speed	The outbound SYN/ACK packet forwarding rate. Unit: PPS.

6.2.8. Firewall management

If the cloud firewall is deployed in your environment, you can use the firewall feature to isolate or restore the firewall.

Prerequisites

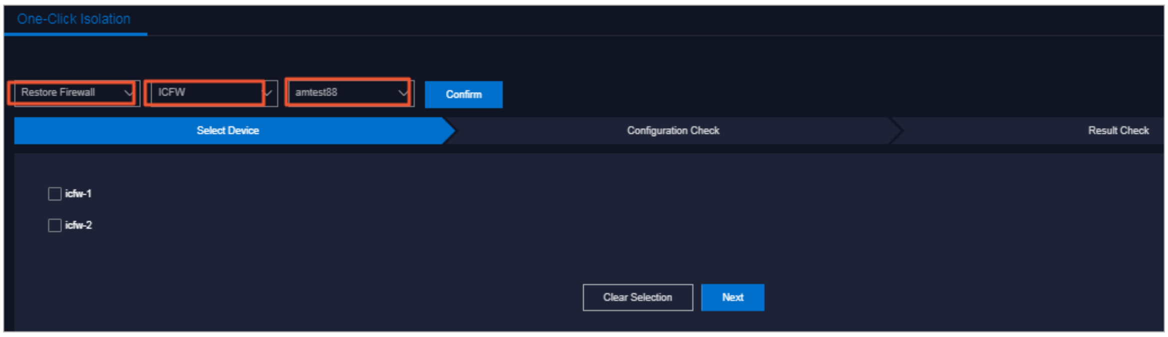
Notice Confirm with the administrator that the cloud firewall is deployed in your environment. Otherwise, you cannot use the firewall feature to isolate or restore the firewall.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Cloud Firewall Management**.
4. Select the operation type, firewall type, and data center from the corresponding drop-down list and click **Confirm**.

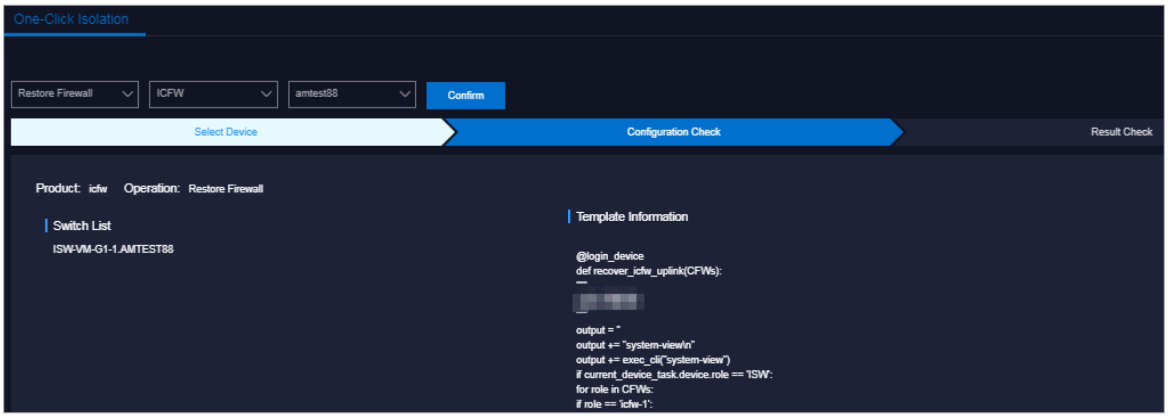
   Supported operations:

   - **Isolate Firewall**: physically isolates the firewall from the network structure. If an exception occurs on the cloud firewall service, the system removes the firewall device from the network forwarding path to ensure that the normal business traffic forwarding is not affected.
   - **Restore Firewall**: restores the firewall from the network isolated state to the normal state. After the exception on the cloud firewall is resolved, the system restores the firewall device back to the network forwarding path to ensure that the firewall is restored to the initial online status.



5. In the **Select Device** step, select devices and click **Next**.

6. In the **Configuration Check** step, check the selected devices and template information. If the information is correct, click **Confirm**.



Product: icfw Operation: Restore Firewall

Switch List

ISW-VM-G1-1.AMTEST88

Template Information

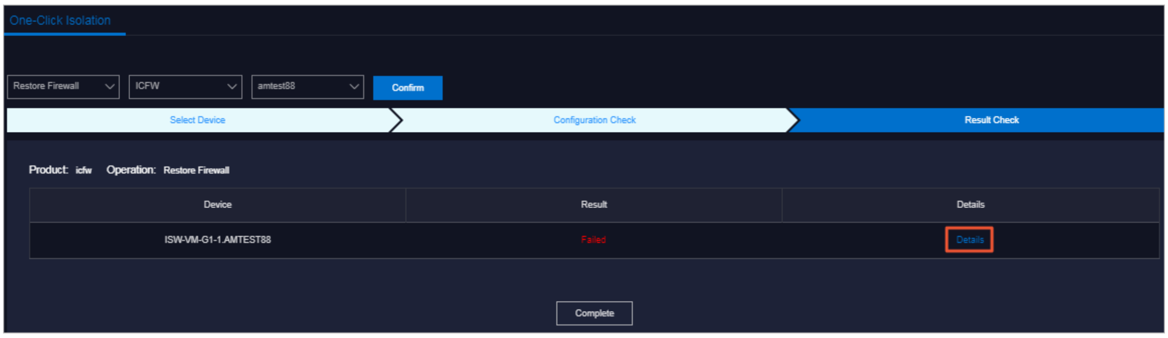
```
@login_device
def recover_icfw_uplink(CFWs):
—
[redacted]
—
output = "
output += "system-view\n"
output += exec_cli("system-view")
if current_device_task.device.role == 'ISW':
for role in CFWs:
if role == 'icfw-1':
```

7. In the message that appears, click **OK**.

   Then, the system automatically isolates or restores the firewall in the selected devices based on the configuration template.

   The results are automatically displayed in the **Result Check** step.

8. In the **Result Check** step, click **Details** in the **Details** column corresponding to each device to view the corresponding result.



Product: icfw Operation: Restore Firewall

Device	Result	Details
ISW-VM-G1-1.AMTEST88	Failed	Details

9. Click **Complete**.

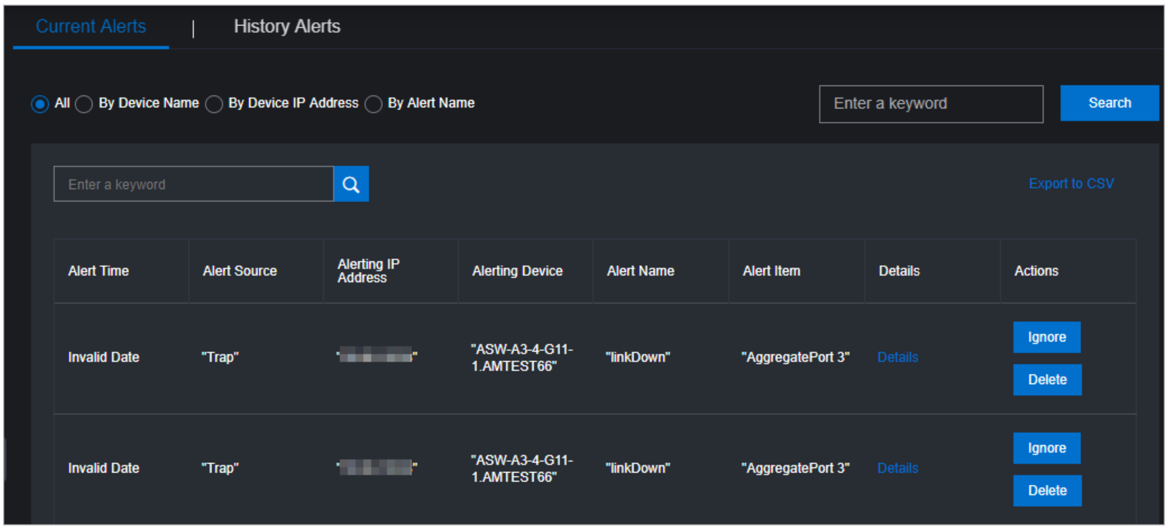
6.2.9. Alerts

6.2.9.1. View and process current alerts

You can view and process current alerts on the Current Alerts tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Alerts**.
4. Click the **Current Alerts** tab.
5. In the upper-right corner, enter a keyword in the search box and click **Search**. Alerts that meet the search conditions are displayed.



● All ○ By Device Name ○ By Device IP Address ○ By Alert Name

Alert Time	Alert Source	Alerting IP Address	Alerting Device	Alert Name	Alert Item	Details	Actions
Invalid Date	"Trap"	"[redacted]"	"ASW-A3-4-G11-1.AMTEST66"	"linkDown"	"AggregatePort 3"	Details	Ignore Delete
Invalid Date	"Trap"	"[redacted]"	"ASW-A3-4-G11-1.AMTEST66"	"linkDown"	"AggregatePort 3"	Details	Ignore Delete

6. (Optional)Filter the search results by the device name, device IP address, or alert name.
7. Find an alert and move the pointer over **Details** in the **Details** column to view the detailed alert information.
8. Find the reason why the alert is triggered and then process the alert.
   - If the alert does not affect the operation of the system, you can click **Ignore** in the **Actions** column corresponding to the alert. In the **Confirmation** message, click **OK** to ignore the alert.
   - If the alert is no longer significant, you can click **Delete** in the **Actions** column corresponding to the alert. In the **Confirm Operation** message, click **OK** to delete the alert.

     After the alert is deleted, you can query it on the **History Alerts** tab.
9. (Optional)Click **Export to SCV** to export the alert information to your computer.

6.2.9.2. View historical alerts

You can view historical alerts on the History Alerts tab.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Alert Dashboard**.
4. Click the **History Alerts** tab.
5. Select Alert Source, Alerting IP Address, Alerting Device, Alert Name, Alert Item, or Alerting Instance from the drop-down list, and then enter a keyword in the field. Select a time range and click **Search**. Alerts that meet the search conditions are displayed.
6. Click **Details** in the **Details** column corresponding to an alert to view detailed information about the alert.
7. (Optional)Click **Export to SCV** to export the alert information to your computer.

6.2.10. Alert settings

6.2.10.1. Add a trap

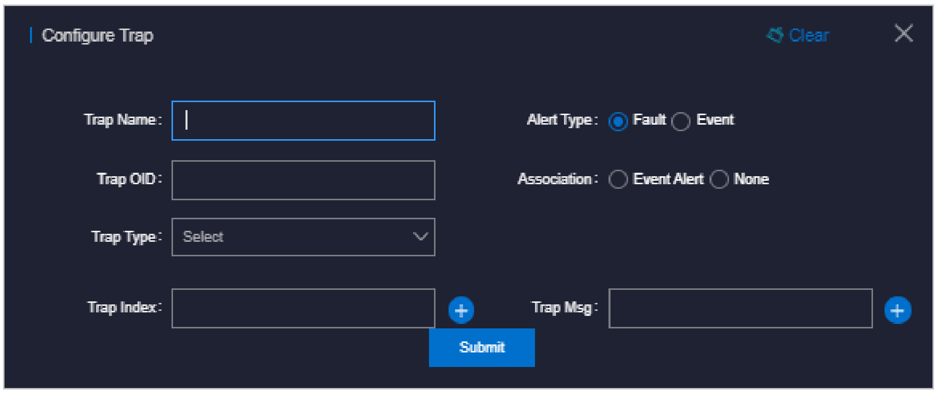
If the initially configured trap subscription does not meet the monitoring requirements, you can add a trap for monitoring match.

Context

Simple Network Management Protocol (SNMP) traps are used in this topic. SNMP trap is a part of SNMP and a mechanism that enables devices being managed (here refers to network devices such as switches and routers) to send SNMP messages to NOC monitoring servers. If an exception occurs on the device being monitored or the switch monitoring metrics have an exception, the SNMP agent running in the switch sends an alert event to the NOC monitoring server.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Alert Settings**.
4. On the **Alert Settings** page, click **Configure Trap**.
5. In the **Configure Trap** dialog box, configure the parameters.



Configure Trap

Trap Name:

Trap OID:

Trap Type: Select

Trap Index:

Alert Type: ● Fault ○ Event

Association: ○ Event Alert ○ None

Trap Msg:

The following table describes the parameters.

Parameter	Description	Example
Trap Name	The name of the alert event.	linkdown or BGPneighbor down. You can customize the value.
Trap OID	The OID of the alert event.	.1.3.6.1.4.1.25506.8.35.12.1.12 The value must be configured based on the device document and cannot be customized.
Trap Type	The type of the alert event.	N/A

Parameter	Description	Example
Trap Index	The index ID of the alert item. The KV information in trap messages, which is used to identify alert objects. Typically, the value of this parameter can be an API name, protocol ID, or index ID. You can configure multiple values for this parameter. The value must be configured based on the device document and cannot be customized.	N/A
Trap Msg	The message of the alert item. The KV information in trap messages, which is used to identify the alert data. Typically, the value of this parameter can be the additional information of the alert item, such as a system message or a message indicating the location of the state machine or the current status. You can configure multiple values for this parameter. The value must be configured based on the device document and cannot be customized.	N/A
Alert Type	Specifies whether the alert is of the fault type or the event type.	N/A
Association	Specifies whether the alert has an event alert. **Note** If **Event** is selected, you must enter the associated alert trap configurations.	N/A

6. Click **Submit**. After the configuration is submitted, the system checks whether the values of Trap OID and Trap Name are the same as the existing ones. If not, the trap is configured.

   After the trap is added, the alert events of the configured Trap OID are monitored and are displayed on the **Current Alerts** and **Alert History** tabs of the **Alert Management** module.

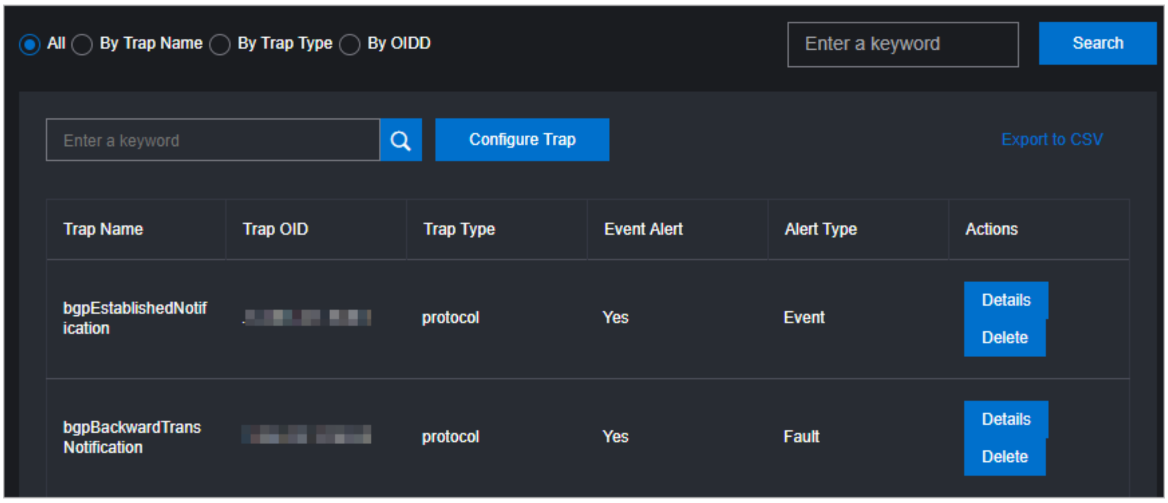
6.2.10.2. View traps

You can view traps configured in the current system.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Alert Settings**.
4. Enter a keyword in the search box in the upper-right corner and click **Search**.

   > Note You can click **Export to CSV** in the upper-right corner of the list to export the trap information to your computer.



Trap Name	Trap OID	Trap Type	Event Alert	Alert Type	Actions
bgpEstablishedNotification	[redacted]	protocol	Yes	Event	Details Delete
bgpBackwardTransNotification	[redacted]	protocol	Yes	Fault	Details Delete

5. (Optional)Filter the search results by trap name, trap type, or OID.
6. Move the pointer over **Details** in the **Actions** column corresponding to a trap to view detailed information about the trap.

   > Note If a trap is no longer needed, you can click **Delete** in the **Actions** column.

6.2.11. Physical network integration

The Physical Network Integration module allows network operations engineers to automate the integration of physical networks in the Apsara Uni-manager Operations Console by specifying the integration parameters. Network Operations Center (NOC) automatically generates and issues the configurations to specified devices and then performs the network integration test.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Physical Network Integration**.
4. Enter a project name and click **Create**. You must create a project file for this change to store the parameters related to the change. In the **History** section, you can choose **Manage > Import** in the Actions column.
5. In the upper-right corner, click **Save Project** to save the project details. Click **Next**.
6. Select a device.
   i. In the **Select Device** step, enter a device name in the search box of the **Devices on Live Network** section and click **Search**. After you add a device, you can click **Reset** to clear the search condition and then search for another device and add it.
   ii. Find a device and click **Add** in the Actions column to add it to the Target Device section on the right. To remove a device from the Target Device section, choose **Manage > Delete** in the Actions column corresponding to the device. You can also choose **Manage > Set the username and password** in the Actions column to modify the logon username and password of the device.
   iii. In the upper-right corner, click **Save Project** to save the information of devices added to the Target Device section.
   iv. Click **Next**.
7. Configure the interface parameters.
   i. In the **Configure Interfaces** step, click **Edit** in the Actions column. The **Configure Interfaces** section appears.
   ii. In the **Configure Interfaces** section, configure the parameters and click **Add**. You can choose **Manage > Edit** or **Manage > Delete** to modify or delete the added interface.
   iii. In the upper-right corner, click **Save Project** to save the configurations.
   iv. Click **Next**.
8. Configure the route parameters.
   i. In the **Configure Routes** step, click **Edit** in the Actions column. The **Configure Routes** section appears.
   ii. In the **Configure Routes** dialog box that appears, configure the parameters and click **Add**. You can choose **Manage > Edit** or **Manage > Delete** to modify or delete the added route.
   iii. In the upper-right corner, click **Save Project** to save the configurations.
   iv. Click **Next**.
9. Configure the route policies.
   i. In the **Configure Route Policies** step, click **Edit** in the Actions column. The **Configure Route Policies** section appears.
   ii. In the Configure Route Policies section, configure the parameters and click **Add**. You can choose **Manage > Delete** or **Manage > Delete** in the Actions column to modify or delete the added route policy.
   iii. In the upper-right corner, click **Save Project** to save the information.
   iv. Click **Next**.

10. In the **Generate Integration Configuration** step, click **Generate**.

    The system generates the integration configuration commands and rollback commands for all of the devices that have parameters configured.

    O&M engineers can generate configurations for each device based on the configured parameters. After the configurations are generated, click **View** in the **Actions** column. The corresponding commands are displayed on the left.

    You can also click **Export** to export the file that contains the configuration and rollback commands of detection devices to your computer.

6.2.12. ASW scale-up

This topic describes how to use NOC to automatically scale up ASW devices. After network operations engineers configure the scale-up parameters, NOC automatically generates the configuration and pushes the configuration to a specific device for automatic scale-up.

Prerequisites

Before you scale up ASW devices in the ASO console, you must plan the IP addresses and configure the ASW.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > ASW Scale-up**.
4. Select devices.
    i. In the **Select Device** step, enter a device name in the search box of the **Devices on Live Network** section and click **Search**. After you add a device, you can click **Reset** to clear the search condition and search for other devices to add to the list.
    ii. Find a device and click **Add** in the Actions column to add it to the Target Device section on the right. To remove a device from the Target Device section, choose **Manage > Delete** in the corresponding column. You can also modify the logon username and password of a device by choosing **Manage > Set the username and password** in the Actions column.
5. Click **Next**.
6. Disable the DSW port.
    i. In the **Disable DSW Port** step, find the device for which you want to disable the DSW port and click **Port Settings**.
    ii. Disable the port and click **Implement**.
    iii. In the message that appears, click **OK** to run the script.
7. Click **Next**.
8. Configure the DSW port.
    i. In the **Configure DSW Port** step, find the device for which you want to configure the DSW port and click **Edit** in the Actions column. The **Interface Parameter Configuration** section appears.

   ii. In the **Interface Parameter Configuration** section, set **Display Ports**, **Port Description**, **IP Address**, and **Subnet Mask**, and then click **Add**. You can choose **Manage > Edit** or **Manage > Delete** to modify or delete the added interface.

   iii. After you add the interface, click **Implement** in the Actions column corresponding to the device.

   iv. In the message that appears, click **OK** to run the script command. If an exception occurs after the implementation, you can click **Back** to roll back to the previous version.

9. Click **Next**.
10. Configure BGP.

    i. In the **Configure BGP** step, find the device for which you want to configure BGP and click **Edit** in the Actions column. The **Interface Parameter Configuration** section appears.

    ii. In the **Interface Parameter Configuration** section, set **Group Name**, **Peer ASN**, **Peer IP Address**, and **Local Port Name**, and then click **Add**. You can choose **Manage > Edit** or **Manage > Delete** in the Actions column to modify or delete the added interface.

    iii. After you add the interface, click **Implement** in the Actions column corresponding to the device.

    iv. In the message that appears, click **OK** to run the script. If an exception occurs after the implementation, you can click **Back** to roll back to the previous version.

11. Click **Next**.
12. In the **Upload ASW Configurations** step, upload the new ASW configurations.
13. Click **Next**.
14. Enable the DSW ports.

    i. In the **Enable DSW Port** step, find the device for which you want to enable the DSW port and click **Port Settings** in the Actions column.

    ii. Enable the port and click **Implement** in the Actions column.

    iii. In the message that appears, click **OK** to run the script command.

15. Click **Next**.
16. Perform the scale-up test.

    i. In the **Test Scale-up** step, find the device for which you want to perform the scale-up test and click **Select** in the Actions column. The route table is displayed on the right.

    ii. In the **ASW IP Address** search box, enter the IP address to be tested and then click **Add**.

    iii. Click **Test**. The system returns the test result.

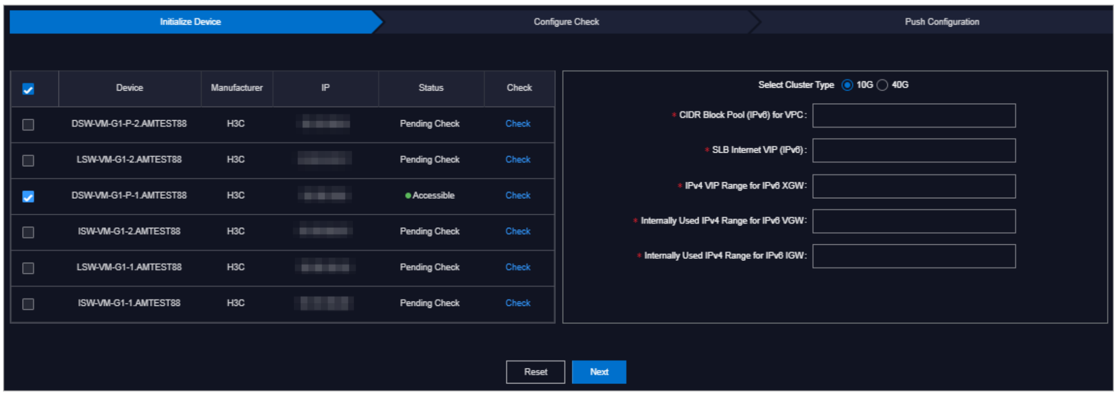
6.2.13. Push IPv6 configurations

The system can automatically push IPv6 configurations. After network operations engineers configure the IPv6 parameters in the IPV6 Configuration module, the system generates the IPv6 configurations and pushes the configurations to specified devices.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > IPV6 Configuration**.

4. In the **Initialize Device** step, select one or more devices and configure the parameters to complete the initialization.
   i. In the device list, find a device and click **Check** in the **Check** column to check whether the device is accessible. You can check multiple devices.
   ii. Select one or more devices whose **Status** is **Accessible**.
   iii. Configure the parameters on the right.



☑	Device	Manufacturer	IP	Status	Check
□	DSW-VM-G1-P-2.AMTEST88	H3C	[redacted]	Pending Check	Check
□	LSW-VM-G1-2.AMTEST88	H3C	[redacted]	Pending Check	Check
☑	DSW-VM-G1-P-1.AMTEST88	H3C	[redacted]	● Accessible	Check
□	ISW-VM-G1-2.AMTEST88	H3C	[redacted]	Pending Check	Check
□	LSW-VM-G1-1.AMTEST88	H3C	[redacted]	Pending Check	Check
□	ISW-VM-G1-1.AMTEST88	H3C	[redacted]	Pending Check	Check

Select Cluster Type ● 10G ○ 40G

* CIDR Block Pool (IPv6) for VPC :

* SLB Internet VIP (IPv6) :

* IPv4 VIP Range for IPv6 XGW :

* Internally Used IPv4 Range for IPv6 VGW :

* Internally Used IPv4 Range for IPv6 IGW :

Parameter	Description
Select Cluster Type	The type of the cluster. Valid values: **10G** and **40G**. Select a value based on the planned cluster type.
CIDR Block Pool (IPv6) for VPC	The VPC CIDR block pool in the IPv6 format.
SLB Internet VIP (IPv6)	The SLB public VIP address in the IPv6 format.
IPv4 VIP Range for IPv6 XGW	The XGW VIP CIDR block in the IPv4 format.
Internally Used IPv4 Range for IPv6 VGW	The internally used CIDR block for VGW in the IPv4 format.
Internally Used IPv4 Range for IPv6 IGW	The internally used CIDR block for IGW in the IPv4 format.

5. Click **Next**.
6. In the **Configure Check** step, check the configurations.

   During the configuration check, the system checks the current configurations of the selected devices and generates the IPv6 configuration script based on the check results. Click **View** on the right of the script file to view the generated configuration script, or click **Download** to download the configuration script to your computer.

   > Note If you select multiple devices in the **Initialize Device** step, you can click **Batch Download** to download multiple configuration scripts to your computer at a time.

   One of the following results may occur during the configuration check:

   - **The configuration is generated. Pending Pushing.**
   - **Failed to check the configuration. No BGP processes have been found.**

   - **Failed to check the configuration. Failed to generate the configuration.**
   - **Failed to check the configuration. The IPv6 configuration already exists.**

7. Click **Next**.

   The system checks whether the configuration pushing feature is enabled. If not, the `Contact the onsite manager to enable the feature before you continue` message appears. If yes, check whether the pushing condition is met based on the configuration check results and generation conditions of IPv6 configuration scripts.

   - If the configuration check is successful and the IPv6 configuration scripts are generated in the previous step, a dialog box appears. Click **Continue** to automatically push the configuration scripts to the selected devices.
   - If the configuration check result is **Failed to check the configuration. No BGP processes have been found.**, **Failed to check the configuration.**, or **Failed to check the configuration. The IPv6 configuration already exists.** in the previous step, a dialog box appears and the system does not push the configurations.

8. After the configurations are pushed, view the pushing results in the **Push Configuration** step.

   If the system indicates that it is pushing the configurations, click **Refresh** to refresh the pushing results.

   After the configurations are pushed, click **View** to view the current running configurations of the selected devices to check whether the IPv6 configurations are pushed.

6.2.14. Check IP address conflicts

The IP Address Conflicts module allows you to check whether the current Apsara Stack environment contains conflicting IP addresses.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > IP Address Conflicts**. After you enter the **IP Address Conflict Check** page, the system checks whether the current Apsara Stack environment contains conflicting IP addresses. If it does, the conflicting IP addresses are displayed in the list. You can also view the port information, device name, and corresponding logon IP address of each conflicting IP address.

6.2.15. Leased line discovery

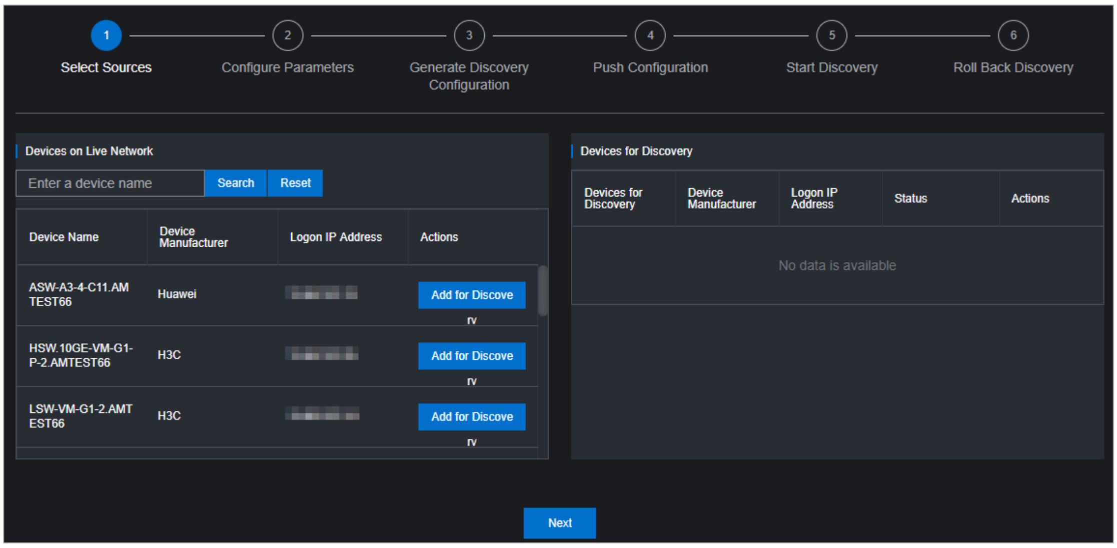
You can automate the leased line discovery for devices in the ASO console. After network operations engineers configure the discovery parameters, Network Operations Center (NOC) automatically generates the discovery configuration, pushes the configuration to a specific device, and then automatically performs the discovery test.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Leased Line Discovery**.

4. Select a discovery source.

   i. In the **Select Sources** step, enter a device name in the search box of the **Devices on Live Network** section and click **Search**. After you add a device, you can click **Reset** to clear the search condition, and then search for another device and add it to the Devices for Discovery list.



Devices on Live Network

Enter a device name | Search | Reset

Device Name	Device Manufacturer	Logon IP Address	Actions
ASW-A3-4-C11.AMTEST66	Huawei	[redacted]	Add for Discove ry
HSW.10GE-VM-G1-P-2.AMTEST66	H3C	[redacted]	Add for Discove ry
LSW-VM-G1-2.AMTEST66	H3C	[redacted]	Add for Discove ry

Devices for Discovery

Devices for Discovery	Device Manufacturer	Logon IP Address	Status	Actions

No data is available

Next

   ii. Click **Add for Discovery** in the Actions column corresponding to a device to add the device on the live network to the Devices for Discovery list on the right. To remove a device from the Devices for Discovery list, choose **Manage > Delete** in the Actions column corresponding to the device. You can also modify the logon username and password of the device by choosing **Manage > Set the username and password** in the Actions column.

   iii. Click **Next**.

5. Configure the discovery parameters.

   i. In the **Configure Parameters** step, click **Edit**. The **Configure Parameters** section is displayed.

   ii. Set **Link Name**, **Destination IP Address**, **Source IP**, **Discovery Interval**, **Discoveries**, and **Discovery Timeout**, and then click **Add** to add the information to the list. You can choose **Manage > Edit** or **Manage > Delete** in the Actions column to modify or delete the discovery parameters.

   iii. Click **Next**.

6. In the **Generate Discovery Configuration** step, click **Generate** to generate the discovery configuration and roll back commands of all devices that have discovery parameters configured.

   i. Click **View** in the **Actions** column. The corresponding commands are displayed on the left.

   ii. You can also select one or more devices and click **Export** to export the files that contain configuration and rollback commands of discovery devices to your computer.

   iii. Click **Next**.

7. In the **Push Configuration** step, click **Push Configurations**.

   i. In the message that appears, click **Continue** to push the discovery configuration commands to the corresponding device.

   ii. After the configuration is pushed, you can click **View Logs** to view detailed push logs.

   iii. Click **Next**.

8. In the **Start Discovery** step, click **Started** in the Actions column corresponding to a device to perform the leased line discovery test.

   After the test is complete, click **Next**.

9. In the **Roll Back Discovery** step, click **Roll Back** in the Actions column corresponding to the device on which you have performed the leased line test to roll back the corresponding NQA configurations in the device.

   i. After the rollback is complete, you can click **View Logs** to view detailed rollback logs.

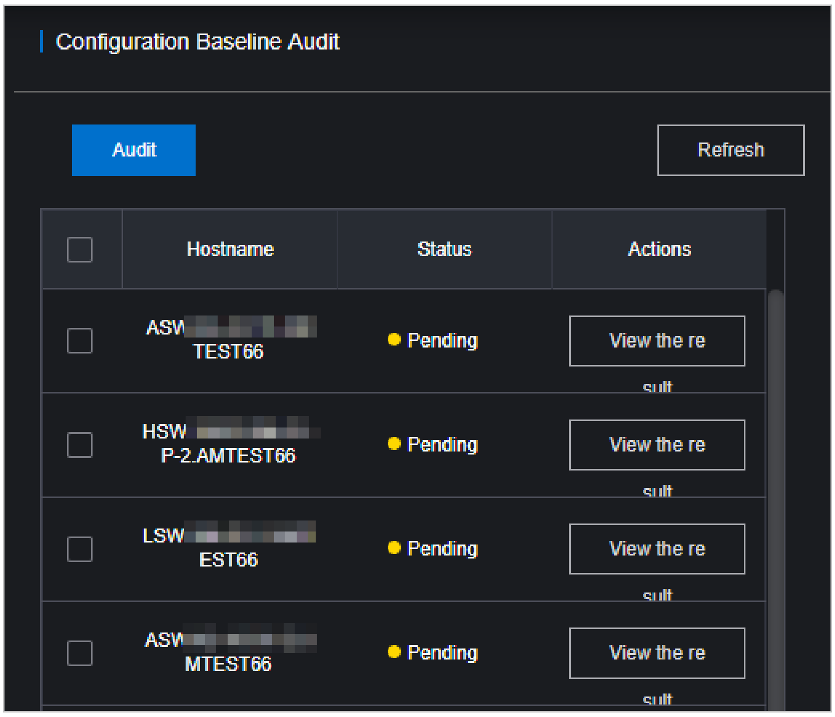
   ii. Click **Completed**.

6.2.16. Baseline configuration audit

The Baseline Configuration Audit module allows you to compare the baseline and the current running configurations of devices.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Baseline Configuration Audit**.
4. Select one or more devices in the device list and click **Audit**. The system begins to audit the baseline configurations of the selected devices.



Configuration Baseline Audit

Audit   Refresh

□	Hostname	Status	Actions
□	ASW[redacted] TEST66	● Pending	View the re sult
□	HSW[redacted] P-2.AMTEST66	● Pending	View the re sult
□	LSW[redacted] EST66	● Pending	View the re sult
□	ASW[redacted] MTEST66	● Pending	View the re sult

The following table describes the audit status.

Status	Description
Pending	The initial status.

Status	Description
Auditing	The baseline configurations of the device are being audited in the background.
Pass	The current configuration is consistent with the baseline configuration.
Fail	The current configuration is not consistent with the baseline configuration.
Disconnected	The system cannot connect to the device.
No Data	The system cannot obtain the baseline configurations of the device.

5. After the audit is complete, click **Refresh** to update the audit results.
6. Click **View the result** in the **Actions** column of the device. The audit result is displayed on the right.

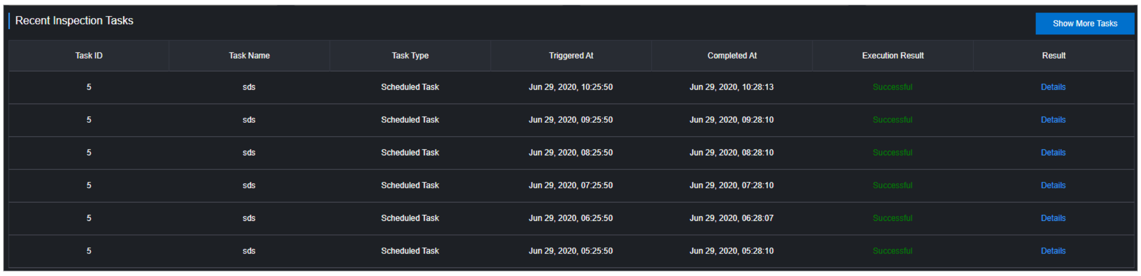
6.2.17. Inspection dashboard

The Inspection Dashboard module allows you to view the inspection data and the last 10 inspection records.

Procedure

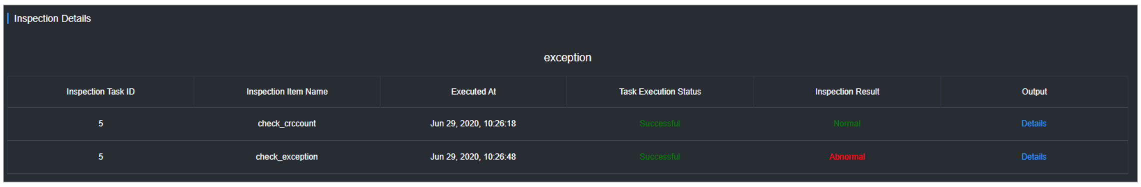
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Inspection Dashboard**.
4. Perform the following operations:
    - View the inspection statistics of the current day and the last 10 inspection records. The inspection statistics include the number of successful tasks, failed tasks, and scheduled tasks for the current day, as well as the progress.
    - View inspection records

      In the **Recent Inspection Tasks** section, click **Details** in the **Result** column corresponding to a task. The following information about the task is displayed: inspection time, inspection template, execution progress, inspection health status, task type, task status, task name, and inspection details of each subtask.

Task ID	Task Name	Task Type	Triggered At	Completed At	Execution Result	Result
5	sds	Scheduled Task	Jun 29, 2020, 10:25:50	Jun 29, 2020, 10:28:13	Successful	Details
5	sds	Scheduled Task	Jun 29, 2020, 09:25:50	Jun 29, 2020, 09:28:10	Successful	Details
5	sds	Scheduled Task	Jun 29, 2020, 08:25:50	Jun 29, 2020, 08:28:10	Successful	Details
5	sds	Scheduled Task	Jun 29, 2020, 07:25:50	Jun 29, 2020, 07:28:10	Successful	Details
5	sds	Scheduled Task	Jun 29, 2020, 06:25:50	Jun 29, 2020, 06:28:07	Successful	Details
5	sds	Scheduled Task	Jun 29, 2020, 05:25:50	Jun 29, 2020, 05:28:10	Successful	Details

      In the **Inspection Details** section, move the pointer over **Details** in the **Rollback** column corresponding to a subtask. The inspection result of the inspection subtask is displayed.



Inspection Details

exception

Inspection Task ID	Inspection Item Name	Executed At	Task Execution Status	Inspection Result	Output
5	check_crccount	Jun 29, 2020, 10:26:18	Successful	Normal	Details
5	check_exception	Jun 29, 2020, 10:26:48	Successful	Abnormal	Details

- Click **Show More Tasks** to go to the **Inspection History** page to view the inspection history.

6.2.18. Inspection history

You can query the inspection history and view detailed inspection records by task type and time range.

Context

Inspection tasks can be divided into one-time tasks and scheduled tasks. A one-time task can be executed only once. You can set an execution interval for a scheduled task.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Inspection History**. By default, all inspection records in the last 24 hours are displayed.
4. Select the inspection type (**All**, **One-time Task**, or **Scheduled Task**), specify the time range, and then click **Search**.
5. View inspection records that meet the query conditions.
6. Click **Details** in the **Result** column corresponding to an inspection record. The following information is displayed: inspection time, inspection template, execution progress, inspection health status, task type, task status, task name, and inspection details of each subtask.
7. In the **Inspection Details** section, move the pointer over **Details** in the **Rollback** column corresponding to a subtask. The inspection result of the inspection subtask is displayed.

6.2.19. Inspection management

The Inspection Management module allows you to create, view, modify, start, suspend, and delete inspection tasks.

6.2.19.1. Create a one-time task

This topic describes how to create a one-time task.

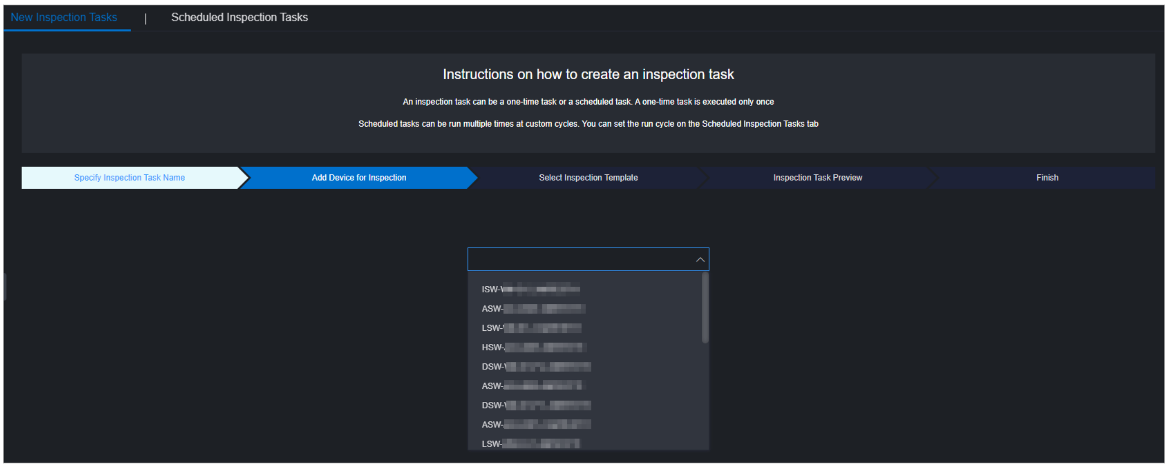
Context

By default, a one-time task can be executed only once after it is created. After a one-time task is executed once, the task automatically enters the **Suspended** state. The task can be manually started and then executed again.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.

3. In the left-side navigation pane, choose **Network Operations Center** > **Inspection Management**.
4. Click the **One-time Task** icon. The configuration wizard for the inspection task appears.
5. In the Specify Inspection Task Name step, enter the inspection task name and click **Next**.
6. In the **Add Device for Inspection** step, select one or more devices from the drop-down list and click **Next**.


New Inspection Tasks
Scheduled Inspection Tasks
Specify Inspection Task Name
Add Device for Inspection
Select Inspection Template
Inspection Task Preview
Finish

Instructions on how to create an inspection task

An inspection task can be a one-time task or a scheduled task. A one-time task is executed only once

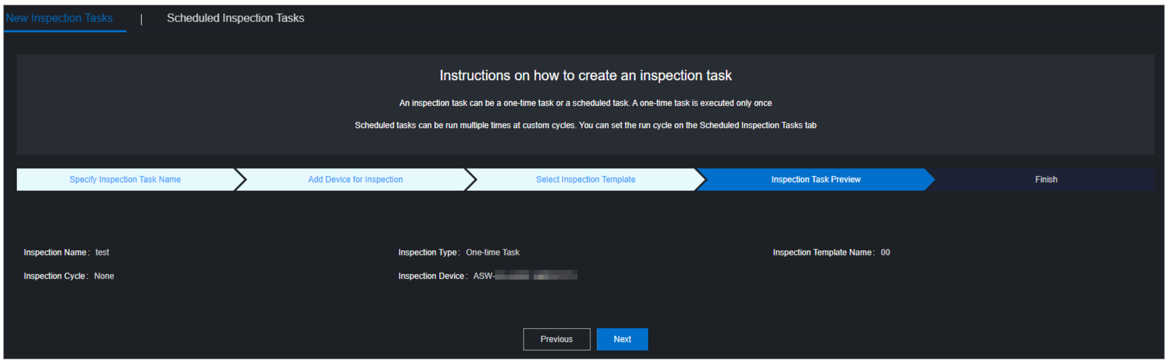
Scheduled tasks can be run multiple times at custom cycles. You can set the run cycle on the Scheduled Inspection Tasks tab

ISW-[redacted]
ASW-[redacted]
LSW-[redacted]
HSW-[redacted]
DSW-[redacted]
ASW-[redacted]
DSW-[redacted]
ASW-[redacted]
LSW-[redacted]

7. In the **Select Inspection Template** step, select an existing template from the drop-down list or click **Create Temporary Inspection Template**. To create a temporary inspection template, click **Create Temporary Inspection Template**. In the dialog box that appears, select the inspection items that you want to associate with the temporary inspection template and click **OK**.

> **Note** Some inspection items are provisioned by manufacturers. You must select proper inspection templates or inspection items based on devices. For more information about inspection templates and items in the system, see View template details and View inspection items.

8. Click **Next**.
9. In the **Inspection Task Preview** step, confirm the inspection task information and click **Next**.


New Inspection Tasks
Scheduled Inspection Tasks
Specify Inspection Task Name
Add Device for Inspection
Select Inspection Template
Inspection Task Preview
Finish
Previous
Next

Instructions on how to create an inspection task

An inspection task can be a one-time task or a scheduled task. A one-time task is executed only once

Scheduled tasks can be run multiple times at custom cycles. You can set the run cycle on the Scheduled Inspection Tasks tab

Inspection Name : test
Inspection Type : One-time Task
Inspection Template Name : 00
Inspection Cycle : None
Inspection Device : ASW-[redacted]

10. Click **Finish**.

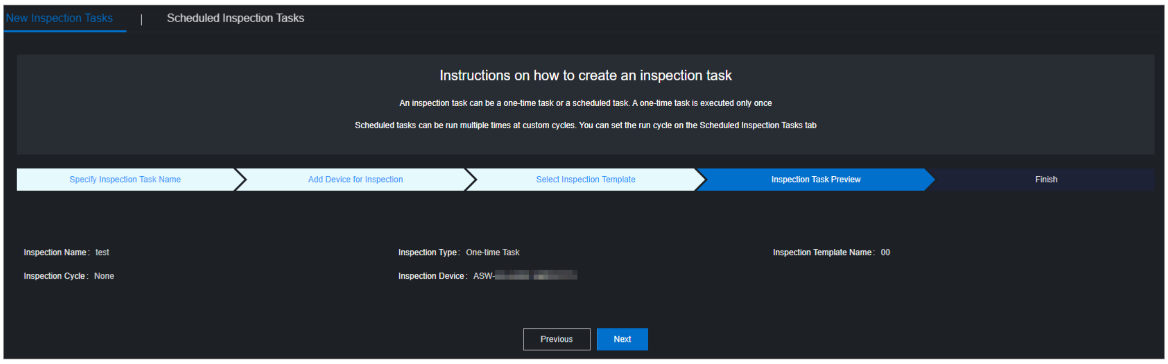
    The message **Created** is displayed. You can choose **Network Operations Center** > **Inspection Management** to view the created one-time inspection task on the **Scheduled Inspection Tasks** tab.

6.2.19.2. Create a scheduled task

This topic describes how to create a scheduled task based on routine inspection requirements. You can set an execution interval for the scheduled task.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Inspection Management**.
4. Click the **Scheduled Task** icon. The configuration wizard for the inspection task appears.
5. In the Specify Inspection Task Name step, enter the inspection task name and click **Next**.
6. In the **Add Device for Inspection** step, select one or more devices from the drop-down list and click **Next**.
7. In the **Select Inspection Template** step, select an existing template from the drop-down list or click **Create Temporary Inspection Template**. To create a temporary inspection template, click **Create Temporary Inspection Template**. In the dialog box that appears, select the inspection items that you want to associate with the temporary inspection template and click **OK**.
8. Click **Next**.
9. Specify the inspection cycle and the time point when the task is triggered and click **Next**.


New Inspection Tasks
Scheduled Inspection Tasks

Instructions on how to create an inspection task

An inspection task can be a one-time task or a scheduled task. A one-time task is executed only once

Scheduled tasks can be run multiple times at custom cycles. You can set the run cycle on the Scheduled Inspection Tasks tab

Specify Inspection Task Name
Add Device for Inspection
Select Inspection Template
Inspection Task Preview
Finish

Inspection Name : test

Inspection Type : One-time Task

Inspection Template Name : 00

Inspection Cycle : None

Inspection Device : ASW-[redacted]

10. In the **Inspection Task Preview** step, confirm the inspection task information and click **Next**.
11. Click **Finish**.

    The message **Created** is displayed. You can choose **Network Operations Center > Inspection Tasks** to view the newly created scheduled task on the **Scheduled Inspection Tasks** tab.

6.2.19.3. Manage scheduled inspection tasks

After an inspection task is created, you can view, modify, start, suspend, or delete the task.

Go to the scheduled inspection task management page

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Inspection Management**.

4. Click the **Scheduled Inspection Tasks** tab.

View tasks

1. View the information of all the created inspection tasks in the system, including the task ID, task name, task type, associated template, creation time, and running status.

Modify task parameters

1. In the task list, find the task that you want to modify and click **Modify** in the **Actions** column.
2. In the dialog box that appears, modify the task parameters.
    - For a one-time task, you can modify the inspection name, inspection type, inspection template, and inspection device.
    - For a scheduled task, you can modify the inspection name, inspection type, inspection template, inspection device, and inspection cycle.
3. Click **OK**.

Start or suspend a task

You can start a suspended task or suspend a running task based on O&M requirements.

1. In the task list, find a task and click **Start** or **Suspend** in the **Actions** column.

    > **Note** After a one-time task is executed, it automatically enters the **Suspended** state. You can click **Start** to execute it again.

2. In the message that appears, click **OK**.

Delete a task

1. In the task list, find the task that you want to delete and click **Delete** in the **Actions** column.
2. In the message that appears, click **OK**.

6.2.20. Inspection templates

The Inspection Templates module allows you to manage, create, view, modify, and delete inspection templates.

6.2.20.1. Create a template

You can create a common inspection template to facilitate routine inspection task creation.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Inspection Templates**.
4. Click **Create Template**.
5. In the dialog box that appears, enter the template name and template tag, and select a manufacturer and a template inspection item collection for the device.

Parameter	Description
Template Name	The name of the inspection template. The name must be unique.
Associated Manufacturer	The manufacturer of the device.
Template Tag	The tag added to the template to make it easier to differentiate.
Template Inspection Item Collection	The collection of inspection items associated with the template.

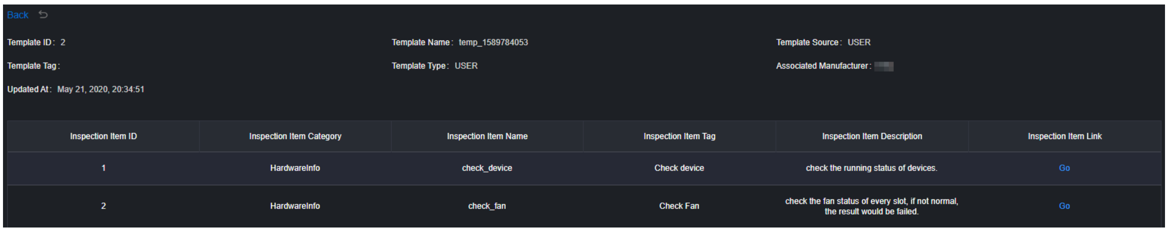
6. Click **OK**. After the template is created, you can view the new template in the template list.

6.2.20.2. View template details

Before you use an inspection template, you can view its details to determine whether it meets your requirements.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Inspection Templates**.
4. In the template list, find the template that you want to view and click **Details** in the **Details** column.



Template ID: 2
Template Name: temp_1589784053
Template Source: USER
Template Tag:
Template Type: USER
Associated Manufacturer: [redacted]
Updated At: May 21, 2020, 20:34:51

Inspection Item ID	Inspection Item Category	Inspection Item Name	Inspection Item Tag	Inspection Item Description	Inspection Item Link
1	HardwareInfo	check_device	Check device	check the running status of devices.	Go
2	HardwareInfo	check_fan	Check Fan	check the fan status of every slot, if not normal, the result would be failed.	Go

5. View the basic information about the template and the inspection items related to the template.
6. (Optional)To manage an inspection item in the template, click **Go** in the **Inspection Item Link** column to go to the inspection item management page. For other management operations that can be performed on inspection items, see **Network operations > Network management and operations > Network automation > Configure templates** in *Apsara Stack Enterprise Operations and Maintenance Guide*.

> **Note** Typically, no other management operations are required for inspection items.

6.2.20.3. Modify a template

After you create a template, you can modify its information based on your needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.

2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Inspection Templates**.
4. In the template list, find the template that you want to modify and click **Modify** in the **Actions** column.
5. In the dialog box that appears, modify the template name, associated manufacturer, template tag, and template inspection item collection.
6. Click **OK**.

6.2.20.4. Delete a template

You can delete inspection templates that are no longer needed for routine O&M.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Inspection Templates**.
4. In the template list, find the template that you want to delete and click **Delete** in the **Actions** column.

   > **Notice** When you delete a template, its associated inspection tasks and records are also deleted. Exercise caution when you delete templates.

5. In the message that appears, click **OK**.

6.2.20.5. View inspection items

You can view the details of all inspection items in the system, including the item ID, category, name, tag, and description.

Procedure

1. Log on to the Apsara Uni-manager Operations Console. For more information, see Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, click **Network Operations Center > Inspection Templates**.
4. Click the **Inspection Items** tab.
5. View the information of all inspection items in the system.
6. To perform other management operations on an inspection item, click **Go** in the **Inspection Item Link** column to go to the inspection item management page. For other management operations that can be performed on inspection items, see **Network operations > Network management and operations > Network automation > Configure templates** in *Apsara Stack Enterprise Operations and Maintenance Guide*.

   > **Note** Typically, no other management operations are required for inspection items.

6.2.21. Use cases

6.2.21.1. Troubleshoot network failures

This topic uses a typical case to describe how to use the Network Operations Network module to troubleshoot network failures.

Scenario

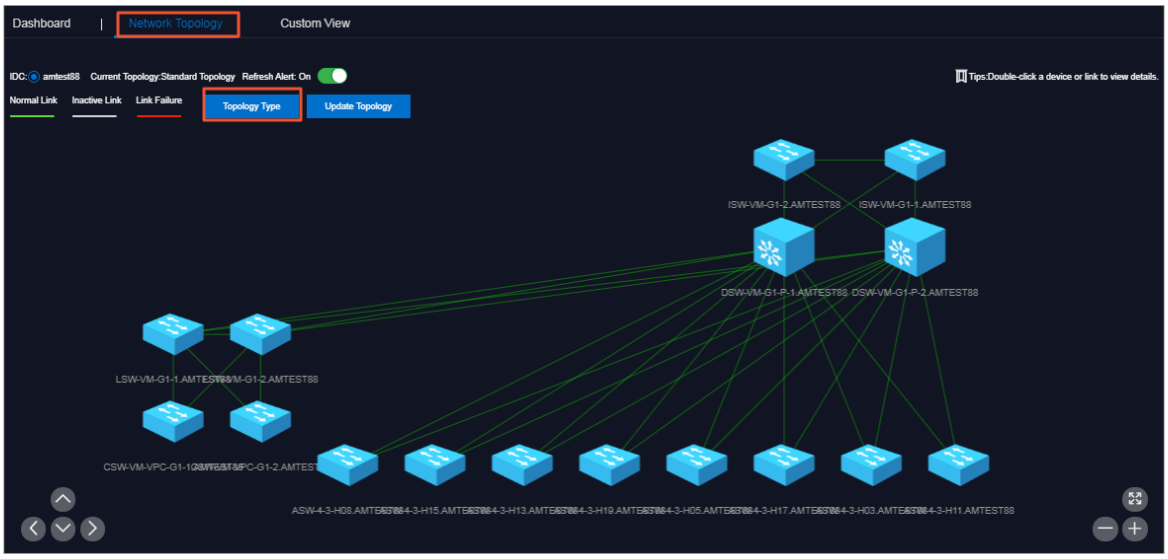
If the visit latency and retransmission time of a cloud service increase, you must determine whether this is caused by network failures.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Dashboard**.
4. Click the **Network Topology** tab.
5. On the tab that appears, click **Topology Type** and select **Standard Topology**.

   Wait five seconds. After the page loads, the system shows the network-wide topology and device connections of the AZ in the current environment.

   If device alerts are not triggered in the network, device icons are blue, links between devices are green, and device names are white in the topology. If device alerts are triggered in the network, the topology updates the alert information in the current network every five seconds and shows the updated alert information.

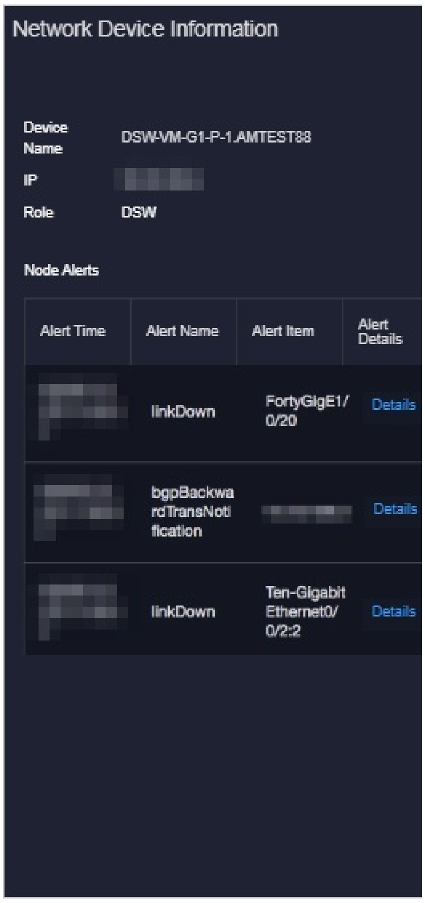


Dashboard | Network Topology Custom View

IDC: ● amtest88 Current Topology:Standard Topology Refresh Alert: On

Tips:Double-click a device or link to view details.

6. If a device name or link in the topology becomes red, alerts are detected in the network device or link port. Double-click the icon of a red device name. In the panel that appears, you can view the basic information of the device and the network alert information related to the device.



Network Device Information

Device Name DSW-VM-G1-P-1.AMTEST88

IP [redacted]

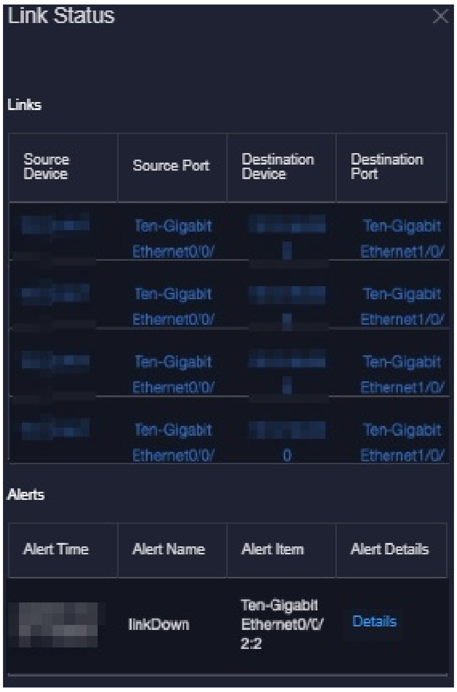
Role DSW

Node Alerts

Alert Time	Alert Name	Alert Item	Alert Details
[redacted]	linkDown	FortyGigE1/0/20	Details
[redacted]	bgpBackwardTransNotification	[redacted]	Details
[redacted]	linkDown	Ten-GigabitEthernet0/0/2:2	Details

In the preceding figure, the port that is connected to the DSW has a **linkDown** alert and a bgp peer alert. An ASW is identified based on the IP address of the BGP peer. This allows you to determine that a problem in a link between DSW and ASW exists, which caused the port to go down and triggered the alerts.

7. Click the red link in the topology. In the panel that appears, you can view one or more physical links contained in the logical link and the alert information of the link between devices.



Link Status

Links

Source Device	Source Port	Destination Device	Destination Port
[redacted]	Ten-Gigabit Ethernet0/0/	[redacted]	Ten-Gigabit Ethernet1/0/
[redacted]	Ten-Gigabit Ethernet0/0/	[redacted]	Ten-Gigabit Ethernet1/0/
[redacted]	Ten-Gigabit Ethernet0/0/	[redacted]	Ten-Gigabit Ethernet1/0/
[redacted]	Ten-Gigabit Ethernet0/0/	[redacted] 0	Ten-Gigabit Ethernet1/0/

Alerts

Alert Time	Alert Name	Alert Item	Alert Details
[redacted]	linkDown	Ten-Gigabit Ethernet0/0/ 2:2	Details

In the preceding figure, the logical link that connects the two devices contains four physical end-to-end links. The port 0/0/2:2 has a port **linkDown** alert. Then, you can proceed to log on to the device and check whether this is caused by the low optical power or damaged modules.

8. When the problem corresponding to the previous alerts is solved, the system updates the alert information. When the fault is repaired, the alerts automatically disappear, the topology is restored to the normal state, and no device names or links remain red.

Use the Alert Management module as a supplement to troubleshoot problems

If a device name or link in the topology becomes red, alerts are detected in the network device or link. You can choose **Network Operations Center > Alerts** and view the current alerts that are not recovered in the network on the **Current Alerts** tab.

The Current Alerts tab shows more detailed alert information.

If an alert is for test or generated because of a cutover, you can click **Ignore** or **Delete** in the **Actions** column corresponding to the alert to ignore or delete the alert.

Use the syslog log query tool as a supplement to troubleshoot problems

If a device name or link in the topology becomes red and you have confirmed that the device alert is not caused by expected changes or because of a cutover by using the alert management feature, you must view the detailed exception logs. You can use the syslog log query tool of vSwitches to search for logs.

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Network Operations Center > Network Element Management**.
4. Click the **Syslogs** tab.

5. In the upper-right corner, select the device that you want to query, specify the time range, and then click **Search**. Logs generated within the specified time range are displayed. By default, you can query a maximum of 1,000 logs.
6. In the upper-left corner, enter a keyword in the search box and click **Search**.
7. After the query is complete, if you want to export logs to submit a ticket or submit logs to device vendors for troubleshooting, click **Export to CSV** in the upper-right corner. Logs are stored in your computer as a .csv file.

6.3. Products

The Products module allows you to click operations and maintenance services of other products on the cloud platform and ISV access configurations to go to the corresponding page.

6.3.1. Product list

On the Product List page, you can go to the O&M page or ISV page corresponding to a product by using Single Sign-On (SSO) and redirection.

Prerequisites

To access the ISV page, make sure that the ISV access information is configured on the **ISV Access Configurations** page. For more information about how to configure the ISV access information, see Configure the ISV access information.

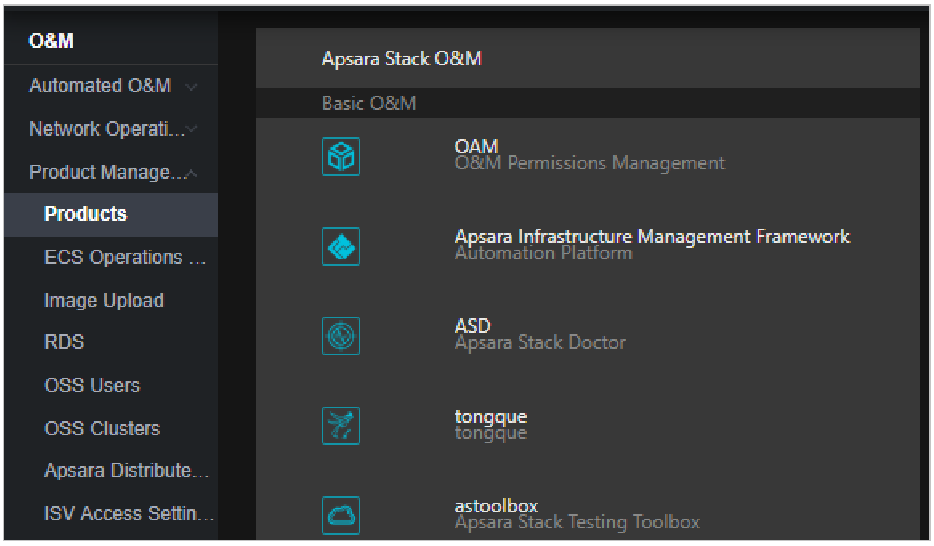
Context

When you use accounts that have different permissions to log on to the ASO console, the product O&M icons and ISV icons on the **Product List** page are displayed in different ways. An operations system administrator can view all the O&M components of the cloud platform.

The read and write permissions for product O&M are separated to allow the system to dynamically assign different permissions based on different roles.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > Products**.



4. On the **Product List** page, you can view the O&M icons of different products and ISV icons based on your permissions.

6.3.2. ISV access settings

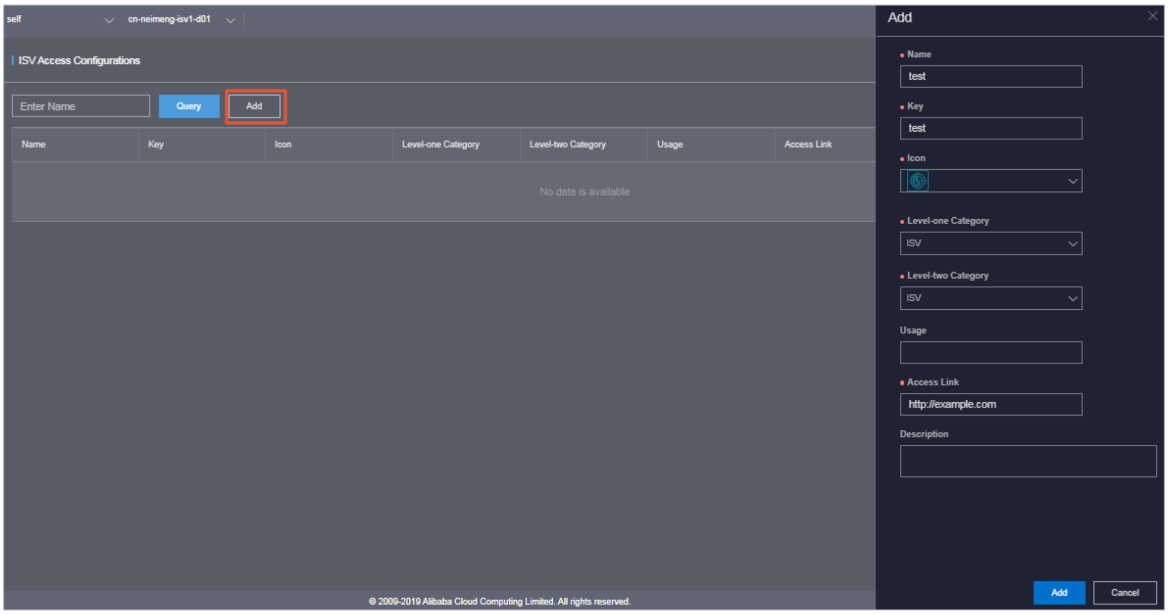
The ISV Access Settings module allows you to configure, modify, and delete the ISV access information.

6.3.2.1. Configure the ISV access information

You can configure the ISV access information in the system to suit your business needs. Then, you can click an icon on the **Product List** page to access the corresponding ISV page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > ISV Access Settings**.
4. On the page that appears, click **Add**.
5. In the **Add** panel, configure the ISV access information.



self | cn-neimeng-isv1-d01

ISV Access Configurations

Enter Name | Query | Add

Name	Key	Icon	Level-one Category	Level-two Category	Usage	Access Link

No data is available

© 2009-2019 Alibaba Cloud Computing Limited. All rights reserved.

Add

- Name: test
- Key: test
- Icon
- Level-one Category: ISV
- Level-two Category: ISV
- Usage
- Access Link: http://example.com
- Description

Add | Cancel

The following table describes the parameters.

Parameter	Description
Name	The name of the ISV to access.
Key	Set the value to an identifier related to the ISV business.
Icon	The icon displayed on the **Product List** page for the ISV to access.
Level-one Category and **Level-two Category**	The category to which the ISV to be accessed belongs on the **Product List** page.
Usage	The feature of the ISV to access.
Access Link	The address of the ISV to access.
Description	The description related to the ISV to access.

6. Click **Add**.

Result

You can view the added ISV icon on the Product List page by choosing **Product Management > Products**. Click the icon and then you can go to the corresponding page.

6.3.2.2. Modify the ISV access information

If the ISV information is changed, you can modify the ISV access information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > ISV Access Settings**.

4. (Optional)Enter the ISV name in the search box and click **Query**. Fuzzy search is supported.
5. Find the ISV for which you want to modify the access information and click **Modify** in the **Actions** column.
6. In the **Modify** panel, modify the name, key, icon, level-one category, level-two category, usage, access link, or description of the ISV.
7. Click **Edit**.

6.3.2.3. Delete the ISV access information

You can delete the ISV access information added to the system based on your business needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > ISV Access Settings**.
4. (Optional)On the page that appears, enter the ISV name in the search box and click **Query**. Fuzzy search is supported.
5. Find the ISV for which you want to delete access information and click **Delete** in the **Actions** column.
6. In the message that appears, click **OK**.

Result

Choose **Product Management > Products**, the deleted ISV is no longer displayed on the Product List page.

6.4. Apsara Distributed File System Management

6.4.1. View ECS disk size rankings

The ECS Disk Size Ranking module allows you to view the amount of space occupied by all disks within the elastic block storage attached to an ECS cluster in Apsara Distributed File System.

Context

When an ECS cluster occupies a large amount of space in Apsara Distributed File System, the on-site O&M personnel must check the space occupied by each disk in the elastic block storage attached to the ECS clusters. Then, they must contact the business side to migrate data and release disks. The ECS disk size ranking feature helps O&M personnel easily identify which disks occupy a large space in Apsara Distributed File System so that they can perform targeted cleaning and quickly lower the space usage.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > ECS**

Disk Size Ranking.

4. Select the ECS cluster that you want to query from the **Cluster** drop-down list and click **Search**. All disks attached to the elastic block storage of the selected ECS cluster are listed from large to small based on the actual size of the space they occupy in Apsara Distributed File System. You can view the cluster name, cluster ID, and zone of the selected cluster, as well as the storage type, size, and identifier of each disk.
5. (Optional) you can click **Reset** to clear the preceding search conditions.

6.4.2. Dashboard

The Dashboard module allows you to view the overview information, health heatmap, and data of the top five clusters.

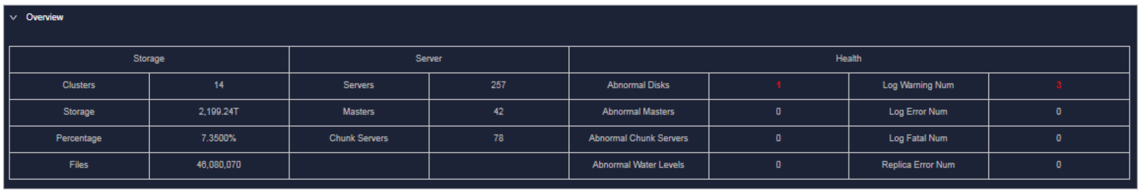
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Dashboard**.
4. Select the service that you want to view from the **Service** drop-down list.

   The Dashboard module shows the overview information, health heatmap, and data of top five clusters of services as of the current date.

   - **Overview**

     The Overview section shows the storage space, server information, and health information of the specified service. In the **Health** column, values that are greater than 0 are displayed in red.

     Overview

Storage		Server		Health			
Clusters	14	Servers	257	Abnormal Disks	1	Log Warning Num	3
Storage	2,199.24T	Masters	42	Abnormal Masters	0	Log Error Num	0
Percentage	7.3500%	Chunk Servers	78	Abnormal Chunk Servers	0	Log Fatal Num	0
Files	46,080,070			Abnormal Water Levels	0	Replica Error Num	0

   - **Heatmap of Health**

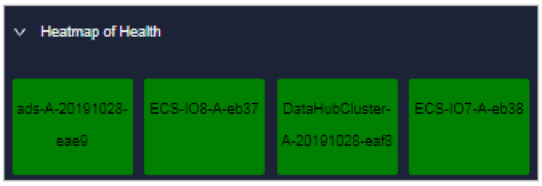
     The Heatmap of Health section shows the health information of all clusters within the specified service. Clusters in different health states are displayed in different colors:

     Notes:

     - Green indicates that the cluster works properly.
     - Yellow indicates that the cluster has a warning.
     - Red indicates that the cluster has an exception.
     - Dark red indicates that the cluster has a fatal error.
     - Grey indicates that the cluster is disabled.

     Click the name of an enabled cluster to go to the corresponding cluster information page.

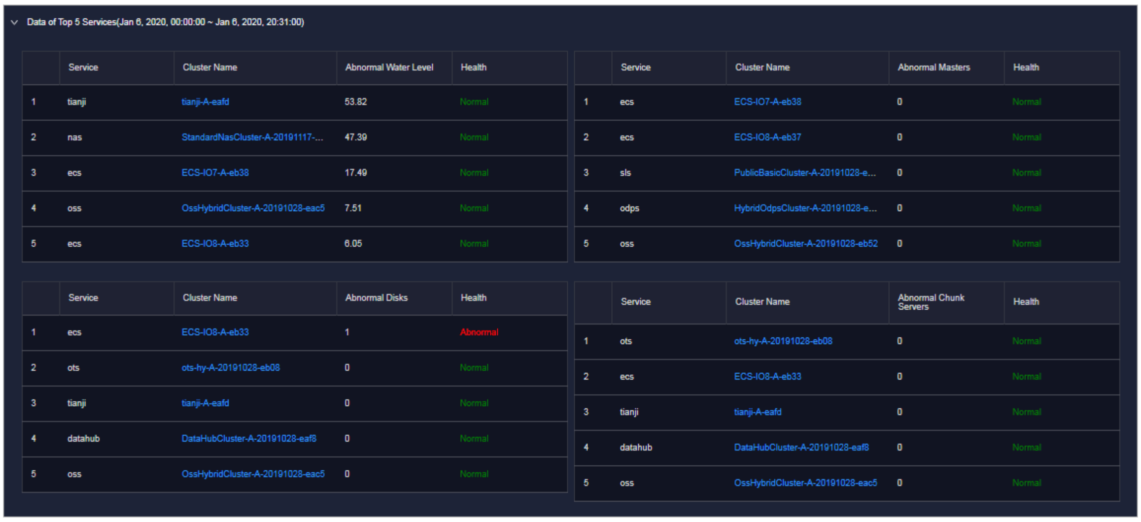
     Move the pointer over the color block of each cluster to view the corresponding service name, server name, and IP address.



- **Data of Top 5 Services**

  The Data of Top 5 Services section shows the data of the top five healthiest clusters of the specified service for the current date over the time range from 00:00 to the current time.

  This section shows the top five clusters in terms of abnormal disk usage, masters, disks, and chunk servers. Click the cluster name to go to the corresponding cluster information page.



Data of Top 5 Services(Jan 6, 2020, 00:00:00 ~ Jan 6, 2020, 20:31:00)

	Service	Cluster Name	Abnormal Water Level	Health
1	tianji	tianji-A-eafd	53.82	Normal
2	nas	StandardNasCluster-A-20191117-...	47.39	Normal
3	ecs	ECS-IO7-A-eb38	17.49	Normal
4	oss	OssHybridCluster-A-20191028-eac5	7.51	Normal
5	ecs	ECS-IO8-A-eb33	6.05	Normal

	Service	Cluster Name	Abnormal Masters	Health
1	ecs	ECS-IO7-A-eb38	0	Normal
2	ecs	ECS-IO8-A-eb37	0	Normal
3	sls	PublicBasicCluster-A-20191028-e...	0	Normal
4	odps	HybridOdpsCluster-A-20191028-e...	0	Normal
5	oss	OssHybridCluster-A-20191028-eb52	0	Normal

	Service	Cluster Name	Abnormal Disks	Health
1	ecs	ECS-IO8-A-eb33	1	Abnormal
2	ots	ots-hy-A-20191028-eb08	0	Normal
3	tianji	tianji-A-eafd	0	Normal
4	datahub	DataHubCluster-A-20191028-eaf8	0	Normal
5	oss	OssHybridCluster-A-20191028-eac5	0	Normal

	Service	Cluster Name	Abnormal Chunk Servers	Health
1	ots	ots-hy-A-20191028-eb08	0	Normal
2	ecs	ECS-IO8-A-eb33	0	Normal
3	tianji	tianji-A-eafd	0	Normal
4	datahub	DataHubCluster-A-20191028-eaf8	0	Normal
5	oss	OssHybridCluster-A-20191028-eac5	0	Normal

6.4.3. Clusters

The Clusters module allows you to view the overview information, alert monitoring information, replica information, and trend charts, and rack information of a cluster.

Procedure

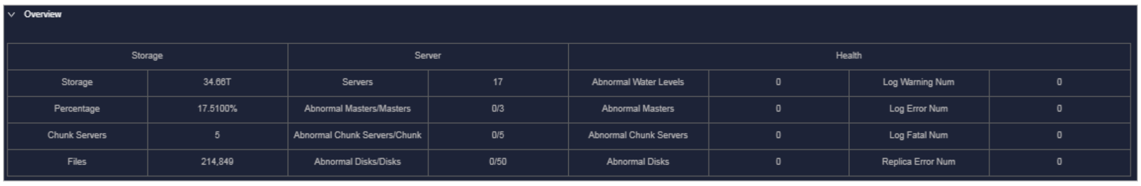
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Clusters**.

   On the page that appears, the data of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select the cluster that you want to view from the **Cluster Name** drop-down list. The following information is displayed:

   > **Note** All the enabled clusters in the current environment are displayed in the **Cluster Name** drop-down list.

   - **Overview**

     This section shows the storage space, device information, and health information of the cluster. In the **Health** column, values that are greater than 0 are displayed in red.

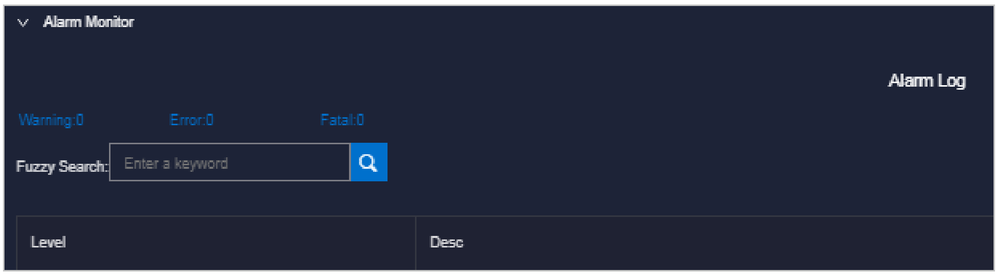


Overview

Storage		Server		Health			
Storage	34.66T	Servers	17	Abnormal Water Levels	0	Log Warning Num	0
Percentage	17.5100%	Abnormal Masters/Masters	0/3	Abnormal Masters	0	Log Error Num	0
Chunk Servers	5	Abnormal Chunk Servers/Chunk	0/5	Abnormal Chunk Servers	0	Log Fatal Num	0
Files	214,849	Abnormal Disks/Disks	0/50	Abnormal Disks	0	Replica Error Num	0

- ### Alert Monitoring

  This section shows the alert information of the specified cluster. You can query data by keywords.



Alarm Monitor

Alarm Log

Warning:0 Error:0 Fatal:0

Fuzzy Search: Enter a keyword

Level	Desc

- ### Replica

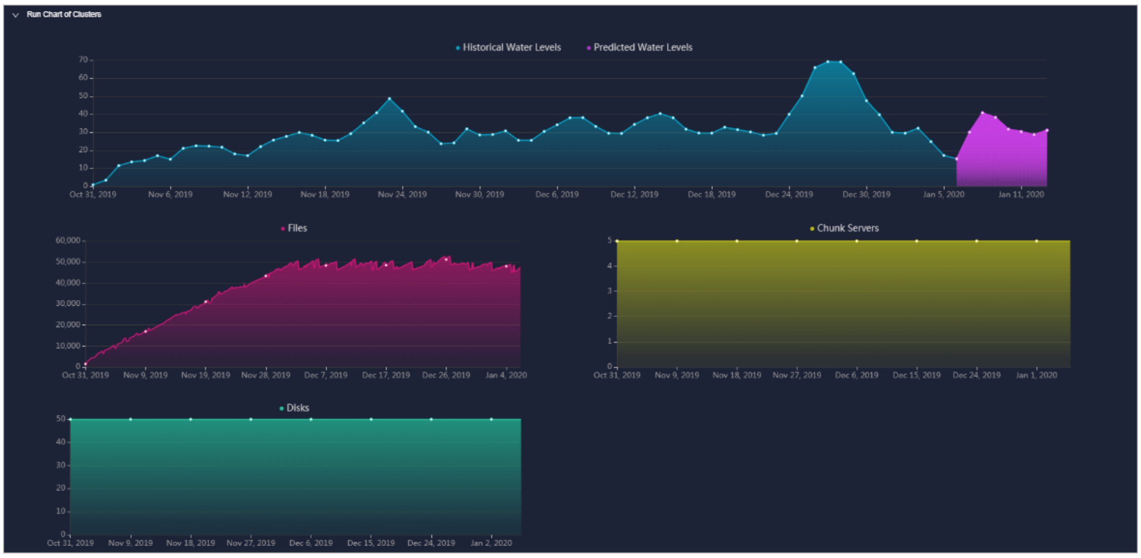
  This section shows the replica information of the specified cluster.

- ### Run Chart of Clusters

  This section shows the charts of historical and predicted usage information, number of files, number of chunk servers, and number of disks for the specified cluster.

  Predicted disk usage predicts the run chart of the next seven days.

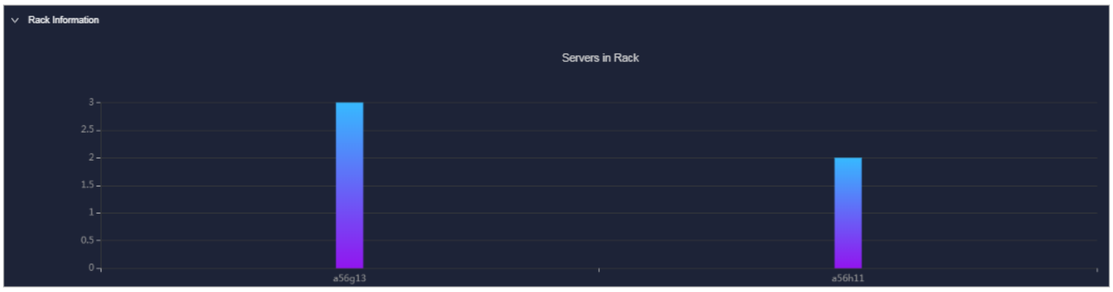
  > **Note** The disk usage can only be predicted if historical disk usage data exist. Some clusters may not have predicted disk usage data.



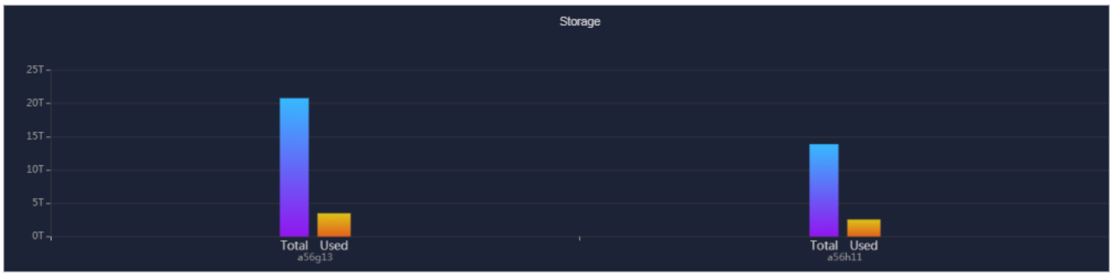
- ### Rack Information

  This section contains Storage and Servers in Rack.

- **Servers in Rack** shows the number of machines in each rack of the specified cluster.



- **Storage** shows the total and used storage of each rack in the specified cluster.



6.4.4. Nodes

The Nodes module allows you to view the information of master and chunk servers within a cluster.

Procedure

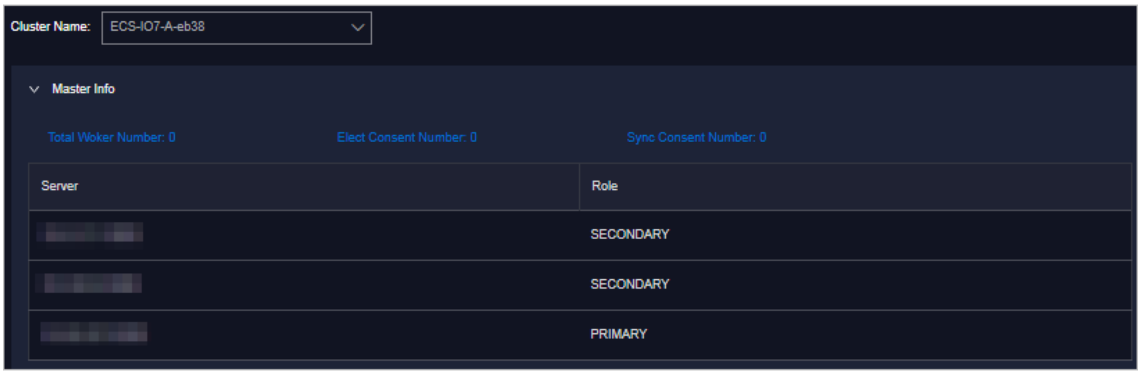
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Nodes**.

   On the page that appears, the data of the first cluster in the **Cluster Name** drop-down list is displayed, including the information of master and chunk servers.
4. Select the name of the cluster that you want to view from the **Cluster Name** drop-down list. The following information is displayed.

   > **Note** All the enabled clusters in the current environment are displayed in the **Cluster Name** drop-down list.

   - **Master Info**

     This section shows the master node information of the specified cluster. You can click **Refresh** in the upper-right corner of the section to refresh the master node information of the cluster.



Cluster Name: ECS-IO7-A-eb38

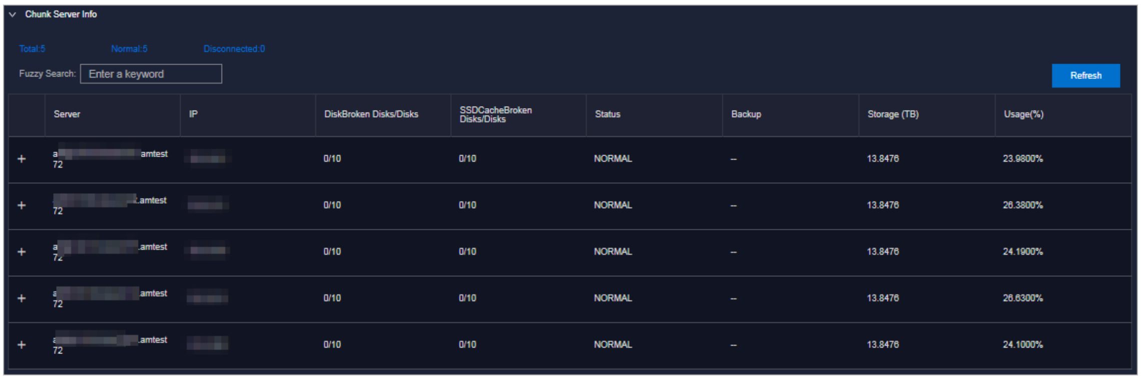
Master Info

Total Woker Number: 0 Elect Consent Number: 0 Sync Consent Number: 0

Server	Role
[redacted]	SECONDARY
[redacted]	SECONDARY
[redacted]	PRIMARY

- Chunk Server Info

  This section shows the chunk server information of the specified cluster. You can click **Refresh** in the upper-right corner of the section to refresh the chunk server information of the specified cluster. Click the ＋ icon in front of a server, the disk and SSD cache information of the server is displayed. Fuzzy search is supported in this section.



Chunk Server Info

Total:5 Normal:5 Disconnected:0

Fuzzy Search: Enter a keyword

Refresh

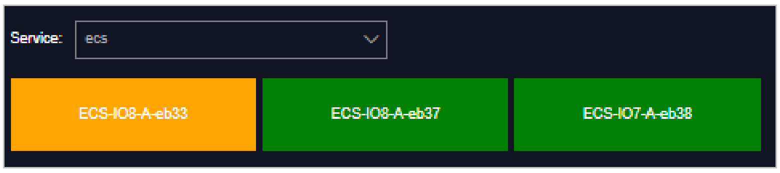
	Server	IP	DiskBroken Disks/Disks	SSDCacheBroken Disks/Disks	Status	Backup	Storage (TB)	Usage(%)
+	a[redacted]amtest 72	[redacted]	0/10	0/10	NORMAL	--	13.8476	23.9800%
+	[redacted].amtest 72	[redacted]	0/10	0/10	NORMAL	--	13.8476	26.3800%
+	a[redacted].amtest 72	[redacted]	0/10	0/10	NORMAL	--	13.8476	24.1900%
+	a[redacted].amtest 72	[redacted]	0/10	0/10	NORMAL	--	13.8476	26.6300%
+	a[redacted].amtest 72	[redacted]	0/10	0/10	NORMAL	--	13.8476	24.1000%

6.4.5. Operations and maintenance

The Operations and Maintenance module allows you to view the status of each cluster.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Operations and Maintenance**.
4. Select a service from the **Service** drop-down list to view the cluster status of the service. Clusters in different health states are displayed in different colors:
   - Green indicates that the cluster is working properly.
   - Yellow indicates that the cluster has a warning.
   - Red indicates that the cluster has an exception.
   - Dark red indicates that the cluster has a fatal error.
   - Grey indicates that the cluster is disabled.



Service: ecs

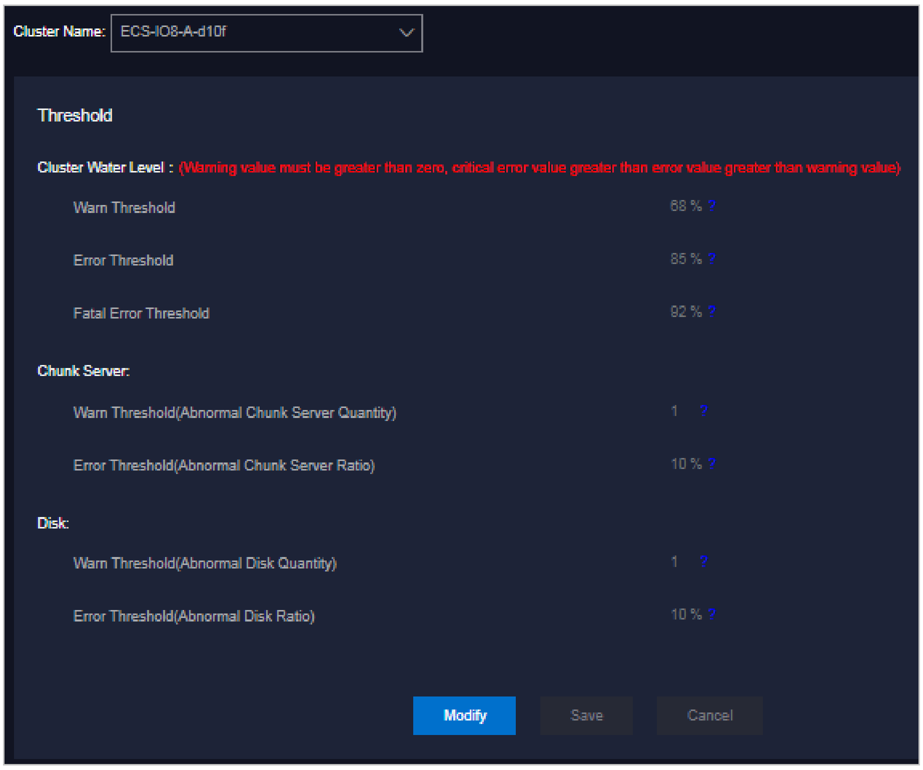
5. Move the pointer over a cluster name to view the service name, server name, and IP address of the cluster.

6.4.6. Modify cluster thresholds

By default, thresholds for all clusters are configured by the system. You can modify the thresholds for storage usage, chunk server, and disk of each cluster based on your needs.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Settings**.
4. In the **Cluster Name** drop-down list, select a cluster for which you want to modify the thresholds.
5. In the lower part of the page, click **Modify** and configure the parameters.



Cluster Name: ECS-IO8-A-d10f

Threshold

Cluster Water Level : (Warning value must be greater than zero, critical error value greater than error value greater than warning value)

Warn Threshold 68 %

Error Threshold 85 %

Fatal Error Threshold 92 %

Chunk Server:

Warn Threshold(Abnormal Chunk Server Quantity) 1

Error Threshold(Abnormal Chunk Server Ratio) 10 %

Disk:

Warn Threshold(Abnormal Disk Quantity) 1

Error Threshold(Abnormal Disk Ratio) 10 %

The following table describes the parameters.

Parameter	Description

Parameter		Description
Cluster Water Level	Warn Threshold	When the storage usage of the cluster is greater than or equal to this value, a warning alert is triggered and the health heatmap of the cluster is displayed in yellow. Value range: (0,100]. The default threshold for the cluster storage usage is 65%. Note: The fatal error threshold value must be greater than the error threshold value, and the error threshold value must be greater than the warn threshold value.
	Error Threshold	When the storage usage of the cluster is greater than or equal to this value, an error alert is triggered and the health heatmap of the cluster is displayed in red. Value range: (0,100]. The default threshold for the cluster storage usage is 85%. Note: The fatal error threshold value must be greater than the error threshold value, and the error threshold value must be greater than the warn threshold value.
	Fatal Error Threshold	When the storage usage of the cluster is greater than or equal to this value, a fatal-error alert is triggered and the health heatmap of the cluster is displayed in dark red. Value range: (0,100]. The default threshold for the cluster storage usage is 92%. Note: The fatal error threshold value must be greater than the error threshold value, and the error threshold value must be greater than the warn threshold value.
Chunk Server	Warn Threshold (Abnormal Chunk Server Quantity)	When the number of abnormal chunk servers is greater than or equal to this value, a warning alert is triggered and the health heatmap of the cluster is displayed in yellow. The default threshold for the number of abnormal chunk servers is 1.
	Error Threshold (Abnormal Chunk Server Ratio)	If the ratio of abnormal chunk servers to all the chunk servers is greater than this value, an error alert is triggered and the health heatmap of the cluster is displayed in red. The default threshold for the ratio of abnormal chunk servers to all the chunk servers is 10%.

Parameter		Description
Disk	**Warn Threshold (Abnormal Disk Quantity)**	When the number of abnormal disks is greater than or equal to this value, a warning alert is triggered and the health heatmap of the cluster is displayed in yellow. The default threshold for the number of abnormal disks is 1.
	Error Threshold (Abnormal Disk Ratio)	When the ratio of abnormal disks to all the disks is greater than this value, an error alert is triggered and the health heatmap of the cluster is displayed in red. The default threshold for the ratio of abnormal disks to all the disks is 10%.

> ⓘ **Note** To reset the configurations, you can click **Cancel** to cancel the current configurations.

6. Click **Save**.

6.4.7. Load information

The Load Information module allows you to view the NC information, VM information, and block device information.

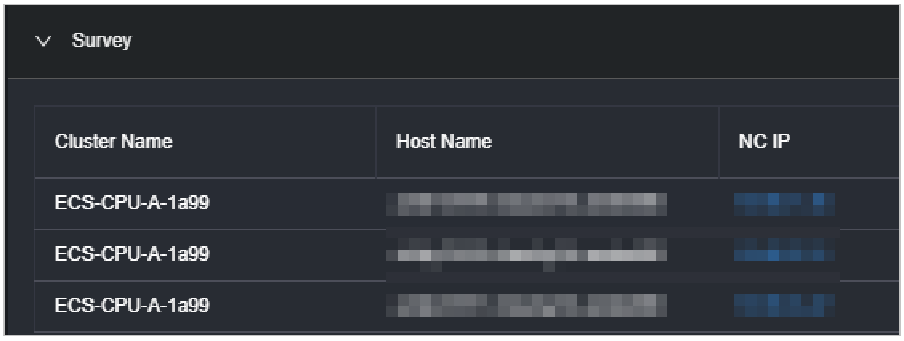
6.4.7.1. View NC information

The Load Information module allows you to view the data overview information for each NC and real-time data such as the load, CPU utilization, memory information, sda usage, traffic, TCP information, network exception metrics, read and write rate, BPS, kernel status, IOPS, and latency.

Procedure

1. Log on to the Apsara Uni-manager Operations Console. For more information, see Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Load Information**. The **NC Info** tab appears.
4. Select a cluster from the **Cluster Name** drop-down list and specify **Time Frame**. You can select **One Hour**, **Three Hours**, **Six Hours**, or **One Day**, or you can customize a time range. Click **Search** and view the following information:
   - Survey

     The **Survey** section shows all NCs in the current cluster. You can click the IP address of an NC to view the trend charts of real-time data of the NC in the current cluster.



Survey

Cluster Name	Host Name	NC IP
ECS-CPU-A-1a99	[redacted]	[redacted]
ECS-CPU-A-1a99	[redacted]	[redacted]
ECS-CPU-A-1a99	[redacted]	[redacted]

- Real-time load

  In the **Survey** section, click the IP address of an NC. In the **Real Time Load** section, the load trend chart of the NC within the specified time range is displayed. By default, the real-time load trend chart corresponding to the NC in the first row of the **Data Overview** section is displayed.

  The following information is displayed in the real-time load trend chart:

  - **load_1**: the average load of the NC within the last minute.
  - **load_5**: the average load of the NC within the last 5 minutes.
  - **load_15**: the average load of the NC within the last 15 minutes.

  You can drag the slider below the chart to zoom in or out the chart.

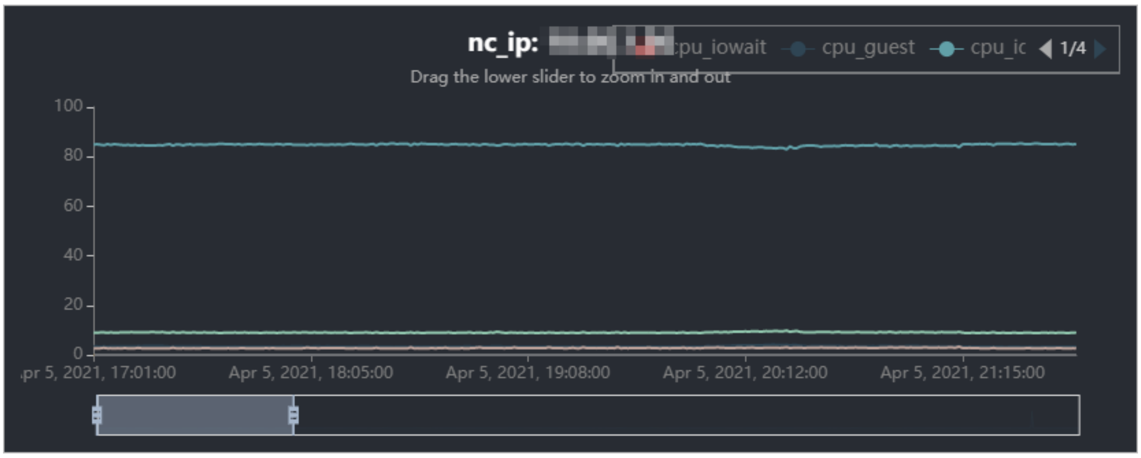
- Real-time CPU utilization

  In the **Survey** section, click the IP address of an NC. In the **Real-time CPU Utilization** section, the CPU utilization trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time CPU utilization trend chart:

  - **cpu_iowait**: the amount of time spent waiting for an I/O response.
  - **cpu_guest**: the run time duration of vCPUs in a guest OS.
  - **cpu_idle**: the duration for which vCPUs are available.
  - **cpu_hardirp**: the amount of time spent handling hardware interrupts.
  - **cpu_user**: the CPU time in user mode.
  - **cpu_softirp**: the amount of time spent handling software interrupts.
  - **cpu_steal**: the duration for which vCPUs are occupied by other VMs.
  - **cpu_sys**: the CPU time in system mode.
  - **cpu_nice**: the amount of CPU times consumed to process data for low-priority programs in user mode.

  You can drag the slider below the chart to zoom in or out the chart.



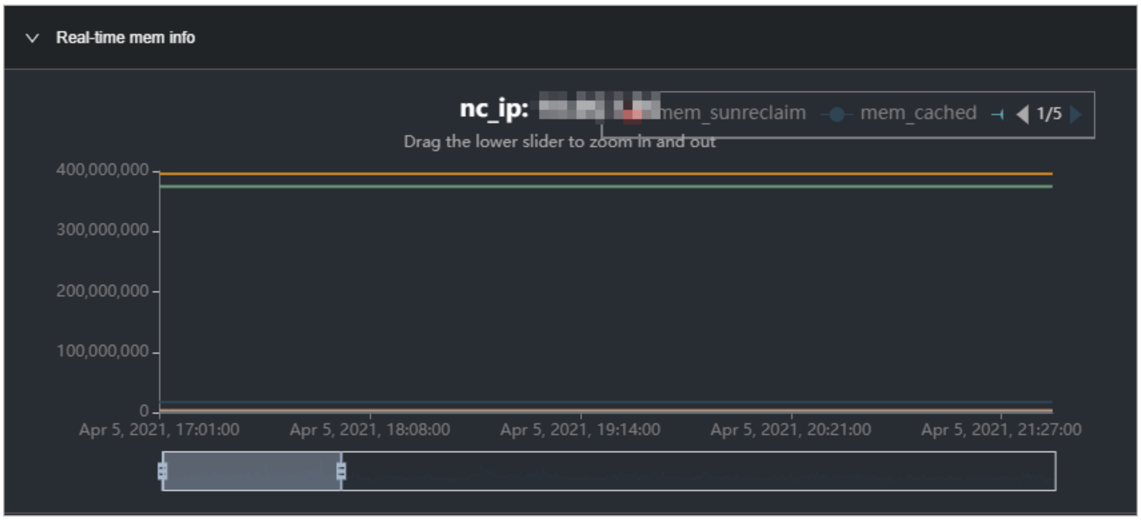
- Real-time memory information

  In the **Survey** section, click the IP address of an NC. In the **Real-time mem info** section, the memory usage trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time memory usage trend chart:

  - **mem_sunreclaim**: the amount of slab capacity in which the object is active and cannot be reclaimed.
  - **mem_cached**: the amount of physical memory that has been cached.
  - **mem_slab**: the total amount of the memory allocated by the slab allocator.
  - **mem_free**: the amount of available physical memory and swap space.
  - **mem_shmem**: the memory usage.
  - **mem_used**: the amount of physical memory and swap space that is occupied.
  - **mem_total**: the total amount of the physical memory and swap space of the system.
  - **mem_buffer**: the physical memory that has been buffered.
  - **mem_dirty**: the amount of dirty data, which is the data that is stored in the buffer zone but has not been written to physical disks.

  You can drag the slider below the chart to zoom in or out the chart.

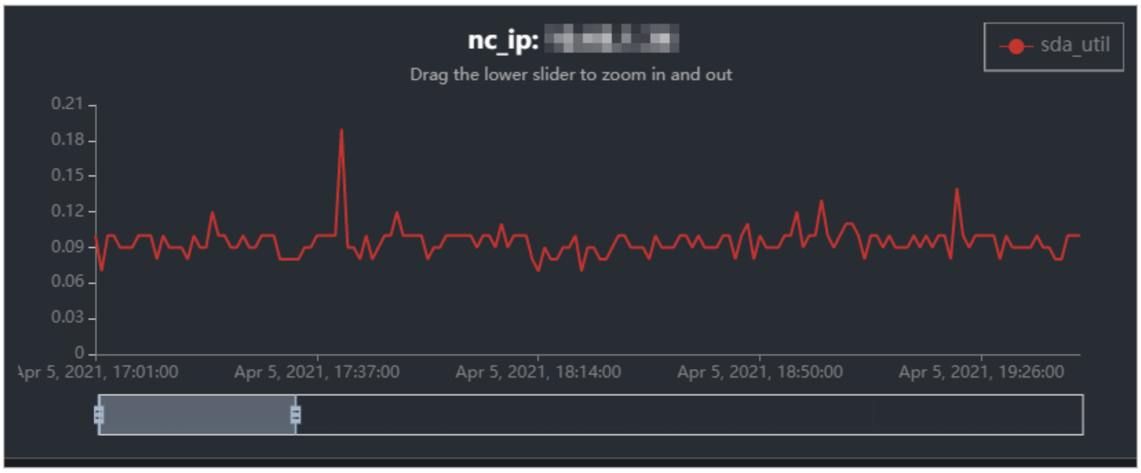


- Real-time sda usage

In the **Survey** section, click the IP address of an NC. In the **Real-time SDA utilization** section, the disk usage trend chart of the NC within the specified time range is displayed .

In the real-time sda usage trend chart, **sda_until** indicates the sda usage.

You can drag the slider below the chart to zoom in or out the chart.



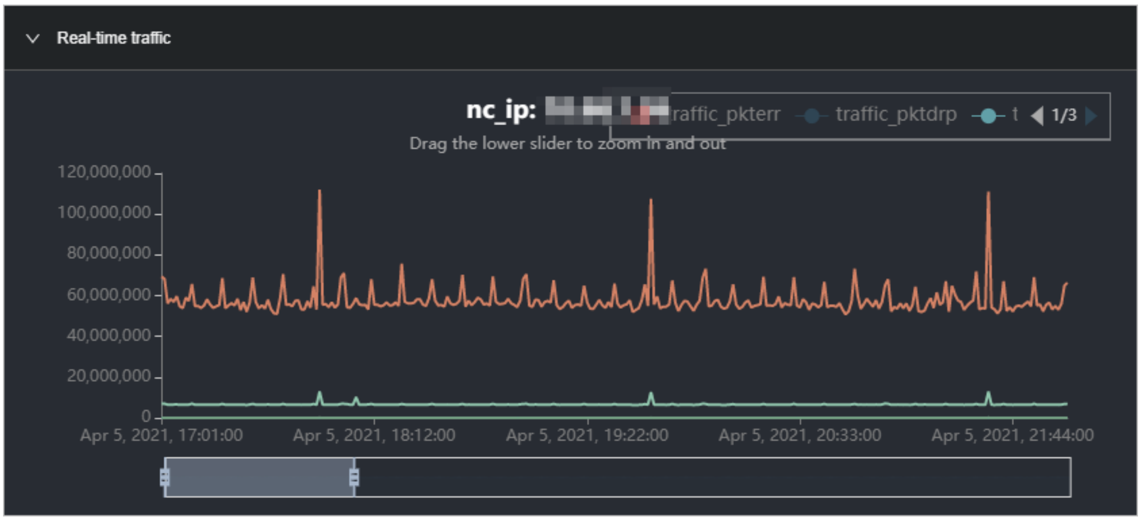
- Real-time traffic

  In the **Survey** section, click the IP address of an NC. In the **Real-time traffic** section, the traffic trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time traffic trend chart:

  - **traffic_pkterr**: the number of times that errors occur for transmission packages.
  - **traffic_pktdrp**: the number of times that transmission packets are lost.
  - **traffic_pktin**: the number of input bytes during the traffic peak.
  - **traffic_bytesout**: the number of output bytes.
  - **traffic_bytesin**: the number of input bytes.
  - **traffic_pktout**: the number of output bytes during the traffic peak.

  You can drag the slider below the chart to zoom in or out the chart.



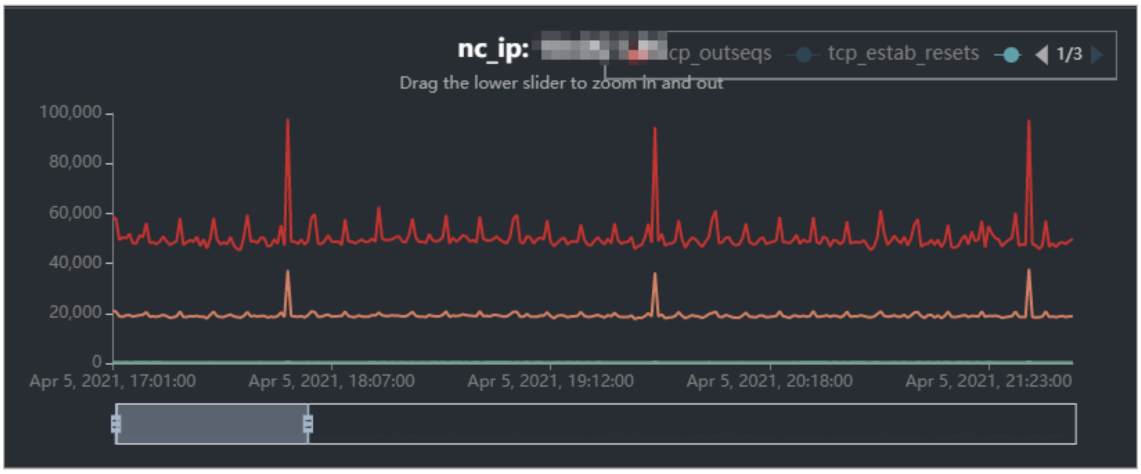
- Real-time TCP information

In the **Survey** section, click the IP address of an NC. In the **Real-time tcp Info** section, the TCP connection trend chart of the NC within the specified time range is displayed.

The following information is displayed in the real-time TCP connection trend chart:

- **tcp_outseqs**: the number of TCP packets that have been sent.
- **tcp_estab_resets**: the retry times of TCP connections that are in the ESTABLISHED state.
- **tcp_opens**: the number of open TCP connections.
- **tcp_inseqs**: the number of received TCP packets.
- **tcp_attempt_fails**: the number of failed connection attempts.
- **tcp_curr_estab**: the number of TCP connections that are in the ESTABLISHED state.

You can drag the slider below the chart to zoom in or out the chart.



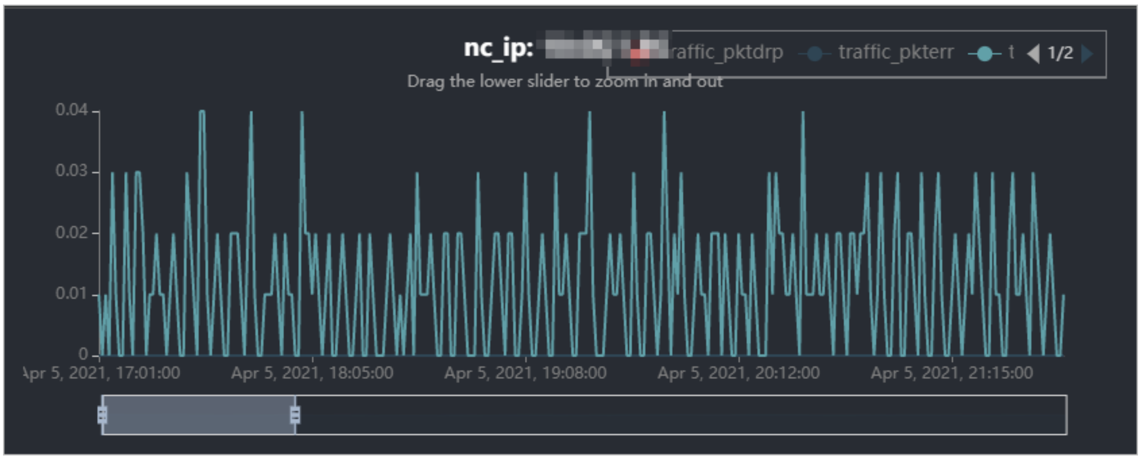
- ○ Real-time network exception metrics

  In the **Survey** section, click the IP address of an NC. In the **Real-time network anomaly metrics** section, the trend chart of the network exception metrics of the NC within the specified time range is displayed.

  The following information is displayed in the trend chart of the real-time network exception metrics:

  - **traffic_pktdrp**: the number of times that transmission packets are lost.
  - **traffic_pkterr**: the number of times that errors occur for transmission packets.
  - **traffic_retrans_ratio**: the number of times that transmission packets are retried.

  You can drag the slider below the chart to zoom in or out the chart.



- Reading and writing B/S

  In the **Survey** section, click the IP address of an NC. In the **Reading and Writing B/S** section, the trend chart of the reading and writing rate of the NC within the specified time range is displayed.

  The following information is displayed in the trend chart of the read and write rate :

  - **bs_w**: the write rate in byte/s.
  - **bs_r**: the read rate in byte/s.

  You can drag the slider below the chart to zoom in or out the chart.

- Real-time BPS

  In the **Survey** section, click the IP address of an NC. In the **Real-time BPS** section, the BPS trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time BPS trend chart:

  - **bps_w**: the writing rate in bps.
  - **bps_r**: the reading rate in bps.

  You can drag the slider below the chart to zoom in or out the chart.

- Real-time kernel status

  In the **Survey** section, click the IP address of an NC. In the **Real-time Kernel State** section, the kernel status trend chart of the NC within the specified time range is displayed.

  In the real-time kernel status trend chart, **kernel_status** indicates the real-time kernel status.

  You can drag the slider below the chart to zoom in or out the chart.

- Real-time IOPS

  In the **Survey** section, click the IP address of an NC. In the **Real-time iops** section, the IOPS trend chart of the NC within the specified time range is displayed.

  The following information is displayed in the real-time IOPS trend chart:

  - **iops_w**: the number of input operations per second.
  - **iops_r**: the number of output operations per second.

  You can drag the slider below the chart to zoom in or out the chart.

- Real-time latency

In the **Survey** section, click the IP address of an NC. In the **Real-time latency** section, the latency trend chart of the NC within the specified time range is displayed.

The following information is displayed in the real-time latency trend chart:

- **latency_w**: the real-time latency of data writes
- **latency_r**: the real-time latency of data reads
- **latency_w_qos**: the QoS intelligent adjustment for real-time latency of data writes
- **latency_r_qos**: the QoS intelligent adjustment for real-time latency of data reads

You can drag the slider below the chart to zoom in or out the chart.

6.4.7.2. View virtual machine information

The Load Information module allows you to view the data overview information and trend charts of read and write rate, real-time BPS, real-time IOPS, and real-time latency of all virtual machines (VMs).

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Load Information**. The **NC Info** tab appears.
4. Click the **Virtual Machine Information** tab.
5. Select a cluster from the **Cluster Name** drop-down list, select an NC IP address from the **nc_Ip** drop-down list, and then set **Time Frame** to **One Hour**, **Three Hours**, **Six Hours**, **One Day**, or a customized time range. Click **Search** and view the following information:
   - Survey

     The **Survey** section shows a list of all VMs under an NC of the selected cluster. Click a VM name to view the trend charts of the real-time data of the VM.
   - Reading and Writing B/S

     Click a VM name in the **Survey** section. In the **Reading and Writing B/S** section, the trend chart of the reading and writing rate of the current VM within the specified time range is displayed.

     You can drag the slider below the chart to zoom in or out the chart.

     - bs_w: the instance writing rate
     - bs_r: the instance reading rate
   - Real-time BPS

     Click a VM name in the **Survey** section. In the **Real-time BPS** section, the BPS trend of the current VM within the specified time range is displayed.

     You can drag the slider below the chart to zoom in or out the chart.

     - bps_w: the amount of data written per unit time
     - bps_r: the amount of data read per unit time
   - Real-time IOPS

Click a VM name in the **Survey** section. In the **Real-time iops** section, the IOPS trend chart of the current VM within the specified time range is displayed.

You can drag the slider below the chart to zoom in or out the chart.

- iops_w: the number of times per second data is written to the disk
- iops_r: the number of times per second data is read from the disk

- Real-time latency

  Click a VM name in the **Survey** section. In the **Real-time latency** section, the latency trend of the current VM within the specified time range is displayed.

  You can drag the slider below the chart to zoom in or out the chart.

  - latency_w: the real-time latency of data writes
  - latency_r: the real-time latency of data reads
  - latency_w_qos: the intelligent QoS adjustment of real-time data writing latency
  - latency_r_qos: the intelligent QoS adjustment of real-time delay in reading data

6.4.7.3. View block device information

The Load Information module allows you to view the overview information and the trend charts of the data read/write rate, real-time BPS, real-time IOPS, and real-time latency for each device.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Load Information**. The **NC Info** tab appears.
4. Click the **Block Device Information** tab.
5. Select a cluster from the **Cluster Name** drop-down list, select an NC IP from the **nc_Ip** drop-down list, select an instance name from the **vmName** drop-down list, and then specify **Time Range** (**1 Hour**, **3 Hours**, **6 Hours**, **One Day** or a customized time range). Click **Search**. View the following information:
   - Survey

     The **Survey** section shows the information about all block devices in each VM of an NC in the current cluster. You can click a disk ID to view the real-time data trend charts for the device.

   - Reading and Writing B/S

     In the **Survey** section, click a disk ID. In the **Reading and Writing B/S** section, the read/write rate trend chart of the current block device within the specified time range appears.

     You can drag the slider below the chart to zoom in or out the chart.

     - bs_w: the instance writing rate
     - bs_r: the instance reading rate

   - Real-time BPS

In the **Survey** section, click a disk ID. In the **Real-time BPS** section, the BPS trend chart of the current block device within the specified time range appears.

You can drag the slider below the chart to zoom in or out the chart.

- bps_w: the volume of data written per unit time
- bps_r: the volume of data read per unit time

- Real-time IOPS

  In the **Survey** section, click a disk ID. In the **Real-time iops** section, the IOPS trend chart of the current block device within the specified time range appears.

  You can drag the slider below the chart to zoom in or out the chart.

  - iops_w: the number of times that data is written to the disk per second
  - iops_r: the number of times that data is read from the disk per second

- Real-time latency

  In the **Survey** section, click a disk ID. In the **Real-time latency** section, the latency trend chart of the current block device with the specified time range appears.

  You can drag the slider below the chart to zoom in or out the chart.

  - latency_w: the real-time latency of data writes
  - latency_r: the real-time latency of data reads
  - latency_w_qos: the QoS intelligent adjustment for real-time latency of data writes
  - latency_r_qos: the QoS intelligent adjustment for real-time latency of data reads

6.4.8. EBS dashboard

The EBS Dashboard module allows you to view the overview information and cluster usage trend charts of EBS clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > EBS Dashboard**. On the page that appears, cluster overview information and cluster usage trend charts of all EBS clusters are displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. View the following information:
   - The **Overview** section shows data overview information of the selected cluster, including the storage space, server information, and health information.

     In the **Health** section, when the value of **Abnormal Cloud Disks**, **Abnormal Masters**, **Abnormal Block GcWorker**, or **Abnormal Block Servers** is greater than 0, it is displayed in red.
   - The **Trend Chart of Cluster Usage** section shows the storage usage curve of the cluster for the last 30 days.

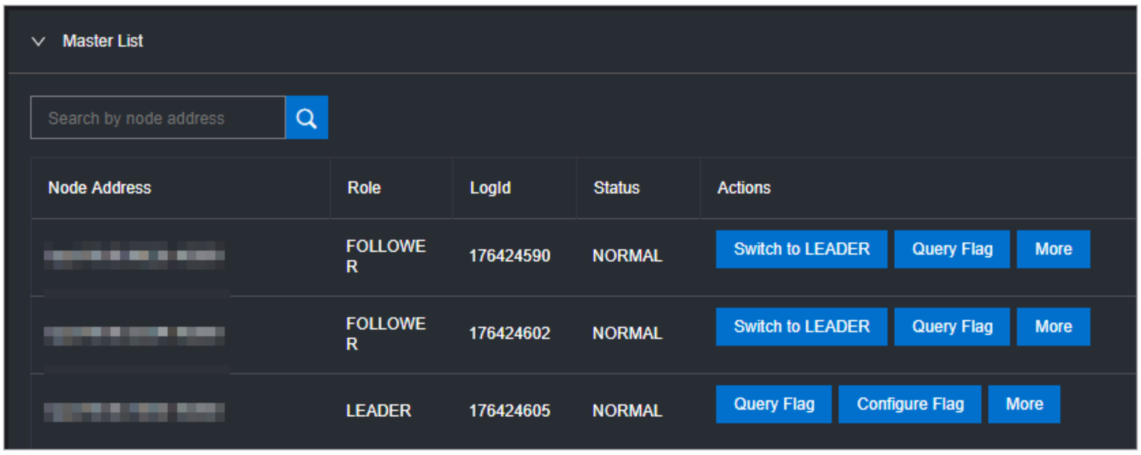
6.4.9. Block master operations

The Block Master Operations module shows the block master node information of EBS clusters, including the IP addresses and roles of nodes. The module also allows you to switch the role of a node to LEADER as well as query and configure flags.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Block Master Operations**. On the page that appears, the master node list and cluster information of the first cluster in the **Cluster Name** drop-down list are displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. In the **Master List** section, perform the following steps:
   - View the master node list

     You can view the master node information of the selected cluster, including the IP address, role, log ID, and status.



Master List

Search by node address

Node Address	Role	LogId	Status	Actions
[redacted]	FOLLOWER	176424590	NORMAL	Switch to LEADER Query Flag More
[redacted]	FOLLOWER	176424602	NORMAL	Switch to LEADER Query Flag More
[redacted]	LEADER	176424605	NORMAL	Query Flag Configure Flag More

   - Switch to LEADER

     A LEADER role for a master node has the same functions as a FOLLOWER role, including controlling and scheduling resources, as well as controlling deployment and service configurations.

     If a node in the master node list assumes a FOLLOWER role, you must switch its role to LEADER. Click **Switch to LEADER** in the **Actions** column. In the message that appears, click **OK**.

   - Query a flag

     In the master node list, click **Query Flag** in the **Actions** column corresponding to a node. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the block master node are displayed.

     Perform the following steps to query the flag_key value:

     a. In the left-side navigation pane of the Apsara Infrastructure Management Framework console, choose **Operations > Cluster Operations**.

     b. Enter EBS in the **Cluster** search box.

     c. Find the EBS cluster and click the cluster name.

   d. Click the **Configure** tab.

   e. Find the *pangu_blockmaster_flag.json* file in */services/EbsBlockMaster/user/pangu_blockmaster.*

      The flag_key values of all block master nodes are stored in the *pangu_blockmaster_flag.json* file.

- Configure a flag

  If you want to modify the deployment and service configurations of a block master node, you can configure a flag and assign it to the node.

  In the master list, find a node that assumes the LEADER role and click **Configure Flag** in the **Actions** column. In the dialog box that appears, configure the parameters and click **OK**.

  The following table describes the parameters.

Parameter	Description
flag_key	This value is obtained from the service template of the EBS cluster that is stored in the *pangu_blockmaster_flag.json* file.
flag_value	This value is customized.
flag_type	Select a flag type. Valid values: ■ **int** ■ **bool** ■ **string** ■ **double**

- Check the maser node status

  In the master node lits, choose **More > Check Master Status** in the **Actions** column corresponding to a node.

- Query the version information

  In the master node list, choose **More > Query Version Information** in the **Actions** column corresponding to a node.

6. In the **Cluster Overview** section, you can query the disk size, number of segments, total storage size, and storage usage of the cluster.

6.4.10. Block server operations

The Block Server Operations module shows the block server node information of EBS clusters, including the IP address, status, and real-time server load. The module also allows you to query and modify flags, configure server node status, as well as add nodes to and delete nodes from blacklists.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.

3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Block Master Operations**. On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. In the **Server List** section, perform the following operations:
   - View the server node list

     You can view server node information of the cluster, including the IP addresses, status, number of segments, and real-time load (read IOPS, write IOPS, read bandwidth, write bandwidth, read latency, and write latency).
   - Query a flag

     In the server list, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the block server node are displayed.

     Perform the following steps to query the flag_key value:

     a. In the left-side navigation pane of the Apsara Infrastructure Management Framework console, choose **Operations > Cluster Operations**.
     b. Enter EBS in the **Cluster** search box.
     c. Find the EBS cluster and click the cluster name.
     d. Click the **Configure** tab.
     e. Find the *pangu_blockserver_flag.json* file in */services/EbsBlockServer/user/pangu_blockserver*.

        The flag_key values of all block server nodes are stored in the *pangu_blockserver_flag.json* file.
   - Configure a flag

     In the server list, find a node and click **Configure Flag** in the **Actions** column. In the dialog box that appears, set flag_key and flag_value, select flag_type, and then click **OK**.

     The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the *pangu_blockserver_flag.json* file.
flag_value	The customized falg value.
flag_type	The flag type. Valid values: ▪ int ▪ bool ▪ string ▪ double

- Configure server node status

  In the server list, find a node and choose **More > Set Server Status** in the **Actions** column. In the dialog box that appears, specify server node status and click **OK**.

  The following table describes the server node status.

Status	Description
NORMAL	Indicates that the node is running normally.
DISCONNECTED	Indicates that the node is disconnected.
OFFLOADING	Indicates that the node is being disabled.
OFFLOADED	The node is disabled.
UPGRADE	The node is upgraded.
RECOVERY	The node is restored.

- Query the version information

  In the server list, find a node and choose **More > Query Version Information** in the **Actions** column. In the dialog box that appears, view the version information of the block server node.

6. In the **Block Server Blacklist** section, perform the following operations:

   - Add a block server node to the blacklist

     In the upper-right corner of the **Block Server Blacklist** section, click **Add**. In the dialog box that appears, select the IP address of the block server node that you want to add to the blacklist and click **OK**.

     The block server node that was added to the blacklist is disabled and no longer provides services.

   - View the block server blacklist

     You can view all block server nodes that are added to the blacklist in the **Block Server Blacklist** section.

   - Remove a block server node from the blacklist

     In the **Block Server Blacklist** section, find the block server node that you want to remove from the blacklist and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

     The block server node that is removed from the blacklist can continue to provide services.

6.4.11. SnapShotServer

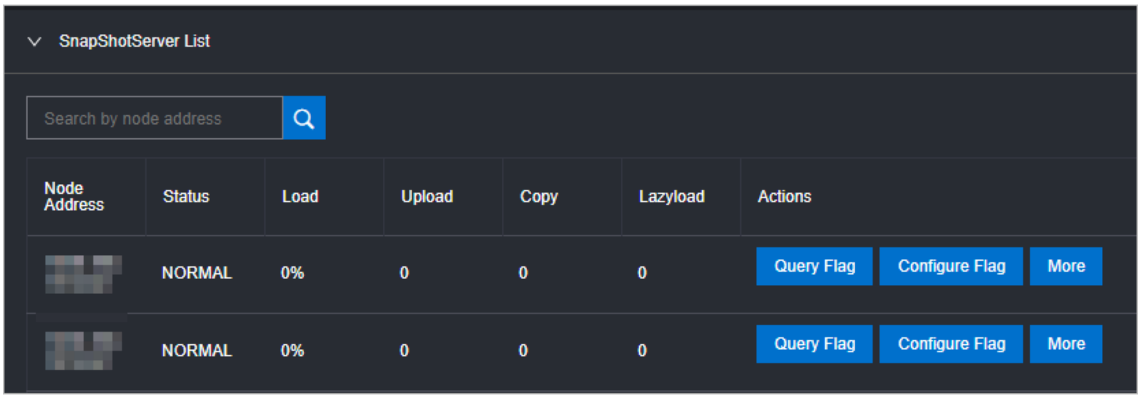
The SnapShotServer module shows the snapshot server node information of EBS clusters, including the IP address, status, and other performance parameters. The module also allows you to query and modify flags and configure snapshot server node status.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.

3. In the left-side navigation pane, choose **Apsara Distributed File System Management > SnapShotServer**. On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. Perform the following operations:
   - View the snapshot server node list

     You can view snapshot server node information of the cluster, including the IP address, status, loading rate, and the number of uploads, replicas, and delayed loadings.

Node Address	Status	Load	Upload	Copy	Lazyload	Actions
[redacted]	NORMAL	0%	0	0	0	Query Flag Configure Flag More
[redacted]	NORMAL	0%	0	0	0	Query Flag Configure Flag More

   - Query a flag

     In the snapshot server node list, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the snapshot server node are displayed.

     Perform the following steps to query the flag_key value:

     a. In the left-side navigation pane of the Apsara Infrastructure Management Framework console, choose **Operations > Cluster Operations**.
     b. Enter EBS in the **Cluster** search box.
     c. Find the EBS cluster and click the cluster name.
     d. Click the **Configure** tab.
     e. Find the *pangu_snapshotserver_flag.json* file in */services/EbsSnapshotServer/user/pangu_snapshotserver*.

        The flag_key values of all snapshot server nodes are stored in the *pangu_snapshotserver_flag.json* file.

   - Configure a flag

     In the snapshot server node list, find a node and click **Configure Flag** in the **Actions** column. In the dialog box that appears, set flag_key, flag_value, and flag_type, and then click **OK**.

     The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the *pangu_snapshotserver_flag.json* file.

Parameter	Description
flag_value	The customized flag value.
flag_type	The flag type. Valid values: ▪ **int** ▪ **bool** ▪ **string** ▪ **double**

- Configure the snapshot server node status

  In the snapshot server node list, find a node and choose **More** > **Set snapshotserver Status** in the **Actions** column. In the dialog box that appears, select the snapshot server node status and click **OK**.

  The following table describes the snapshot server node status.

Status	Description
NORMAL	Indicates that the node is running normally.
DISCONNECTED	Indicates that the node is disconnected.
OFFLOADING	Indicates that the node is being disabled.
OFFLOADED	Indicates that the node is disabled.

- Query the version information

  In the snapshot server node list, find a node and choose **More** > **Version Information** in the **Actions** column. In the dialog box that appears, view the version information of the node.

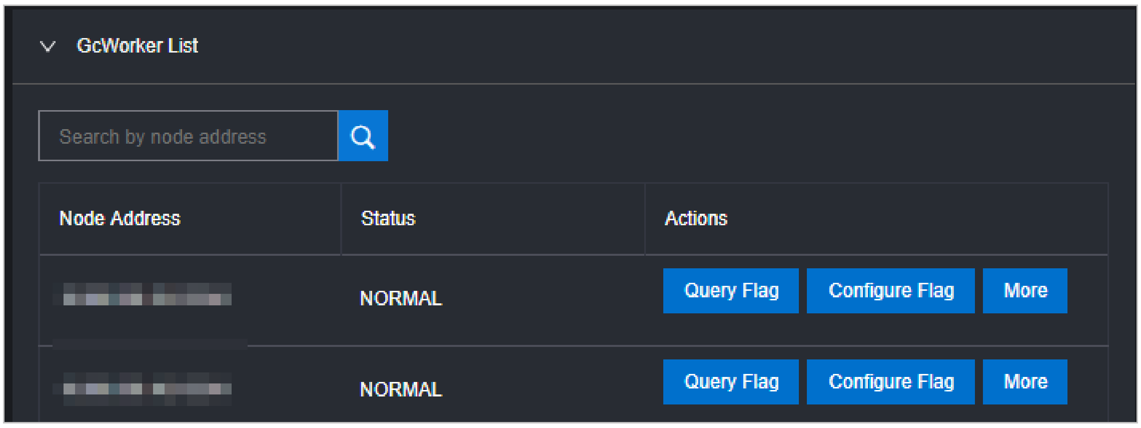
6.4.12. Block gcworker operations

The Block Gcworker Operations module allows you to view the IP addresses and status of block gcworker nodes in EBS clusters. You can also query and modify flags, configure the gcworker node status, and query version information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management** > **Block Gcworker Operations**. On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. Perform the following operations:
   - View the gcworker node list

You can view the IP addresses and status of the block gcworker nodes in the selected cluster.



Node Address	Status	Actions
[redacted]	NORMAL	Query Flag Configure Flag More
[redacted]	NORMAL	Query Flag Configure Flag More

- Query a flag

  In the gcworker node list, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the block gcworker node are displayed.

  Perform the following steps to query the flag_key value:

  a. In the left-side navigation pane of the Apsara Infrastructure Management Framework console, choose **Operations > Cluster Operations**.

  b. Enter EBS in the **Cluster** search box.

  c. Find the EBS cluster and click the cluster name.

  d. Click the **Configure** tab.

  e. Find the *pangu_blockgcworker_flag.json* file in */services/EbsBlockGCWorker/user/pangu_blockgcworker*.

     The flag_key values of all block server nodes are stored in the *pangu_blockgcworker_flag.json* file.

- Configure a flag

  In the gcworker node list, find a node and click **Configure Flag** in the **Actions**column. In the dialog box that appears, set flag_key, flag_value, and flag_type and click **OK**.

  The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the *pangu_blockgcworker_flag.json* file.
flag_value	The customized flag value.

Parameter	Description
flag_type	The flag type. Valid values: ■ int ■ bool ■ string ■ double

- Configure the gcworker node status

  In gcworker node list, find a node and choose **More > Configure gcworker Status** in the **Actions** column. In the dialog box that appears, specify the gcworket node status and click **OK**.

  The following table describes the gcworker node status.

Status	Description
NORMAL	Indicates that the node is running normally.
DISCONNECTED	Indicates that the node is disconnected.
OFFLOADING	Indicates that the node is being disabled.
OFFLOADED	Indicates that the node is disabled.

- Query the version information

  In the gcworker node list, find a node and choose **More > Query Version Information** in the **Actions** column. In the dialog box that appears, view the version information of the block gcworker node.

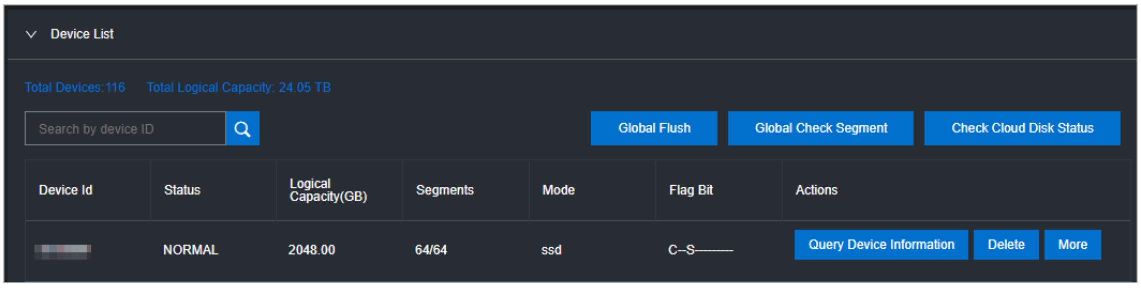
6.4.13. Device operations

The Device Operations module allows you to view disk information in EBS clusters, such as the disk ID, status, capacity, and category. You can also perform flush operations, modify disk configurations, query segment information, and enable, disable, delete, or restore devices.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Device Operations**. On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. Perform the following operations:
   - View the device list

You can view the total number of devices, the total logical space of devices, and information about each device in the cluster, including the device ID, status, logical capacity, number of segments, mode, and flags.



Total Devices:116 Total Logical Capacity: 24.05 TB

Device Id	Status	Logical Capacity(GB)	Segments	Mode	Flag Bit	Actions
[redacted]	NORMAL	2048.00	64/64	ssd	C--S--------	Query Device Information Delete More

- Global check segments

  In the upper-right corner of the **Device List** section, click **Global Check Segment**. You can view all the segments in the selected cluster and their indexes and status.

- Check disk status

  In the upper-right corner of the **Device List** section, click **Check Cloud Disk Status**. You can view the number of invalid disks in the selected cluster.

- Query device information

  In the device list, click **Query Device Information** in the **Actions** column corresponding to a device. In the dialog box that appears, view the disk information such as the disk ID, status, and capacity.

- Delete a device

  In the device list, click **Delete** in the **Actions** column corresponding to a disk.

  After you delete the disk, its status becomes **DELETING**, and the disk is unavailable. You are not allowed to perform operations on the deleted disk, such as enabling the device or modifying the configurations.

- Restore a device

  In the device list, find a deleted device that is in the **DELETING** state and click **Restore** in the **Actions** column. In the dialog box that appears, click **OK** to restore the deleted device to its normal state.

  After you restore the disk, it becomes available. You can perform operations on the disk, such as enabling the disk and modifying the configurations.

- Enable a device

  In the device list, find a device and choose **More** > **Enable** in the **Actions** column. In the dialog box that appears, configure the required parameters and click **Submit**.

  > **Note** You can perform read and write operations on a disk only after the disk is enabled.

  The following table describes the parameters for enabling a device.

Parameter	Description

Parameter	Description
client_ip	Optional. Specifies the client on which the disk is enabled. The client IP address is the IP address of the block server. If the client IP address is not specified, the IP address of the local server is used.
token	Specifies a string as a token to be used to disable the device.
mode	Specifies the disk mode. Valid values: ■ **ro**: read-only ■ **rw**: read/write Default value: **rw**.

- Disable a device

  > **Notice** After a disk is disabled, data can no longer be read from or written to the disk. Proceed with caution.

  In the device list, find a device and choose **More > Disable** in the **Actions** column corresponding to the device. In the dialog box that appears, configure the parameters and click **Submit**.

  The following table describes the parameters for disabling a device.

Parameter	Description
client_ip	Specifies the client IP address of the disk to be disabled. If the client IP address is not specified, the IP address of the local server is used.
token	Specifies the token for disabling the device, which is configured when the device is enabled. You can query the token by running the **dev -query** command on any server located in the EBS cluster.
open_ver	Specifies the current openversion of the device if the client IP address is not specified. If a client IP address is specified, you do not need to specify openversion. You can query openversion by running the **dev -query** command on any server in the EBS cluster.

- Flush

  In the device list, find a device and choose **More > Flush** in the **Actions** column corresponding to the device. In the dialog box that appears, configure the parameters and click **Submit**.

  The following table describes the parameters.

Parameter	Description
segment	Specifies the segments to be flushed. If you do not specify segments, all segments are flushed.
ifnsw	Valid values: ▪ **0**: specifies to flush the index file. ▪ **1**: specifies not to flush the index file.
dfnsw	Valid values: ▪ **0**: specifies to flush the data files. ▪ **1**: specifies not to flush the data files.

- Global flush

  You can perform the flush operation to clear disks or the transaction logs of segments.

  On the right of the **Device List** section, click **Global Flush**. In the dialog box that appears, select ifnsw and dfnsw, and click **OK**. Then, the transaction logs of all the disks or segments in the current cluster are flushed.

- Query configuration status

  In the device list, find a device and choose **More > Query Configuration Status** in the **Actions** column corresponding to the device. In the dialog box that appears, enter config_ver and click **OK**. You can determine whether the disk is configurable based on the check result.

  config_ver is the config_version parameter of the queried device information.

- Modify device configurations

  You can modify the configurations of a disk, such as specifying whether to enable data compression, compression algorithms, and storage modes.

  In the device list, find a device and choose **More > Modify Device Configurations** in the **Actions** column corresponding to the device. In the dialog box that appears, modify the parameters and click **OK**.

  The following table describes the parameters.

Parameter	Description
compress	Specifies whether to enable data compression. Valid values: ▪ **enable** ▪ **disable**

Parameter	Description
algorithm	Specifies a data compression algorithm. Valid values: ■ **0**: indicates that no data compression algorithms are used. ■ **1**: indicates that the snappy data compression algorithm is used. ■ **2**: indicates that the LZ4 data compression algorithm is used.
ec	Specifies whether to enable the EC storage mode. Default value: disable. Valid values: ■ **enable** ■ **disable**
data_chunks	Specifies the number of data chunks. Default value: 8.
parity_chunks	Specifies the number of parity chunks. Default value: 3.
packet_bits	Specifies the size of single data block in EC mode. Default value: 15.
copy	Specifies the number of data replicas. Default value: 3.
storage_mode	Specifies the storage mode of the disk.
cache	Specifies whether to enable the cache mode. Default value: 0. Valid values: ■ **0**: disabled ■ **1**: enabled
storage_app_name	Specifies the data storage name.
simsuppress	Specifies whether to enable the delay simulation feature. Default value: disable. Valid values: ■ **enable** ■ **disable**
baselatency	Specifies the basic latency. Default value: 300.
consumespeed	Specifies the processing speed. Default value: 256 bit/μs.
lat80th	Specifies the quantile jitter control of the latency as 80%.
lat90th	Specifies the quantile jitter control of the latency as 90%.
lat99th	Specifies the quantile jitter control of the latency as 99%.

- Query segment information

  In the device list, find a device and choose **More > Segment Information** in the **Actions** column corresponding to the device. In the dialog box that appears, view the information about the segments, such as the index and status.

- Check a segment

  In the device list, find a device and choose **More > Check Segment** in the **Actions** column corresponding to the device. In the dialog box that appears, select the segment to be checked and click **Submit**.

6.4.14. Enable or disable Rebalance

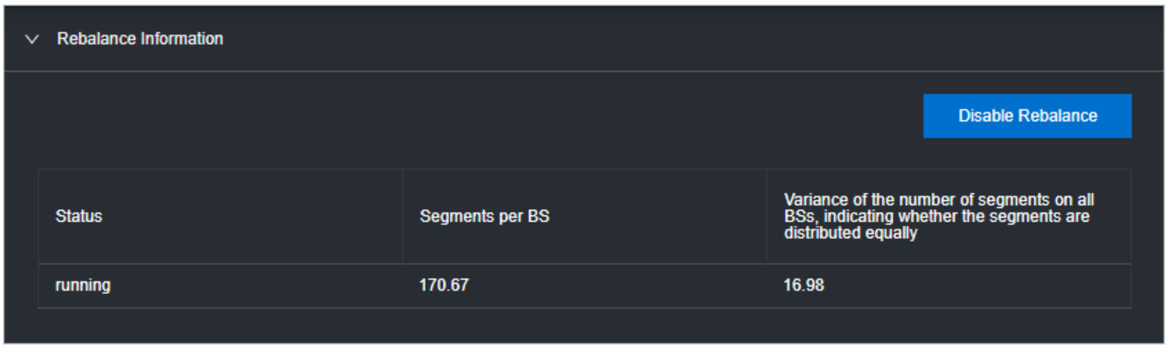
When segments are unevenly distributed among block servers, you can enable the Rebalance feature to redistribute the segments. After you redistribute the segments, you can disable Rebalance.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Rebalance**.
4. Click **Enable Rebalance** or **Disable Rebalance**.

   After you click **Enable Rebalance**, the status of Rebalance changes to **running**.

   After you click **Disable Rebalance**, the status of Rebalance changes to **stopped**.



Status	Segments per BS	Variance of the number of segments on all BSs, indicating whether the segments are distributed equally
running	170.67	16.98

6.4.15. IO hang fault analysis

The IO HANG module allows you to view the affected virtual machine (VM) list, VM cluster statistics, and device cluster statistics.

Procedure

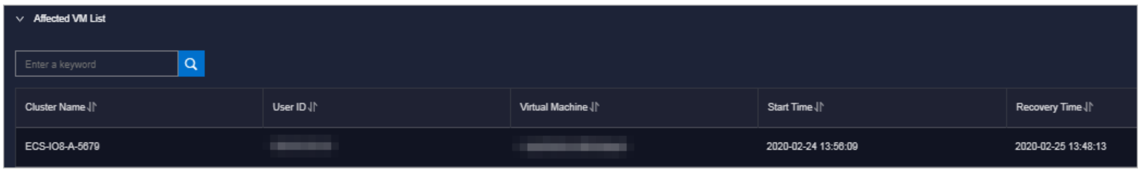
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > IO HANG**. By default, the system shows the affected VM list, VM cluster statistics, and device cluster statistics for the last 24 hours.
4. Select a time range (**One Hour**, **Three Hours**, **Six Hours**, **One Day**, or a customized time range)

and click **Search**. View the following information:

- **Affected VM List**

  The **Affected VM List** section shows the IO hang start time and recovery time of all the VMs, as well as the cluster name and user ID of the cluster to which these VMs belong.

  To view the information of a cluster, a user, or a VM, enter the cluster name, user ID, or VM name in the search box to perform a fuzzy search.

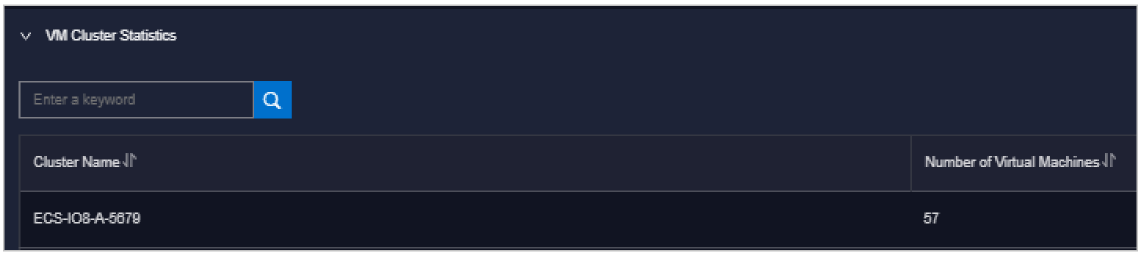
  

Cluster Name	User ID	Virtual Machine	Start Time	Recovery Time
ECS-IO8-A-5679	[redacted]	[redacted]	2020-02-24 13:56:09	2020-02-25 13:48:13

- **VM Cluster Statistics**

  The **VM Cluster Statistics** section shows the number of affected VMs in a cluster.

  To view the VM statistics of a cluster, enter the cluster name in the search box to perform a fuzzy search.

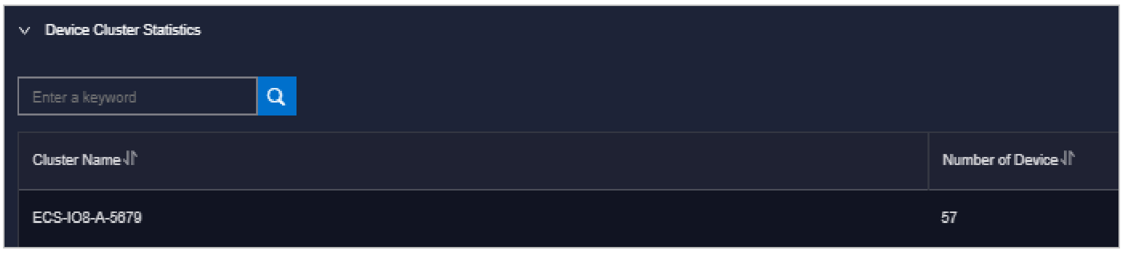
  

Cluster Name	Number of Virtual Machines
ECS-IO8-A-5679	57

- **Device Cluster Statistics**

  The **Device Cluster Statistics** section shows the number of affected devices in a cluster.

  To view the device statistics of a cluster, enter the cluster name in the search box to perform a fuzzy search.

Cluster Name	Number of Device
ECS-IO8-A-5679	57

6.4.16. Slow IO analysis

The Slow IO Analysis page allows you to view the slow IO list, top ten NCs, cluster statistics, top five cluster statistics, and reasons.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > SLOW IO**. By default, the system shows the slow IO list, top ten NCs, cluster statistics, top five cluster statistics, and reasons in the last 24 hours.

4. Select the time range (**One Hour**, **Three Hours**, **Six Hours**, **One Day**, or customize the time range) and click **Search**. View the following information:
   - **Slow IO List**

     The **Slow IO List** section shows the slow IO-related cluster name, NC IP address, virtual machine, device ID, storage type, start time, recovery time, number of slow IOs, and causes.

     To view the information of a cluster, an NC, or a block device, you can enter the cluster name, NC IP address, or device ID in the search box to perform a fuzzy search.

     You can also sort data by Cluster Name, NC IP, Virtual Machine, Device ID, Storage Type, Start Time, Recovery Time, Number of Slow IO, or Reason.
   - **Top10 NC**

     The system shows the information of the top ten NCs on a graph and table.

     Notes:

     - The **Graphical Analysis** section shows the proportion for the number of slow IO in each cluster of the top ten NCs by using a pie chart.
     - The **Top10 NC** section shows the NC IP address, cluster name, number of slow IOs, percentage, and primary cause of slow IOs on the top ten NCs.

       To view the information of a cluster or NC, enter the NC IP address or cluster name in the search box to perform a fuzzy search.

       You can also sort data by NC IP, Cluster Name, Slow IO, and Major Reason.
   - **Cluster Statistics**

     The **Cluster Statistics** section shows the cluster name, number of devices, number of slow IOs, percentage, and primary cause of slow IOs on clusters.

     To view the information of a cluster, enter the cluster name in the search box to perform a fuzzy search.

     You can also sort data by Cluster Name, Number of Device, Number of Slow IO, and Major Reason.
   - **Top Five Cluster Statistics**

     The system shows the statistics of top five clusters by using a graph and a table.

     Notes:

     - The **Graphical Analysis** section shows the proportion for the number of slow IOs on each of the top five clusters on a pie chart.
     - The **Top Five Cluster Statistics** section shows the cluster name, number of devices, number of slow IOs, percentage, and primary cause of slow IOs on the top five clusters on a table.

       To view the information of a cluster, enter the cluster name in the search box to perform a fuzzy search.

       You can also sort data by Top Five Cluster, Number of Device, Number of Slow IO, and Major Problem.
   - **Reason**

     The system shows the primary cause on a graph and table.

     Notes:

- The **Graphical Analysis** section shows the proportion of reasons by using a pie chart.
- The **Reason** section shows the number of slow IO from the dimension of reasons.

  To query the information of a reason, enter the reason information in the search box to perform a fuzzy search.

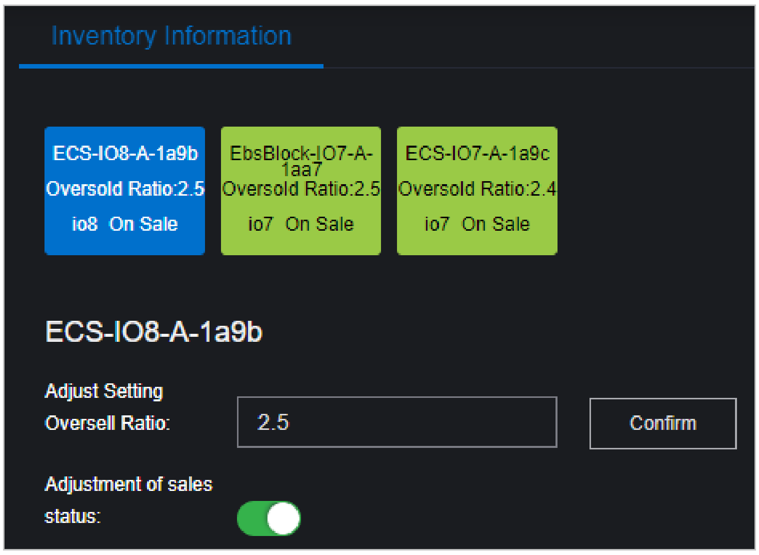
  You can also sort data by Reason and Number of Slow IO.

6.4.17. Product settings

The Product Settings module allows you to view the sales status of a cluster, configure the oversold ratio of a cluster, and specify whether a cluster is available for sale.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Product Settings**. By default, the system shows the data of each cluster within the current environment, including the cluster name, oversold ratio, and sales status.



4. Perform the following operations:
   - Select a cluster, enter a number in the **Adjust Setting Oversell Ratio** field, and then click **Confirm** to set the oversold ratio of the cluster.
   - Select a cluster and turn on or off **Adjustment of sales status** to enable or disable the cluster for sale.

6.5. Task Management

The system allows you to run operations scripts on the cloud platform, which reduces your actions by using command lines, lowers misoperations, and improves the security and stability of the cloud platform.

6.5.1. Overview

The Task Management module supports the following features:

- Supports task overview and quick task creation.
- Supports the manual, scheduled, regular, and advanced modes.
- Supports the breakpoint feature for scripts, which allows a task to be paused between two scripts to wait for manual intervention.
- Supports querying tasks by name, status, and creation time.
- Supports uploading scripts by using .tar packages.

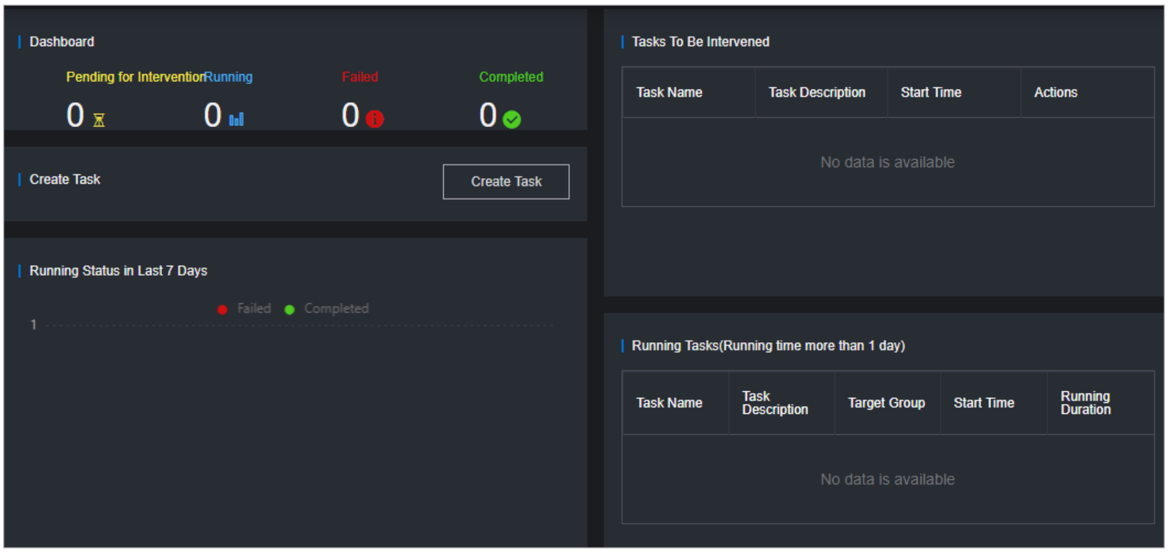
6.5.2. View task overview

The Task Overview page shows the overall running conditions of tasks in the system. You can also create a task on this page.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Task Management > Overview**.

   The **Task Overview** page appears.



Task Name	Task Description	Start Time	Actions
No data is available			

Task Name	Task Description	Target Group	Start Time	Running Duration
No data is available				

4. Perform the following operations:
   - In the **Dashboard** section, view the number of tasks that are in the **Pending for Intervention**, **Running**, **Failed**, or **Completed** state.

     Click a state or number to view the tasks of the corresponding state.
   - In the **Create Task** section, click **Create Task** to create an operations task.

     For more information about how to create a task, see Create a task.
   - If a task has a breakpoint and reaches the breakpoint, the task stops and waits for manual confirmation to proceed. You can view and process tasks that require manual intervention in the **Tasks To Be Intervened** section.
   - In the **Running Status in Last 7 Days** section, view the run trend and success information of tasks within the last seven days.

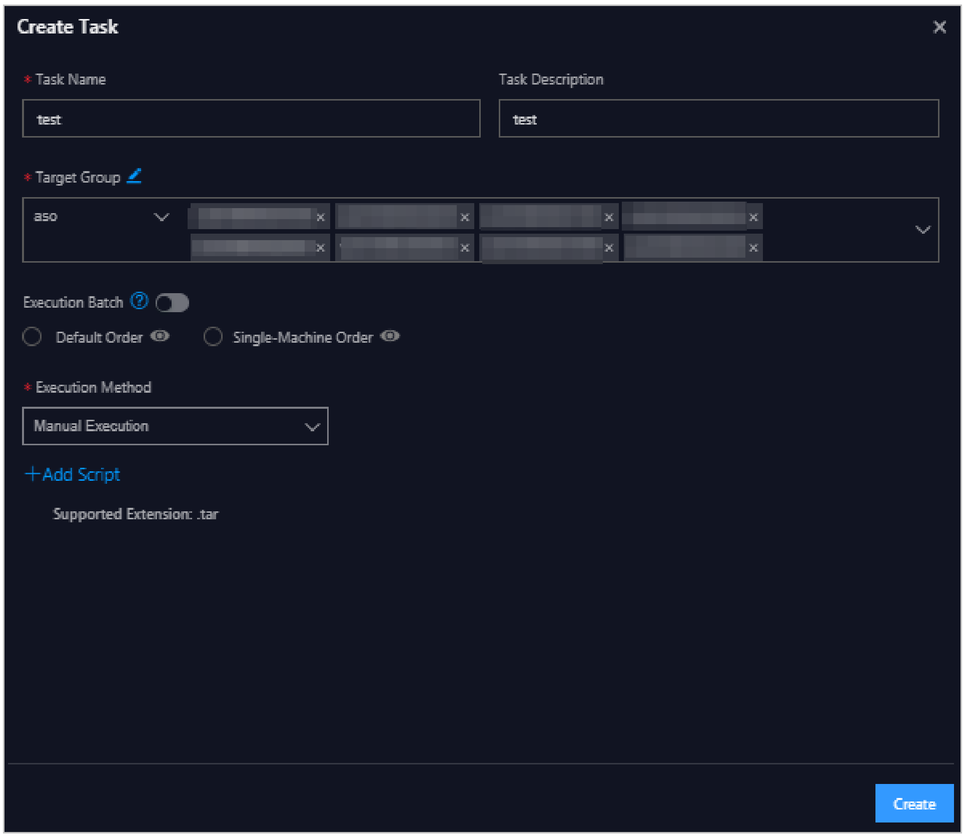
- In the **Running Tasks (Running time more than 1 day)** section, view the running status of tasks within the last 24 hours.

6.5.3. Create a task

You can make regular modifications as tasks to run in the ASO console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Task Management > Tasks**.
4. Click **Create**.
5. In the dialog box that appears, configure the parameters.



Create Task

* Task Name: test

Task Description: test

* Target Group: aso [redacted]

Execution Batch

○ Default Order ○ Single-Machine Order

* Execution Method: Manual Execution

+Add Script

Supported Extension: .tar

Parameter	Description
Task Name	The name of the O&M task.
Task Description	The description of the O&M task.

Parameter	Description
Target Group	The task target. You can use one of the following methods to configure the target group: ◦ Select a product, enter a VM or physical machine name in the field and press the Enter key. Multiple VMs or physical machines can be specified in sequence. ◦ Click the ✎ icon next to **Target Group**. In the dialog box that appears, specify the target group, with one VM or physical machine in each line. Click **OK**.
Execution Batch	Optional. This option appears after you specify the target group. If **Execution Batch** is not specified, **Target Group** is displayed in the **Target Group** column, which can be viewed by choosing **Task Management > Tasks**. If you specify **Execution Batch**, **Batch Execution Policy** is displayed in the **Target Group** column. You can set **Execution Batch** to one of the following values: ◦ **Default Order** By default, if the number of machines is less than or equal to 10, the machines are allocated to different batches, with one machine in batch 1, one machine in batch 2, two machines in batch 3, three machines in batch 4, and the remaining machines in batch 5. You can adjust the batch for machines based on your needs. By default, if the number of machines is greater than 10, the machines are allocated to different batches, with one machine in batch 1, three machines in batch 2, five machines in batch 3, N/3-1 (an integer) machines in batch 4, N/3-1 (an integer) machines in batch 5. You can adjust the batch for machines based on your needs. ◦ **Single-Machine Order**: By default, each batch has one machine. You can adjust the batch for machines based on your actual needs.

Parameter	Description
Execution Method	If **Execution Batch** is specified, **Execution Method** can be set only to **Manual Execution**. If **Execution Batch** is not specified, you can select one of the following execution methods: ○ **Manual Execution**: Start the task manually. With **Manual Execution** specified, you must click **Start** in the **Actions** column to run the task after the task is created. ○ **Scheduled Execution**: Select the execution time. The task automatically starts when the execution time is reached. ○ **Regular Execution**: Select the time interval and times to run the task. If the execution condition is met, the task starts again. ○ **Advanced**: Configure the command to run the task periodically.
Add Script	Click **Add Script**. Select one or more .tar packages to upload the script file. After you upload a script, you can delete and re-upload the script. After you upload a script, if **Execution Method** is set to **Manual Execution**, you must specify whether to enable **Intervention Required**. If manual intervention is enabled, when you run the script, the task is suspended and waits for manual intervention.

6. Click **Create**.

Result

The created task is displayed in the task list.

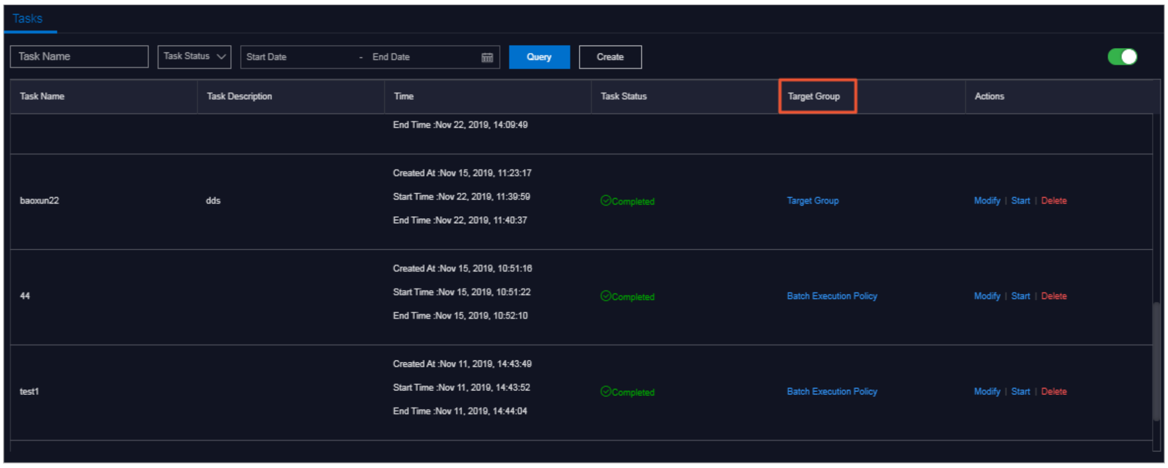
6.5.4. View the execution status of a task

After a task starts, you can view its execution status.

Procedure

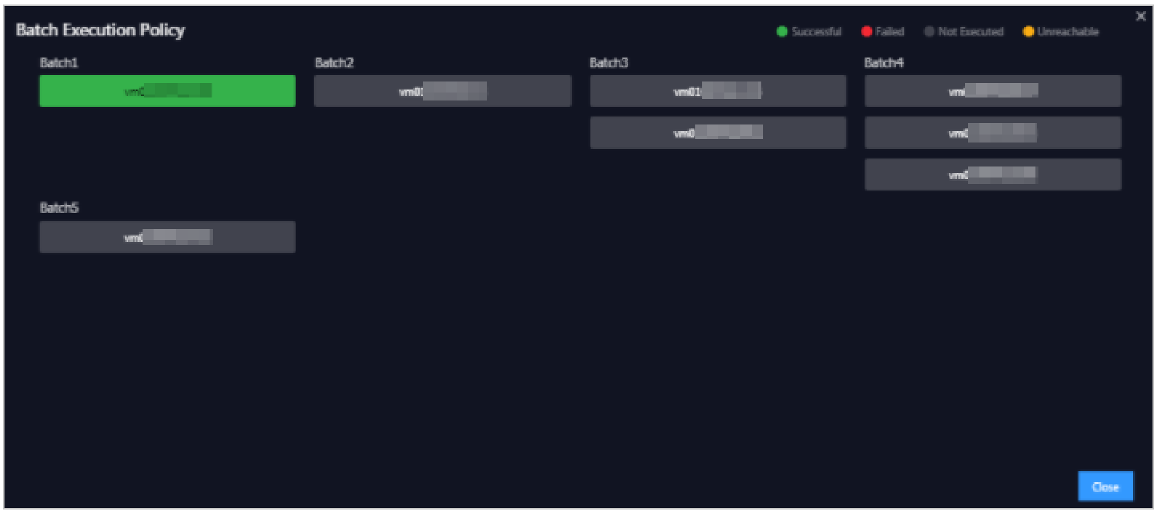
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Task Management > Tasks**.
4. (Optional)Enter the task name, select the task status, start date, and end date, and then click **Query** to search for tasks.
5. Find the task that you want to view and click **Target Group** or **Batch Execution Policy** in the **Target Group** column.

> ⓘ **Note** If **Execution Batch** is not selected when you create a task, **Target Group** is displayed in the **Target Group** column. If you select **Execution Batch** when you create a task, **Batch Execution Policy** is displayed in the **Target Group** column.



Task Name	Task Description	Time	Task Status	Target Group	Actions
		End Time :Nov 22, 2019, 14:09:49			
baoxun22	dds	Created At :Nov 15, 2019, 11:23:17 Start Time :Nov 22, 2019, 11:39:59 End Time :Nov 22, 2019, 11:40:37	Completed	Target Group	Modify | Start | Delete
44		Created At :Nov 15, 2019, 10:51:16 Start Time :Nov 15, 2019, 10:51:22 End Time :Nov 15, 2019, 10:52:10	Completed	Batch Execution Policy	Modify | Start | Delete
test1		Created At :Nov 11, 2019, 14:43:49 Start Time :Nov 11, 2019, 14:43:52 End Time :Nov 11, 2019, 14:44:04	Completed	Batch Execution Policy	Modify | Start | Delete

6. In the dialog box that appears, view the task execution status based on the machine color. Click a machine to view the execution results of the task.



6.5.5. Start a task

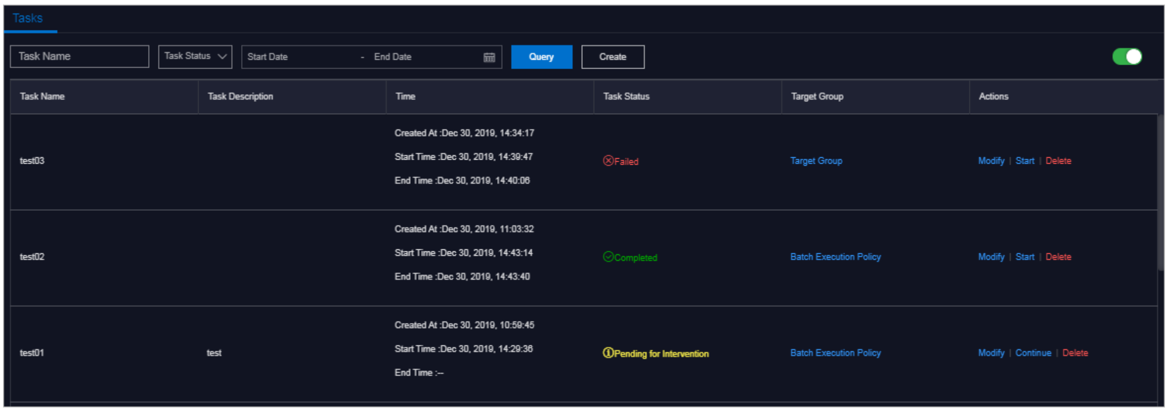
If you select **Manual Execution** when you create a task, you must manually start the task after it is created.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Task Management > Tasks**.
4. (Optional)On the Tasks page, enter the task name, select the task status, start date, and end date, and then click **Query**.
5. Find the task that you want to start and click **Start** in the **Actions** column.
6. In the dialog box that appears, select the batches to start and click **Start**.

   For a new task, after you click **Start** for the first time, the system indicates that the task is started. The virtual machines (VMs) or physical machines in batch 1 start to run the task. Click **Start** again and you can select VMs or physical machines in one or more batches to run the task.

If the task has enabled Intervention Required, you must intervene the script after you click **Start**. The **Task Status** turns to **Pending for Intervention**, and the task can only be resumed by clicking **Continue** in the **Actions** column.



Task Name	Task Description	Time	Task Status	Target Group	Actions
test03		Created At :Dec 30, 2019, 14:34:17 Start Time :Dec 30, 2019, 14:39:47 End Time :Dec 30, 2019, 14:40:06	⊗Failed	Target Group	Modify | Start | Delete
test02		Created At :Dec 30, 2019, 11:03:32 Start Time :Dec 30, 2019, 14:43:14 End Time :Dec 30, 2019, 14:43:40	✓Completed	Batch Execution Policy	Modify | Start | Delete
test01	test	Created At :Dec 30, 2019, 10:59:45 Start Time :Dec 30, 2019, 14:29:36 End Time :--	ⓘPending for Intervention	Batch Execution Policy	Modify | Continue | Delete

6.5.6. Delete a task

You can delete tasks that are no longer needed.

Procedure

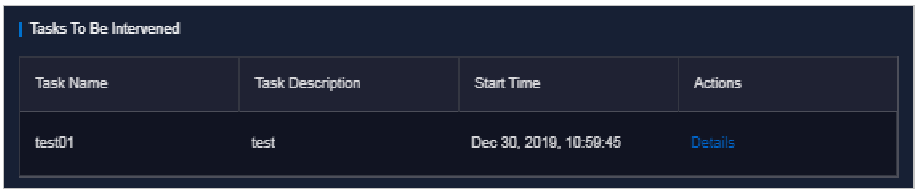
1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Task Management > Tasks**.
4. (Optional)Enter the task name, select the task status, start date, and end date, and then click **Query** to search for tasks.
5. Find the task that you want to delete and click **Delete** in the **Actions** column.
6. In the message that appears, click **OK**.

6.5.7. Process tasks to be intervened

If a task reaches a breakpoint, the task stops and waits for manual confirmation. The task proceeds only after receiving manual confirmation.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Task Management > Overview**.
4. In the **Task To Be Intervened** section, find the task to be intervened and click **Details** in the **Actions** column.



Task Name	Task Description	Start Time	Actions
test01	test	Dec 30, 2019, 10:59:45	Details

5. On the **Task Details** tab, check the information and click **Continue** for the task to continue.

6.6. Apsara Infrastructure Management Framework O&M

6.6.1. Old console

6.6.1.1. What is Apsara Infrastructure Management Framework?

This topic describes what Apsara Infrastructure Management Framework is from the aspects of core functions and basic concepts.

6.6.1.1.1. Overview

Apsara Infrastructure Management Framework is a distributed data center management system, which manages applications on clusters containing multiple machines and provides the basic functions such as deployment, upgrade, expansion, contraction, and configuration changes.

Apsara Infrastructure Management Framework also supports monitoring data and analyzing reports, which facilitates users to perform one-stop Operation & Maintenance (O&M) control. Based on the Apsara Infrastructure Management Framework services, automated O&M is implemented in the large-scale distributed environment, which greatly improves the operations efficiency and enhances the system availability.

Apsara Infrastructure Management Framework is mainly composed of TianjiMaster and TianjiClient. Apsara Infrastructure Management Framework installs TianjiClient as the agent on machines it manages. Then, TianjiMaster accepts and issues the upper-layer instructions to TianjiClient for execution. In the upper layer, Apsara Infrastructure Management Framework is divided into different components based on different functions, and then provides API server and portal for external use.

Core functions

- Network initialization in data centers
- Server installation and maintenance process management
- Deployment, expansion, and upgrade of cloud products
- Configuration management of cloud products
- Automatic application for cloud product resources
- Automatic repair of software and hardware faults
- Basic monitoring and business monitoring of software and hardware

6.6.1.1.2. Basic concepts

Before using Apsara Infrastructure Management Framework, you must know the following basic concepts for a better understanding.

project

A collection of clusters, which provides service capabilities for external entities.

cluster

A collection of physical machines, which logically provides services and is used to deploy project software.

- A cluster can only belong to one project.
- Multiple services can be deployed on a cluster.

service

A set of software, which provides relatively independent functions. A service is composed of one or more server roles and can be deployed on multiple clusters to form multiple sets of services and provide the corresponding service capabilities. For example, Apsara Distributed File System, Job Scheduler, and Apsara Name Service and Distributed Lock Synchronization System are all services.

service instance

A service that is deployed on a cluster.

server role

One or more indivisible deployment units into which a service can be divided based on functions. A server role is composed of one or more specific applications. If a service is deployed on a cluster, all the server roles of the service must be deployed to machines of this cluster. Multiple server roles, such as PanguMaster and TianjiClient, can be deployed on the same server.

server role instance

A server role that is deployed on a machine. A server role can be deployed on multiple machines.

application

Applications correspond to each process-level service component in a server role and each application works independently. The application is the minimum unit for deployment and upgrade in Apsara Infrastructure Management Framework, and can be deployed to each machine. Generally, an application is an executable software or Docker container.

If a server role is deployed on a machine, all applications in the server role must be deployed to this machine.

rolling

Each time when a user updates configurations, Apsara Infrastructure Management Framework upgrades services and modifies the cluster configurations based on the updated configurations. This process is called rolling.

service configuration template

Some configurations are the same when services are deployed on clusters. A service configuration template can be created to quickly write the same configurations to different clusters. The service configuration template is basically used for large-scale deployment and upgrade.

associated service template

A *template.conf* file that exists in the configurations. This file declares the service configuration template and its version, of which the configuration is used by the service instance.

final status

If a cluster is in this status, all hardware and software on each of its machines are normal and all software are in the target version.

dependency

The dependency between server roles in a service defines that server roles with dependencies run tasks or are upgraded based on the dependency order. For example, if A depends on B, B is upgraded first. A starts to be downloaded after B is downloaded successfully, and upgraded after B is successfully upgraded. (By default, the dependency does not take effect for configuration upgrade.)

upgrade

A way of aligning the current status with the final status of a service. After a user submits the version change, Apsara Infrastructure Management Framework upgrades the service version to the target version. With the server role as the processing unit, upgrade aims to update the versions of all machines to the target version.

At the beginning, the final status and current status of the cluster are the same. When a user submits the change, the final status is changed, whereas the current status is not. A rolling task is generated and has the final status as the target version. During the upgrade, the current status is continuously approximating to the final status. Finally, the final status and the current status are the same when the upgrade is finished.

6.6.1.2. Log on to the Apsara Infrastructure Management Framework console

This topic describes how to log on to the Apsara Infrastructure Management Framework console.

Prerequisites

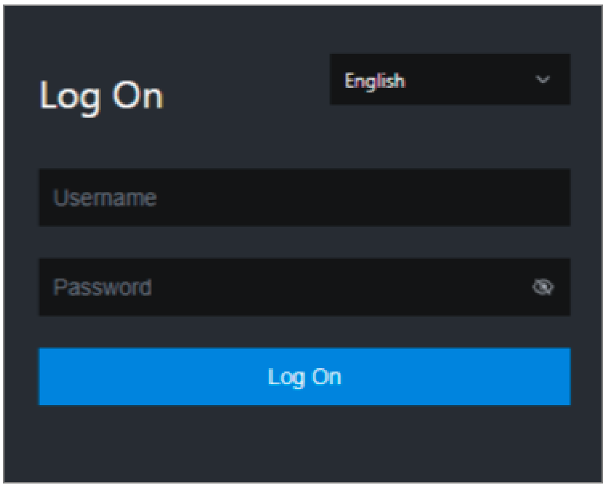
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.



> Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   > Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

   When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   For security reasons, your password must meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password must be 10 to 20 characters in length.
4. Click **Log On**.
5. In the top navigation bar, click **O&M**.
6. In the left-side navigation pane, choose **Product Management** > **Products**.
7. In the **Apsara Stack O&M** section, choose **Basic O&M** > **Apsara Infrastructure Management Framework**.

6.6.1.3. Web page introduction

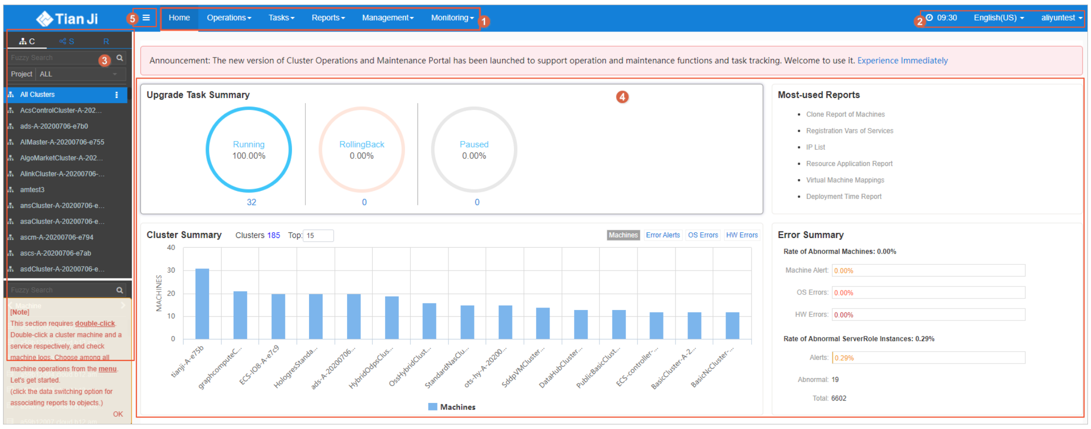
Before performing Operation & Maintenance (O&M) operations on Apsara Infrastructure Management Framework, you must have a general understanding of the Apsara Infrastructure Management Framework page.

6.6.1.3.1. Instructions for the homepage

After you log on to the Apsara Infrastructure Management Framework console, the homepage appears. This topic describes the basic operations and functions on the homepage.

Log on to Apsara Infrastructure Management Framework. The homepage appears, as shown in Homepage of the Apsara Infrastructure Management Framework console.

Homepage of the Apsara Infrastructure Management Framework console



Announcement: The new version of Cluster Operations and Maintenance Portal has been launched to support operation and maintenance functions and task tracking. Welcome to use it. Experience Immediately

[Note]
This section requires double-click. Double-click a cluster machine and a service respectively, and check machine logs. Choose among all machine operations from the menu. Let's get started.
(click the data switching option for associating reports to objects.)

Rate of Abnormal Machines: 0.00%

Machine Alert: 0.00%

OS Errors: 0.00%

HW Errors: 0.00%

Rate of Abnormal ServerRole Instances: 0.29%

Alerts: 0.29%

Abnormal: 19

Total: 6602

Description of functional sections describes the functional sections on the homepage.

Description of functional sections

Section		Description
①	Top navigation bar	• **Operations**: the quick entrance to operations and maintenance (O&M) operations and their objects. This menu consists of the following submenus: ○ **Cluster Operations**: allows you to use the project permissions to perform O&M and management operations on clusters. For example, you can view the cluster status. ○ **Service Operations**: allows you to use the service permissions to manage services. For example, you can view the service list. ○ **Machine Operations**: allows you to perform O&M and management operations on machines. For example, you can view the machine status. • **Tasks**: Rolling tasks are generated when you modify the configurations in the system. This menu allows you to view the running tasks, task history, and deployment of clusters, services, and server roles in all projects. • **Reports**: allows you to view monitoring data in tables and find specific reports by using fuzzy search. • **Monitoring**: monitors metrics during system operations and sends alert notifications for abnormal conditions. This menu allows you to view the alert status, modify alert rules, and search alert history.

Section		Description
②	Upper-right buttons	• 🕘: ○ **TJDB Synchronization Time**: the time when the data on the current page is generated. ○ **Final Status Computing Time**: the time when the desired-state data on the current page is calculated. The system processes data as fast as it can after the data is generated. Latency exists because Apsara Infrastructure Management Framework is an asynchronous system. Time information helps explain why data on the current page is generated and determine whether the system experiences an error. • English(US) ▾: the current display language of the console. You can select another language from the drop-down list. • aliyuntest ▾: your logon account. You can select **Logout** from the drop-down list to log out of your account.
③	Left-side navigation pane	In the left-side navigation pane, you can view the logical architecture of Apsara Infrastructure Management Framework. The tabs allow you to view details and perform operations. For more information, see Introduction on the left-side navigation pane.
④	Workspace	The workspace shows a summary of tasks and other information. • **Upgrade Task Summary**: shows the numbers and proportions of running, rolling back, and suspended upgrade tasks. • **Cluster Summary**: shows the numbers of machines, error alerts, operating system errors, and hardware errors in each cluster. • **Error Summary**: shows metric values about the rate of abnormal machines and the rate of abnormal server role instances. • **Most-used Reports**: shows links of common statistical reports.
⑤	Show/hide button	If you do not need to use the left-side navigation pane, click this button to hide the pane and enlarge the workspace.

6.6.1.3.2. Instructions for the left-side navigation pane

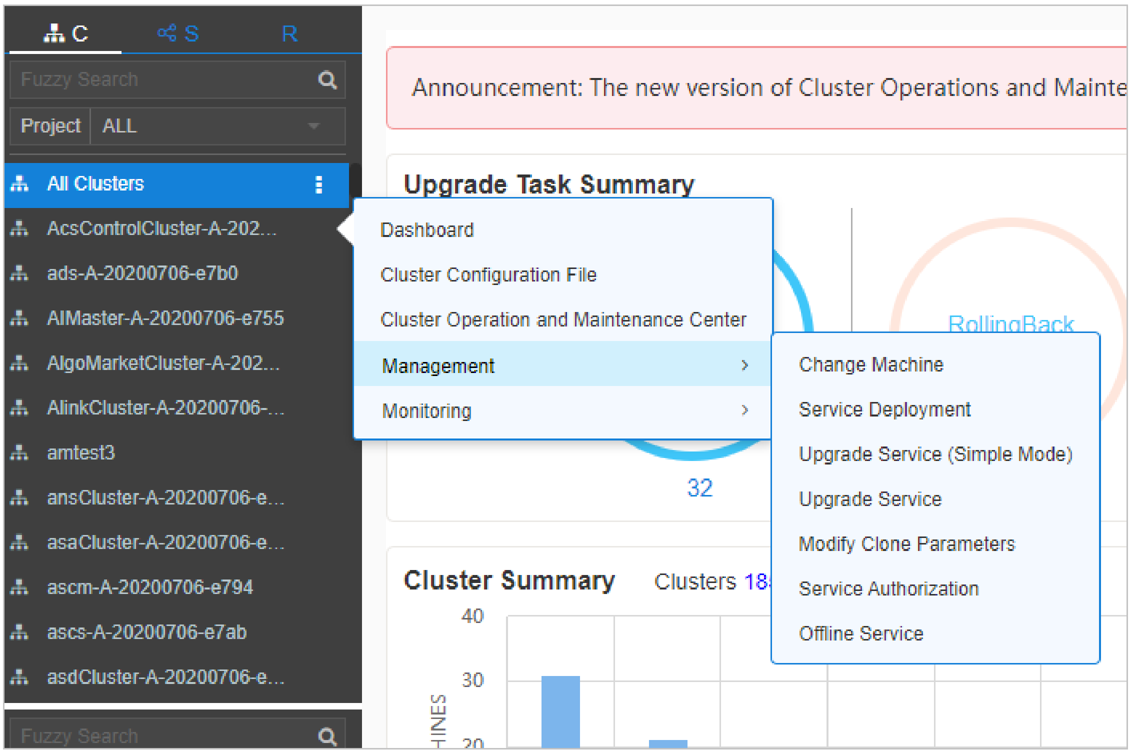
The left-side navigation pane contains three tabs: **C** (cluster), **S** (service), and **R** (report). This topic describes how to use the tabs to view information.

Cluster

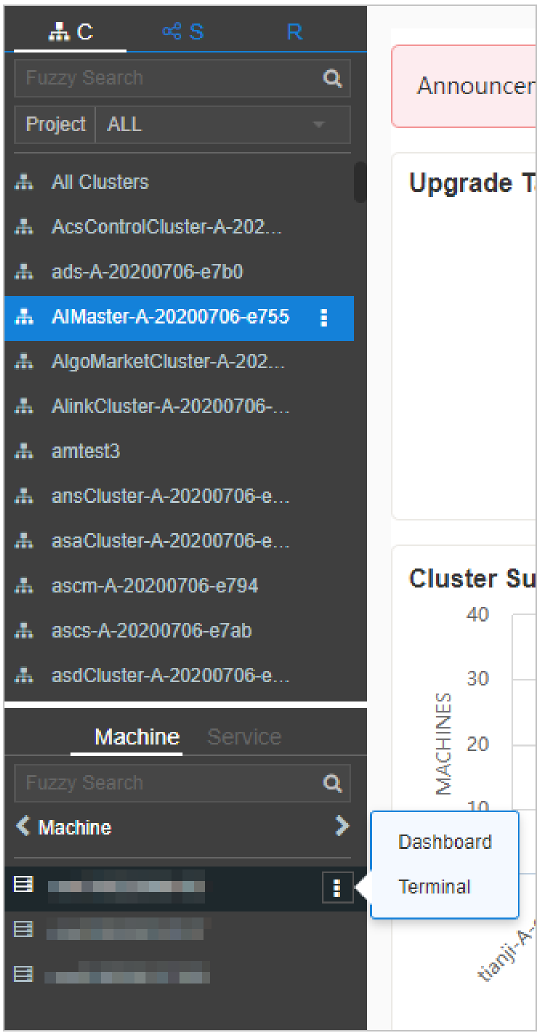
You can search for clusters in a project and their information such as the cluster status, cluster operations and maintenance (O&M), service desired state, and logs by fuzzy match.

On the **C** tab of the left-side navigation pane, you can perform the following operations:

- Enter a cluster name or a part of a cluster name in the search box to filter clusters.
- Select a project from the **Project** drop-down list to view all clusters in the project.
- Move the pointer over the ⋮ icon next to a cluster and select menu items to perform corresponding operations on the cluster.



- Click a cluster. All machines and services within the cluster are displayed in the lower part of the left-side navigation pane. Move the pointer over the ⋮ icon next to a machine or service on the **Machine** or **Service** tab and select menu items to perform corresponding operations on the machine or service.



- Click the **Machine** tab. Double-click a machine to view information about all server roles on the machine. Double-click a server role to view applications, and then double-click an application to view log files.
- Click the **Service** tab. Double-click a machine to view information about all server roles on the machine. Double-click a server role to view machines, double-click a machine to view applications, and then double-click an application to view log files.
- Double-click a log file. Move the pointer over the log file, click the ⋮ icon next to the log file, and then click **Download** to download the log file.

  Alternatively, move the pointer over a log file and click **View** next to the log file. The time-ordered log details are displayed on the **Log Viewer** page. You can search for log details by keyword.

Service

You can search for services and view information about services and service instances by fuzzy match.

On the S tab of the left-side navigation pane, you can perform the following operations:

- Enter a service name or a part of a service name in the search box to filter services.
- Move the pointer over the ⋮ icon next to a service and select menu items to perform corresponding operations on the service.

- Click a service. All service instances within the service are displayed in the lower part of the left-side navigation pane. Move the pointer over the ⋮ icon next to a service instance and select menu items to perform corresponding operations on the service instance.

Report

You can search for reports by fuzzy match and view report details.

On the **R** tab of the left-side navigation pane, you can perform the following operations:

- Enter a report name or a part of a report name in the search box to filter reports.
- Click **All Reports** or **Favorites**. Corresponding groups are displayed in the lower part of the left-side navigation pane. Double-click a group to view all reports in the group. Double-click a report to view details of the report.

6.6.1.4. Cluster operations

This topic describes the actions about cluster operations.

6.6.1.4.1. View configuration information of a cluster

This topic describes how to view the basic information, deployment plan, and configuration information of a cluster.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Operations > Cluster Operations**.The **Cluster Operations** page contains the following information:
    - Cluster

      The name of a cluster. Click a cluster name to go to the Cluster Dashboard page. For more information, see View dashboard information of a cluster.
    - Scale-Out/Scale-In

      The numbers of machines and server roles that are scaled in and out. Click a number to go to the Cluster Operation and Maintenance Center page. For more information, see View information of the cluster O&M center.
    - Abnormal Machine Count

      The number of machines that are not in the Good state within a cluster. Click the number to go to the Cluster Operation and Maintenance Center page. For more information, see View information of the cluster O&M center.
    - Final Status of Normal Machines

      Specifies whether a cluster has reached the desired state. Select **Clusters not Final** above the cluster list to view all clusters that have not reached the desired state. Click a link in the column to view desired state information. For more information, see View the desired state of a service.
    - Rolling

Specifies whether rolling tasks are running within a cluster. Select **Rolling Tasks** above the cluster list to view all clusters that have rolling tasks. Click rolling in the column to view rolling tasks. For more information see View rolling tasks.

3. (Optional)Select a project from the drop-down list or enter a cluster name to search for the cluster.
4. Click the cluster name or click **Cluster Configuration** in the **Actions** column to go to the **Cluster Configuration** page.

   Cluster configuration description describes the parameters on the **Cluster Configuration** page.

   Cluster configuration description

Section	Parameter	Description
Basic Information	**Cluster**	The name of the cluster.
	Project	The project to which the cluster belongs.
	Clone Switch	○ **Pseudo-clone**: The system is not cloned when a machine is added to the cluster. ○ **Real Clone**: The system is cloned when a machine is added to the cluster.
	Machines	The number of machines included in the cluster. Click View Clustering Machines to view the list of machines.
	Security Verification	The access control among processes. By default, security verification is disabled in non-production environments. You can enable or disable security verification based on your business requirements.
	Cluster Type	○ RDS ○ NETFRAME ○ T4: a type of cluster that renders special configurations for the mixed deployment of e-commerce ○ Default
Deployment Plan	**Service**	The service that is deployed within the cluster.
	Dependency Service	The service on which the current service depends.
	Service Information	The service that you want to view. Select a service from the drop-down list to view its configuration information.
	Service Template	The template that is used by the service.

Section	Parameter	Description
Service Information	**Monitoring Template**	The monitoring template that is used by the service.
	Machine Mappings	The machines where server roles of the service are deployed.
	Software Version	The version of the software that is included in server roles of the service.
	Availability Configuration	The percentage of availability configuration for server roles of the service.
	Deployment Plan	The deployment plan of server roles of the service.
	Configuration Information	The configuration file that is used for the service.
	Role Attribute	The server roles and their parameter information.

5. Click **Operation Logs** in the upper-right corner to view version differences. For more information about operation logs, see View operation logs.

6.6.1.4.2. View dashboard information of a cluster

This topic describes how to view the basic information and related statistics of a cluster.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Use one of the following methods to go to the **Cluster Dashboard** page:
   - In the left-side navigation pane, click the **C** tab. Move the pointer over the i icon next to the target cluster and select **Dashboard**.
   - In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, click the name of the target cluster.
3. View all information about the cluster on the **Cluster Dashboard** page. The following table describes the information that you can view, such as basic information, desired state information, rolling tasks, dependencies, resources, virtual machine (VM) mappings, and monitoring status.

Parameter	Description

Parameter	Description
Basic Cluster Information	The basic information about the cluster. ○ **Project Name**: the name of the project. ○ **Cluster Name**: the name of the cluster. ○ **IDC**: the data center to which the cluster belongs. ○ **Final Status Version**: the latest version of the cluster. ○ **Cluster in Final Status**: specifies whether the cluster has reached the desired state. ○ **Machines Not In Final Status**: the number of machines that have not reached the desired state. ○ **Real/Pseudo Clone**: specifies whether the system is cloned when a machine is added to the cluster. ○ **Expected Machines**: the number of machines that are expected within the cluster. ○ **Actual Machines**: the number of machines that are deployed in the current environment. ○ **Machines Not Good**: the number of machines that are not in the Good state within the cluster. ○ **Actual Services**: the number of services that are deployed within the cluster. ○ **Actual Server Roles**: the number of server roles that are deployed within the cluster. ○ **Cluster Status**: specifies whether the cluster is starting or shutting down machines.
Machine Status Overview	The status of machines within the cluster.
Machines In Final State	The distribution of machines where services are deployed, based on whether the machines have reached the desired state.
Load-System	The statistics chart of the cluster system load.
CPU-System	The statistics chart of the CPU load.
Mem-System	The statistics chart of the memory load.
Disk_Usage-System	The statistics chart of the disk usage.
Traffic-System	The statistics chart of the system traffic.
TCP State-System	The statistics chart of the CPU request status.
TCP Retrans-System	The statistics chart of the CPU retransmission traffic.
Disk_IO-System	The statistics chart of the disk I/O information.

Parameter	Description
Service Instances	The service instances that are deployed within the cluster and their desired state information. ○ **Service Instance**: the service instance that is deployed within the cluster. ○ **Final Status**: specifies whether the service instance has reached the desired state. ○ **Expected Server Roles**: the number of server roles that are expected to deploy in the service instance. ○ **Server Roles in Final Status**: the number of server roles that have reached the desired state in the service instance. ○ **Server Roles Going Offline**: the number of server roles that are being unpublished from the service instance. ○ Actions: Click **Details** to go to the **Service Instance Information Dashboard** page. For more information about the service instance dashboard, see View the service instance dashboard.
Upgrade Tasks	The upgrade tasks within the cluster. ○ **Cluster Name**: the name of the cluster. ○ **Type**: the type of the upgrade task. Valid values: app and config. app indicates version upgrade, and config indicates configuration change. ○ **Git Version**: the change version of the upgrade task. ○ **Description**: the description of the change. ○ **Rolling Result**: the result of the upgrade task. ○ **Submitted By**: the user who submits the change. ○ **Submitted At**: the time when the change is submitted. ○ **Start Time**: the time when rolling starts. ○ **End Time**: the time when the upgrade task ends. ○ **Time Used**: the time consumed for the upgrade. ○ Actions: Click **Details** to go to the **Rolling Task** page. For more information about rolling tasks, see View rolling tasks.
Cluster Resource Request Status	○ **Version**: the version of the resource request. ○ **Msg**: the error message. ○ **Begintime**: the time when the resource request analysis starts. ○ **Endtime**: the time when the resource request analysis ends. ○ **Build Status**: the build status of resources. ○ **Resource Process Status**: the resource request status of the version.

Parameter	Description
Cluster Resource	○ **Service**: the name of the service. ○ **Service Role**: the name of the server role. ○ **App**: the name of the application of the server role. ○ **Name**: the name of the resource. ○ **Type**: the type of the resource. ○ **Status**: the status of the resource request. ○ **Error_Msg**: the error message. ○ **Parameters**: the parameters of the resource. ○ **Result**: the result of the resource request. ○ **Res**: the ID of the resource. ○ **Reprocess Status**: the request status of AnyTunnel VIP addresses. ○ **Reprocess Msg**: the error message reported when AnyTunnel VIP addresses are requested. ○ **Reprocess Result**: the request result of AnyTunnel VIP addresses. ○ **Refer Version List**: the version that uses the resource.
VM Mappings	The VMs within the cluster. VM information is displayed only when VMs are deployed within the cluster. ○ **VM**: the hostname of the VM. ○ **Currently Deployed On**: the hostname of the physical machine where the VM is deployed. ○ **Target Deployed On**: the hostname of the physical machine where you expect to deploy the VM.
Service Dependencies	The dependency configuration of service instances and server roles within the cluster, and the desired state information of dependency services or server roles. ○ **Service**: the name of the service. ○ **Server Role**: the name of the server role. ○ **Dependent Service**: the service on which the server role depends. ○ **Dependent Server Role**: the server role on which the server role depends. ○ **Dependent Cluster**: the cluster where the dependency server role is deployed. ○ **Dependency in Final Status**: specifies whether the dependency server role has reached the desired state.

6.6.1.4.3. View information of the cluster O&M center

This topic describes how to view the status and statistics of services and machines within a cluster.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Use one of the following methods to go to the **Cluster Operation and Maintenance Center** page:
   - In the left-side navigation pane, click the **C** tab. Move the pointer over the ⋮ icon next to the target cluster and select **Cluster Operation and Maintenance Center**.
   - In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find the target cluster and choose **Monitoring > Cluster Operation and Maintenance Center** in the Actions column.
   - In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, click the name of the target cluster. On the **Cluster Dashboard** page, choose **Operations Menu > Cluster Operation and Maintenance Center**.
3. View information on the **Cluster Operation and Maintenance Center** page.

Parameter	Description
SR not in Final Status	All server roles that have not reached the desired state within the cluster. Click the number to view the list of server roles. Click a server role to view information of machines where the server role is deployed.
Running Tasks	Specifies whether rolling tasks are running within the cluster. Click **Rolling** to go to the **Rolling Task** page. For more information about rolling tasks, see View rolling tasks.
Head Version Submitted At	The time when the HEAD version is submitted. Click the time to view details.
Head Version Analysis	The status of desired state analysis. During desired state analysis, Apsara Infrastructure Management Framework detects the latest cluster version and parses the version to specific change contents. Desired state analysis can be in one of the following states: ◦ **Preparing**: No new version is detected. ◦ **Waiting**: The latest version has been detected, but the analysis module has not started. ◦ **Doing**: The application to be changed is being analyzed. ◦ **done**: The desired state analysis succeeds. ◦ **Failed**: The desired state analysis fails to parse change contents. Apsara Infrastructure Management Framework can obtain change contents of server roles in the latest version only when the desired state analysis is in the **done** state. Click a state to view related information.
Service	The service deployed within the cluster. Select a service from the drop-down list.

Parameter	Description
Server Role	The server role of a service within the cluster. Select a server role from the drop-down list. **Note** After you select a service and a server role, machines that are related to the service or the server role are displayed.
Total Machines	The total number of machines within the cluster or machines where the selected server roles are deployed.
Scale-in Scale-out	The numbers of machines and server roles that are scaled in and out.
Abnormal Machines	The numbers of machines in an abnormal state for the following reasons: ○ **Ping Failed**: the number of machines that experience ping_monitor errors because TianjiMaster cannot ping the machines. ○ **No Heartbeat**: the number of machines that experience TianjiClient or network errors because TianjiClient does not report data on a regular basis. ○ **Status Error**: the number of machines that experience critical or fatal errors. Resolve problems based on alert information.
Abnormal Services	The number of machines that have abnormal services. The following rules are used to check whether a service has reached the desired state: ○ Each server role on the machine is in the GOOD state. ○ The actual version of each application of each server role on the machine is consistent with the HEAD version. ○ Before the Image Builder builds an application of the HEAD version, Apsara Infrastructure Management Framework cannot obtain the value of the HEAD version, and the desired state of the service is unknown. This process is called change preparation. The desired state of the service cannot be obtained when the preparation process is in progress or if the preparation fails.

Parameter	Description
Machines	All machines within the cluster or machines where the selected server roles are deployed. ○ Click the Machine Search search box. In the dialog box that appears, enter one or more machines. Fuzzy match and batch search are supported. ○ Click the name of a machine to view its physical information in the Machine Information dialog box. Click **DashBoard** to go to the **Machine Details** page. For more information about machine details, see View the machine dashboard. ○ Move the pointer over the **Final Status** or **Final SR Status** column and click **Details** to view the machine status and system service information, as well as status information and error messages of server roles on the machine. ○ Before you filter machines by service and service role, move the pointer over the **Running Status** column and click **Details** to view status information and error messages of the machine. After you filter machines by service and service role, move the pointer over the **SR Running Status** column and click **Details** to view status information and error messages of server roles on the machine. ○ Click **Error**, **Warning**, or **Good** in the **Monitoring Statistics** column to view machine and server role metrics. ○ Click **Terminal** in the **Actions** column to log on to the machine and perform operations. ○ Click **Machine Operation** in the **Actions** column to perform reboot, out-of-band reboot, or reclone operations on the machine.

6.6.1.4.4. View the desired state of a service

This topic describes how to check whether a service within a cluster has reached the desired state and how to view desired state details.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Use one of the following methods to go to the **Service Final Status Query** page:
   - In the left-side navigation pane, click the **C** tab. Move the pointer over the ℹ icon next to the target cluster and choose **Monitoring > Service Final Status Query**.
   - In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find the target cluster and choose **Monitoring > Service Final Status Query** in the Actions column.
3. View information on the **Service Final Status Query** page.

Parameter	Description
Project Name	The project to which the cluster belongs.

Parameter	Description
Cluster Name	The name of the cluster.
Head Version Submitted At	The time when the HEAD version is submitted.
Head Version Analysis	The status of desired state analysis. During desired state analysis, Apsara Infrastructure Management Framework detects the latest cluster version and parses the version to specific change contents. Desired state analysis can be in one of the following states: ○ **Preparing**: No new version is detected. ○ **Waiting**: The latest version has been detected, but the analysis module has not started. ○ **Doing**: The application to be changed is being analyzed. ○ **done**: The desired state analysis succeeds. ○ **Failed**: The desired state analysis fails to parse change contents. Apsara Infrastructure Management Framework can obtain change contents of server roles in the latest version only when the desired state analysis is in the **done** state.
Cluster Rolling Status	Specifies whether the cluster has reached the desired state. If a rolling task is running, its task information is displayed.
Cluster Machine Final Status Statistics	The status of all machines within the cluster. Click **View Details** to go to the **Cluster Operation and Maintenance Center** page and view machine details. For more information about the operations and maintenance (O&M) center, see View the cluster operation and maintenance center.
Final Status of Cluster SR Version	The desired state of services within the cluster. **Note** This section includes only the services that have not reached the desired state due to version inconsistency or status exceptions. For other services that fail to reach the desired state due to machine errors, see desired state information of machines within the cluster.
Final Status of SR Version	The number of machines that have not reached the desired state. The number is displayed if server roles have rolling tasks.

6.6.1.4.5. View operations logs

This topic describes how to view differences between Git versions from operation logs.

Procedure

1. Log on to Apsara Infrastructure Management Framework.

2. Use one of the following methods to go to the **Cluster Operation Logs** page:
   - In the left-side navigation pane, click the **C** tab. Move the pointer over the ⋮ icon next to the target cluster and choose **Monitoring > Operation Logs**.
   - In the top navigation bar, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find the target cluster and choose **Monitoring > Operation Logs** in the Actions column.
3. On the **Cluster Operation Logs** page, click **Refresh** in the upper-right corner to view the Git version, description, submission information, and task status.
4. (Optional)On the **Cluster Operation Logs** page, view differences between versions.
   i. Find the target operation log and click **View Release Changes** in the **Actions** column.
   ii. On the **Version Difference** page, configure the following parameters:
      - **Select Base Version**: Select a basic version.
      - **Configuration Type**: Select **Extended Configuration** or **Cluster Configuration**. **Extended Configuration** allows you to view differences between the merging results of cluster and template configurations. **Cluster Configuration** allows you to view differences between cluster configurations.
   iii. Click **Obtain Difference**.

      Difference files are displayed.
   iv. Click each difference file to view its difference details.

6.6.1.5. Service operations

This topic describes the actions about service operations.

6.6.1.5.1. View the service list

The service list allows you to view the list of all services and the related information.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Operations > Service Operations**.
3. View the information on the **Service Operations** page.

Item	Description
Service	The service name.
Service Instances	The number of service instances in the service.
Service Configuration Templates	The number of service configuration templates.

Item	Description
Monitoring Templates	The number of monitoring templates.
Service Schemas	The number of service configuration validation templates.
Actions	Click **Management** to view the service instances, service templates, monitoring templates, monitoring instances, service schemas, and detection scripts.

6.6.1.5.2. View dashboard information of a service instance

This topic describes how to view the basic information and related statistics of a service instance.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the left-side navigation pane, click the **S** tab.
3. (Optional)Enter a service name in the search box to search for the service.
4. Click the service name to view service instances of the service.
5. Move the pointer over the ℹ icon next to the target service instance and select **Dashboard**.
6. View information on the **Service Instance Information Dashboard** page.

Parameter	Description

Parameter	Description
Service Instance Summary	The basic information about the service instance. ◦ **Cluster Name**: the name of the cluster where the service instance is deployed. ◦ **Service Name**: the name of the service to which the service instance belongs. ◦ **Actual Machines**: the number of machines that are deployed in the current environment. ◦ **Expected Machines**: the number of machines that are expected for the service instance. ◦ **Target Total Server Roles**: the number of server roles that are expected for the service instance. ◦ **Actual Server Roles**: the number of server roles that are deployed in the current environment. ◦ **Template Name**: the name of the service template that is used by the service instance. ◦ **Template Version**: the version of the service template that is used by the service instance. ◦ **Schema**: the name of the service schema that is used by the service instance. ◦ **Monitoring System Template**: the name of the Monitoring System template that is used by the service instance.
Server Role Statuses	The status of server roles in the service instance.
Machine Statuses for Server Roles	The status of machines where server roles are deployed.
Service Monitoring Information	◦ **Monitored Item**: the name of the metric. ◦ **Level**: the level of the metric. ◦ **Description**: the description of the metric. ◦ **Updated At**: the time when the data is updated.
Service Alert Status	◦ **Alert Name** ◦ **Instance Information** ◦ **Alert Start** ◦ **Alert End** ◦ **Alert Duration** ◦ **Severity Level** ◦ **Occurrences**: the number of occurrences of the alert.

Parameter	Description
Server Role List	○ **Server Role** ○ **Current Status** ○ **Expected Machines** ○ **Machines In Final Status** ○ **Machines Going Offline** ○ **Rolling Task Status** ○ **Time Used**: the time that is used for the execution of rolling tasks. ○ **Actions**: Click **Details** to go to the View the server role dashboard page.
Service Alert History	○ **Alert Name** ○ **Alert Time** ○ **Instance Information** ○ **Severity Level** ○ **Contact Group**
Service Dependencies	The dependency configuration of service instances and server roles, and the desired state information of dependency services or server roles. ○ **Server Role**: the name of the server role. ○ **Dependent Service**: the service on which the server role depends. ○ **Dependent Server Role**: the server role on which the server role depends. ○ **Dependent Cluster**: the cluster where the dependency server role is deployed. ○ **Dependency in Final Status**: specifies whether the dependency server role has reached the desired state.

6.6.1.5.3. View the server role dashboard

The server role dashboard allows you to view the statistics of a server role.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the left-side navigation pane, click the **S** tab.
3. (Optional)Enter the service name in the search box. Services that meet the search condition are displayed.
4. Click a service name and then service instances in the service are displayed in the lower-left corner.
5. Move the pointer over ℹ at the right of a service instance and then select **Dashboard**.
6. In the **Server Role List** section of the **Service Instance Information Dashboard** page, click **Details** in the **Actions** column.

7. View the information on the **Server Role Dashboard** page.

Item	Description
Server Role Summary	Displays the basic information of the server role as follows: ◦ **Project Name**: the name of the project to which the server role belongs. ◦ **Cluster Name**: the name of the cluster to which the server role belongs. ◦ **Service Instance**: the name of the service instance to which the server role belongs. ◦ **Server Role**: the server role name. ◦ **In Final Status**: whether the server role reaches the final status. ◦ **Expected Machines**: the number of expected machines. ◦ **Actual Machines**: the number of actual machines. ◦ **Machines Not Good**: the number of machines whose status is not Good. ◦ **Machines with Role Status Not Good**: the number of server roles whose status is not Good. ◦ **Machines Going Offline**: the number of machines that are going offline. ◦ **Rolling**: whether a running rolling task exists. ◦ **Rolling Task Status**: the current status of the rolling task. ◦ **Time Used**: the time used for running the rolling task.
Machine Final Status Overview	The statistical chart of the current status of the server role.
Server Role Monitoring Information	◦ **Updated At**: the time when the data is updated. ◦ **Monitored Item**: the name of the monitored item. ◦ **Level**: the level of the monitored item. ◦ **Description**: the description of the monitored item.

Item	Description
Machine Information	◦ **Machine Name**: the hostname of the machine. ◦ **IP**: the IP address of the machine. ◦ **Machine Status**: the machine status. ◦ **Machine Action**: the action that the machine is performing. ◦ **Server Role Status**: the status of the server role. ◦ **Server Role Action**: the action that the server role is performing. ◦ **Current Version**: the current version of the server role on the machine. ◦ **Target Version**: the expected version of the server role on the machine. ◦ **Error Message**: the exception message. ◦ **Actions**: ▪ Click **Terminal** to log on to the machine and perform operations. ▪ Click **Restart** to restart the server roles on the machine. ▪ Click **Details** to go to the **Machine Details** page. For more information about the machine details, see View the machine dashboard. ▪ Click **Machine System View** to go to the **Machine Info Report** page. For more information about the machine info report, see Machine info report. ▪ Click **Machine Operation** to restart, out of band restart, or clone the machine again.
Server Role Monitoring Information of Machines	◦ **Updated At**: the time when the data is updated. ◦ **Machine Name**: the machine name. ◦ **Monitored Item**: the name of the monitored item. ◦ **Level**: the level of the monitored item. ◦ **Description**: the description of the monitored item.
VM Mappings	The information of virtual machines in the cluster. Data is available only when virtual machines are deployed in the cluster. ◦ **VM**: the hostname of the virtual machine. ◦ **Currently Deployed On**: the hostname of the physical machine where the virtual machine is currently deployed. ◦ **Target Deployed On**: the hostname of the physical machine where the virtual machine is expected to be deployed.

Item	Description
Service Dependencies	The dependencies of service instances and server roles in the service instance, and the final status information of the dependent service or server role. ○ **Dependent Service**: the service on which the server role depends. ○ **Dependent Server Role**: the server role on which the server role depends. ○ **Dependent Cluster**: the cluster to which the dependent server role belongs. ○ **Dependency in Final Status**: whether the dependent server role reaches the final status.

6.6.1.6. Machine operations

This topic describes the actions about machine operations.

6.6.1.6.1. View the machine dashboard

The machine dashboard allows you to view the statistics of a machine.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the left-side navigation pane, click the **C** tab.
3. (Optional)On the **Machine** tab in the lower-left corner, enter the machine name in the search box. Machines that meet the search condition are displayed.
4. Move the pointer over ℹ at the right of a machine and then select **Dashboard**.
5. On the **Machine Details** page, view all the information of this machine. For more information, see the following table.

Item	Description
Load-System	The system load chart of the cluster.
CPU-System	The CPU load chart.
Mem-System	The memory load chart.
DISK Usage-System	The statistical table of the disk usage.
Traffic-System	The system traffic chart.
TCP State-System	The TCP request status chart.
TCP Retrans-System	The chart of TCP retransmission amount.
DISK IO-System	The statistical table of the disk input and output.

Item	Description
Machine Summary	○ **Project Name**: the name of the project to which the machine belongs. ○ **Cluster Name**: the name of the cluster to which the machine belongs. ○ **Machine Name**: the machine name. ○ **SN**: the serial number of the machine. ○ **IP**: the IP address of the machine. ○ **IDC**: the data center of the machine. ○ **Room**: the room in the data center where the machine is located. ○ **Rack**: the rack where the machine is located. ○ **Unit in Rack**: the location of the rack. ○ **Warranty**: the warranty of the machine. ○ **Purchase Date**: the date when the machine is purchased. ○ **Machine Status**: the running status of the machine. ○ **Status**: the hardware status of the machine. ○ **CPUs**: the number of CPUs for the machine. ○ **Disks**: the disk size. ○ **Memory**: the memory size. ○ **Manufacturer**: the machine manufacturer. ○ **Model**: the machine model. ○ **os**: the operating system of the machine. ○ **part**: the disk partition.
Server Role Status of Machine	The distribution of the current status of all server roles on the machine.
Machine Monitoring Information	○ **Monitored Item**: the name of the monitored item. ○ **Level**: the level of the monitored item. ○ **Description**: the description of the monitored contents. ○ **Updated At**: the time when the monitoring information is updated.

Item	Description
Machine Server Role Status	○ **Service Instance** ○ **Server Role** ○ **Server Role Status** ○ **Server Role Action** ○ **Error Message** ○ **Target Version** ○ **Current Version** ○ **Actual Version Update Time** ○ **Actions**: ■ Click **Details** to go to the **Server Role Dashboard** page. For more information about the server role dashboard, see View the server role dashboard. ■ Click **Restart** to restart the server roles on the machine.
Application Status in Server Roles	○ **Application Name**: the application name. ○ **Process Number** ○ **Status**: the application status. ○ **Current Build ID**: the ID of the current package version. ○ **Target Build ID**: the ID of the expected package version. ○ **Git Version** ○ **Start Time** ○ **End Time** ○ **Interval**: the interval between the time when Apsara Infrastructure Management Framework detects that the process exits and the time when Apsara Infrastructure Management Framework repairs the process. ○ **Information Message**: the normal output logs. ○ **Error Message**: the abnormal logs.

6.6.1.7. Monitoring center

You can view the alert status, alert rules, and alert history in the monitoring center.

6.6.1.7.1. Modify an alert rule

You can modify an alert rule based on the actual business requirements.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Operations > Service Operations**.

3. (Optional)Enter the service name in the search box.
4. Find the service and then click **Management** in the **Actions** column.
5. Click the **Monitoring Template** tab.
6. Find the monitoring template that you are about to edit and then click **Edit** in the **Actions** column.
7. Configure the monitoring parameters based on actual conditions.
8. Click **Save Change**.

   Wait about 10 minutes. The monitoring instance is automatically deployed. If the status becomes Successful and the deployment time is later than the modified time of the template, the changes are successfully deployed.

6.6.1.7.2. View the status of a monitoring instance

After a monitoring instance is deployed, you can view the status of the monitoring instance.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Operations > Service Operations**.
3. (Optional)Enter the service name in the search box.
4. Find the service and then click **Management** in the **Actions** column.
5. Click the **Monitoring Instance** tab. In the **Status** column, view the current status of the monitoring instance.

6.6.1.7.3. View the alert status

This topic describes how to view the alerts related to different services and the alert details.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Monitoring > Alert Status**.
3. (Optional)Search for an alert by service name, cluster name, alert name, or alert time range.
4. View alert details on the **Alert Status** page. The following table describes the related parameters.

Parameter	Description
Service	The name of the service.
Cluster	The name of the cluster where the service is deployed.
Instance	The name of the monitored instance. Click the name of an instance to view the alert history of the instance.
Alert Status	Two alert states are available, which are Normal and Alerting.

Parameter	Description
Alert Level	Alerts are divided into five levels in descending order of severity: ◦ P0: an alert that has been cleared ◦ P1: an urgent alert ◦ P2: a major alert ◦ P3: a minor alert ◦ P4: a reminder alert
Alert Name	The name of the alert. Click the name of an alert to view alert rule details.
Alert Time	The time when the alert is triggered and how long the alert lasts.
Actions	Click **Show** to view the data before and after the alert time.

6.6.1.7.4. View alert rules

This topic describes how to view alert rules.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Monitoring** > **Alert Rules**.
3. (Optional)Search for alert rules by service name, cluster name, or alert name.
4. View alert rules on the **Alert Rules** page. The following table describes the related parameters.

Parameter	Description
Service	The name of the service.
Cluster	The name of the cluster where the service is deployed.
Alert Name	The name of the alert.
Alert Conditions	The conditions that trigger the alert.
Periods	The frequency at which the alert rule is executed.
Alert Contact	The groups and members to notify when the alert is triggered.
Status	The status of the alert rule. ◦ **Running**: Click it to stop the alert rule. ◦ **Stopped**: Click it to execute the alert rule.

6.6.1.7.5. View the alert history

This topic describes how to view the historical alerts related to different services and the alert details.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Monitoring** > **Alert History**.
3. (Optional)Search for an alert by service name, cluster name, or alert time range.
4. View the alert history on the **Alert History** page. The following table describes the related parameters.

Parameter	Description
Service	The name of the service to which the alert belongs.
Cluster	The name of the cluster where the service is deployed.
Alert Instance	The name of the instance where the alert is triggered.
Status	Two alert states are available, which are Normal and Alerting.
Alert Level	Alerts are divided into five levels in descending order of severity: ○ P0: an alert that has been cleared ○ P1: an urgent alert ○ P2: a major alert ○ P3: a minor alert ○ P4: a reminder alert
Alert Name	The name of the alert. Click the name of an alert to view alert rule details.
Alert Time	The time when the alert is triggered.
Alert Contact	The groups and members to notify when the alert is triggered.
Actions	Click **Show** to view the data before and after the alert time.

6.6.1.8. Tasks and deployment summary

This topic describes how to view rolling tasks, running tasks, history tasks, and deployment summary on Apsara Infrastructure Management Framework.

6.6.1.8.1. View rolling tasks

This topic describes how to view rolling tasks and their status.

Procedure

1. Log on to Apsara Infrastructure Management Framework.

2. In the top navigation bar, choose **Operations > Cluster Operations**.
3. Select **Rolling Tasks** to view all clusters that have rolling tasks.
4. Click **rolling** in the **Rolling** column.
5. On the **Rolling Task** page. view the change task information and change details.Change task parameters

Parameter	Description
Change Version	The source version of the rolling task.
Description	The description of the change.
Head Version Analysis	The status of desired state analysis. During desired state analysis, Apsara Infrastructure Management Framework detects the latest cluster version and parses the version to specific change contents. Desired state analysis can be in one of the following states: ◦ **Preparing**: No new version is detected. ◦ **Waiting**: The latest version has been detected, but the analysis module has not started. ◦ **Doing**: The application to be changed is being analyzed. ◦ **done**: The desired state analysis succeeds. ◦ **Failed**: The desired state analysis fails to parse change contents. Apsara Infrastructure Management Framework can obtain change contents of server roles in the latest version only when the desired state analysis is in the **done** state.
Blocked Server Role	The server role that is blocked by dependencies in the rolling task.
Submitter	The person who submits the change.
Submitted At	The time when the change is submitted.
Actions	Click **View Difference** to go to the **Version Difference** page. For more information, see View operation logs. Click **Stop** to terminate the rolling task. Click **Pause** to suspend the rolling task.

Change details parameters

Parameter	Description
Service Name	The name of the service that has changes.

Parameter	Description
Status	The current status of the service. The rolling status of a service is an aggregation result of rolling statuses of multiple server roles. Services can be in one of the following states: ○ **succeeded**: A task succeeds. ○ **blocked**: A task is blocked. ○ **failed**: A task fails.
Server Role Status	The status of the server role. Click **>** to the left of a service name to view the rolling task status of each server role in the service. Server roles can be in one of the following states: ○ **Downloading**: A task is being downloaded. ○ **Rolling**: A rolling task is in progress. ○ **RollingBack**: A rolling task fails and is performing rollback.
Depend On	The services on which the service depends, or the server roles on which the server role depends.
Actions	Click **Stop** to terminate the change of the server role. Click **Pause** to suspend the change of the server role.

6.6.1.8.2. View running tasks

This topic describes how to view running tasks.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Tasks > Running Tasks**.
3. (Optional)Search for running tasks by cluster name, server role name, task status, task submitter, Git version, or time range.
4. Find the target task, move the pointer over the **Rolling Task Status** column, and then click **View Tasks** to go to the **Rolling Task** page. For more information about rolling task details, see View rolling tasks.

6.6.1.8.3. View historical tasks

This topic describes how to view historical tasks.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Tasks > History Tasks**.
3. (Optional)Search for historical tasks by cluster name, Git version, submitter, or time range.
4. Find the target task and click **Details** in the **Actions** column to go to the **Rolling Task** page. For more information about rolling task details, see View rolling tasks.

6.6.1.8.4. View the deployment summary

On the **Deployment Summary** page, you can view the deployment conditions of clusters, services, and server roles in all projects on Apsara Infrastructure Management Framework.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the top navigation bar, choose **Tasks > Deployment Summary**.
    - View the deployment status and the duration of a certain status for each project.
        - Gray: wait to be deployed. It indicates that some services of the project depend on server roles or service instances that are being deployed, and other service instances or server roles in the project have already been deployed.
        - Blue: being deployed. It indicates that the project has not reached the final status for one time yet.
        - Green: has reached the final status. It indicates that all clusters in the project have reached the final status.
        - Orange: not reaches the final status. It indicates that a server role does not reach the final status for some reason after the project reaches the final status for the first time.
    - Configure the global clone switch.
        - **normal**: Clone is allowed.
        - **block**: Clone is forbidden.
    - Configure the global dependency switch.
        - **normal**: All configured dependencies are checked.
        - **ignore**: The dependency is not checked.
        - **ignore_service**: None of the service-level dependencies, including the server role dependencies across services, are checked, and only the server role-level dependencies are checked.
3. Click the **Deployment Details** tab to view the deployment details.

    For more information, see the following table.

Item	Description

Item	Description
Status Statistics	The general statistics of deployment conditions, including the total number of projects that are currently available. Click each status to display the projects in the corresponding status in the list. The projects have five deployment statuses: ○ **Final**: All the clusters in the project have reached the final status. ○ **Deploying**: The project has not reached the final status for one time yet. ○ **Waiting**: Some services of the project depend on server roles or service instances that are being deployed, and other service instances or server roles in the project have already been deployed. ○ **Non-final**: A server role does not reach the final status for some reason after the project reaches the final status for the first time. ○ **Inspector Warning**: An error is detected on service instances in the project during the inspection.
Start Time	The time when Apsara Infrastructure Management Framework starts the deployment.
Progress	The proportion of server roles that reach the final status to all the server roles in the current environment.
Deployment Status	The time indicates the deployment duration for the following statuses: **Final**, **Deploying**, **Waiting**, and **Inspector Warning**. The time indicates the duration before the final status is reached for the **Non-final** status. Click the time to view the details.
Deployment Progress	The proportion of clusters, services, and server roles that reach the final status to the total clusters, services, and server roles in the project. Move the pointer over the blank area at the right of the data of roles and then click **Details** to view the deployment statuses of clusters, services, and server roles. The deployment statuses are indicated by icons, which are the same as those used for status statistics.
Resource Application Progress	**Total** indicates the total number of resources related to the project. ○ **Done**: the number of resources that have been successfully applied for. ○ **Doing**: the number of resources that are being applied for and retried. The number of retries (if any) is displayed next to the number of resources. ○ **Block**: the number of resources whose applications are blocked by other resources. ○ **Failed**: the number of resources whose applications failed.
Inspector Error	The number of inspection alerts for the current project.
Monitoring Information	The number of alerts generated for the machine monitor and the machine server role monitor in the current project.

Item	Description
Dependency	Click the icon to view the project services that depend on other services, and the current deployment status of the services that are depended on.

6.6.1.9. Reports

The system allows you to search for and view reports based on your business needs, and add commonly used reports to your favorites.

6.6.1.9.1. View reports

The **Reports** menu allows you to view the statistical data.

Context

You can view the following reports on Apsara Infrastructure Management Framework.

- System reports: default and common reports in the system.
- All reports: includes the system reports and custom reports.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. You can go to the report list in the following three ways:
   - In the top navigation bar, choose **Reports > System Reports**.
   - In the top navigation bar, choose **Reports > All Reports**.
   - In the left-side navigation pane, click the **R** tab. Move the pointer over ℹ at the right of **All Reports** and then select **View**.

   See the following table for the report descriptions.

Item	Description
Report	The report name. Move the pointer over ▾ next to **Report** to search for reports by report name.
Group	The group to which the report belongs. Move the pointer over ▾ next to **Group** to filter reports by group name.
Status	Indicates whether the report is published.
Public	Indicates whether the report is public.
Created By	The person who creates the report.
Published At	The published time and created time of the report.

Item	Description
Actions	Click **Add to Favorites** to add this report to your favorites. Then, you can view the report by choosing **Reports > Favorites** in the top navigation bar or moving the pointer over ⋮ at the right of **Favorites** on the **R** tab in the left-side navigation pane and then selecting **View**.

3. (Optional)Enter the name of the report that you are about to view in the search box.
4. Click the report name to go to the corresponding report details page. For more information about the reports, see Appendix.

6.6.1.9.2. Add a report to favorites

You can add common reports to favorites. Then, find them quickly on the **Favorites** page.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. You can go to the report list in the following three ways:
   - In the top navigation bar, choose **Reports > System Reports**.
   - In the top navigation bar, choose **Reports > All Reports**.
   - In the left-side navigation pane, click the **R** tab. Move the pointer over ⋮ at the right of **All Reports** and then select **View**.
3. (Optional)Enter the name of the report that you are about to add to favorites in the search box.
4. At the right of the report, click **Add to Favorites** in the **Actions** column.
5. In the displayed **Add to Favorites** dialog box, enter tags for the report.
6. Click **Add to Favorites**.

6.6.1.10. Appendix

6.6.1.10.1. Project component info report

This report displays the name and status for each type of project components, including services, server roles, and machines.

Item	Description
Project	The project name.
Cluster	The name of a cluster in the project.
Service	The name of a service in the cluster.
Server Role	The name of a server role in the service.

Item	Description
Server Role Status	The running status of the server role on the machine.
Server Role Action	The action that the server role performs on the machine. Data is available only when Apsara Infrastructure Management Framework asks the server role to perform certain actions, such as rolling and restart actions.
Machine Name	The hostname of the machine.
IP	The IP address of the machine.
Machine Status	The running status of the machine.
Machine Action	The action that Apsara Infrastructure Management Framework asks the machine to perform, such as the clone action.

6.6.1.10.2. IP list

This report displays the IP addresses of physical machines and Docker applications.

IP List of Physical Machines

Item	Description
Project	The project name.
Cluster	The cluster name.
Machine Name	The hostname of the machine.
IP	The IP address of the machine.

IP List of Docker Applications

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Machine Name	The hostname of the machine.
Docker Host	The Docker hostname.
Docker IP	The Docker IP address.

6.6.1.10.3. Machine info report

This report displays the statuses of machines and server roles on the machines.

Machine Status

Displays all the machines currently managed by Apsara Infrastructure Management Framework and their corresponding statuses. In the **Global Filter** section at the top of the page, select the project, cluster, and machine from the **project**, **cluster**, and **machine** drop-down lists, and then click **Filter** on the right to filter the data.

Item	Description
Machine Name	The machine name.
IP	The IP address of the machine.
Machine Status	The machine status.
Machine Action	The action currently performed by the machine.
Machine Action Status	The action status.
Status Description	The description about the machine status.

Expected Server Role List

Select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The machine name.
Server Role	The name of the expected server role on the machine.

Abnormal Monitoring Status

Select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The machine name.
Monitored Item	The name of the monitored item.
Level	The level of the monitored item.
Description	The description of the monitored item contents.
Updated At	The updated time of the monitored item.

Server Role Version and Status on Machine

Select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The machine name.
Server Role	The server role name.
Server Role Status	The status of the server role.
Target Version	The expected version of the server role on the machine.
Current Version	The current version of the server role on the machine.
Status Description	The description about the status.
Error Message	The exception message of the server role.

Monitoring Status

Select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The machine name.
Server Role	The server role name.
Monitored Item	The name of the monitored item.
Level	The level of the monitored item.
Description	The description of the monitored item contents.
Updated At	The updated time of the monitored item.

6.6.1.10.4. Rolling info report

This report displays the running and completed rolling tasks and the task-related status.

Choose a rolling action

This list only displays the running rolling tasks. If no rolling task is running, no data is available in the list.

Item	Description
Cluster	The cluster name.
Git Version	The version of change that triggers the rolling task.
Description	The description about the change entered by a user when the user submits the change.
Start Time	The start time of the rolling task.

Item	Description
End Time	The end time of the rolling task.
Submitted By	The ID of the user who submits the change.
Rolling Task Status	The current status of the rolling task.
Submitted At	The time when the change is submitted.

Server Role in Job

Select a rolling task in the **Choose a rolling action** section to display the rolling status of server roles related to the selected task. If no rolling task is selected, the server role statuses of all historical rolling tasks are displayed.

Item	Description
Server Role	The server role name.
Server Role Status	The rolling status of the server role.
Error Message	The exception message of the rolling task.
Git Version	The version of change to which the rolling task belongs.
Start Time	The start time of the rolling task.
End Time	The end time of the rolling task.
Approve Rate	The proportion of machines that have the rolling task approved by the decider.
Failure Rate	The proportion of machines that have the rolling task failed.
Success Rate	The proportion of machines that have the rolling task succeeded.

Server Role Rolling Build Information

The source version and target version of each application under the server role in the rolling process.

Item	Description
App	The name of the application that requires rolling in the server role.
Server Role	The server role to which the application belongs.
From Build	The version before the upgrade.

Item	Description
To Build	The version after the upgrade.

Server Role Statuses on Machines

Select a server role in the **Server Role in Job** section to display the deployment status of this server role on the machine.

Item	Description
Machine Name	The name of the machine on which the server role is deployed.
Expected Version	The target version of the rolling.
Actual Version	The current version.
State	The status of the server role.
Action Name	The Apsara Infrastructure Management Framework action currently performed by the server role.
Action Status	The action status.

6.6.1.10.5. Machine RMA approval pending list

Some Apsara Infrastructure Management Framework actions (such as restart) on machines and server roles can be triggered by users, but this type of actions must be reviewed and approved. This report is used to process the actions that must be reviewed and approved.

Machine

Displays the basic information of pending approval machines.

Item	Description
Project	The project name.
Cluster	The cluster name.
Hostname	The hostname of the machine.
IP	The IP address of the machine.
State	The running status of the machine.
Action Name	The action on the machine.
Action Status	The status of the action on the machine.

Item	Description
Actions	The approval button.

Machine Serverrole

Displays the information of server roles on the pending approval machines.

Item	Description
Project	The project name.
Cluster	The cluster name.
Hostname	The hostname of the machine.
IP	The IP address of the machine.
Serverrole	The server role name.
State	The running status of the server role.
Action Name	The action on the server role.
Action Status	The status of the action on the server role.
Actions	The approval button.

Machine Component

Displays the hard disk information of pending approval machines.

Item	Description
Project	The project name.
Cluster	The cluster name.
Hostname	The hostname of the machine.
Component	The hard disk on the machine.
State	The running status of the hard disk.
Action Name	The action on the hard disk.
Action Status	The status of the action on the hard disk.
Actions	The approval button.

6.6.1.10.6. Registration vars of services

This report displays values of all service registration variables.

Item	Description
Service	The service name.
Service Registration	The service registration variable.
Cluster	The cluster name.
Update Time	The updated time.

6.6.1.10.7. Virtual machine mappings

Use the global filter to display the virtual machines of a specific cluster.

Displays the information of virtual machines in the cluster. Data is available only when virtual machines are deployed in the cluster.

Item	Description
Project	The project name.
Cluster	The cluster name.
VM	The hostname of the virtual machine.
Currently Deployed On	The hostname of the physical machine on which the virtual machine is currently deployed.
Target Deployed On	The hostname of the physical machine on which the virtual machine is expected to be deployed.

6.6.1.10.8. Service inspector report

Use the global filter to display the service inspection reports of a specific cluster.

Service Inspector: Data is available only for services with inspection configured.

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Description	The contents of the inspection report.
Level	The level of the inspection report.

6.6.1.10.9. Resource application report

In the **Global Filter** section, select the project, cluster, and machine from the **project**, **cluster**, and **machine** drop-down lists and then click **Filter** on the right to display the corresponding resource application data.

Change Mappings

Item	Description
Project	The project name.
Cluster	The cluster name.
Version	The version where the change occurs.
Resource Process Status	The resource application status in the version.
Msg	The exception message.
Begintime	The start time of the change analysis.
Endtime	The end time of the change analysis.

Changed Resource List

Item	Description
Res	The resource ID.
Type	The resource type.
Name	The resource name.
Owner	The application to which the resource belongs.
Parameters	The resource parameters.
Ins	The resource instance name.
Instance ID	The resource instance ID.

Resource Status

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.

Item	Description
APP	The application of the server role.
Name	The resource name.
Type	The resource type.
Status	The resource application status.
Parameters	The resource parameters.
Result	The resource application result.
Res	The resource ID.
Reprocess Status	The status of the interaction with Business Foundation System during the VIP resource application.
Reprocess Msg	The error message of the interaction with Business Foundation System during the VIP resource application.
Reprocess Result	The result of the interaction with Business Foundation System during the VIP resource application.
Refer Version List	The version that uses the resource.
Error Msg	The exception message.

6.6.1.10.10. Statuses of project components

This report displays the status of all server roles in an abnormal status on machines of the project, and the monitoring information (alert information reported by the server role to Apsara Infrastructure Management Framework monitor) of server roles and machines.

Error State Component Table

Only displays the information of server roles that are not in GOOD status and server roles to be upgraded.

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Machine Name	The machine name.

Item	Description
Need Upgrade	Whether the current version reaches the final status.
Server Role Status	The current status of the server role.
Machine Status	The current status of the machine.

Server Role Alert Information

Select a row in the **Error State Component Table** section to display the corresponding information in the list.

Item	Description
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Machine Name	The machine name.
Monitored Item	The monitored item name of the server role.
Level	The alert level.
Description	The description about the alert contents.
Updated At	The updated time of the alert information.

Machine Alert Information

Select a row in the **Error State Component Table** section to display the corresponding information in the list.

Item	Description
Cluster	The cluster name.
Machine Name	The machine name.
Monitored Item	The monitored item name of the server role.
Level	The alert level.
Description	The description about the alert contents.
Updated At	The updated time of the alert information.

Service Inspector Information

Select a row in the **Error State Component Table** section to display the corresponding information in the list.

Item	Description
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Monitored Item	The monitored item name of the server role.
Level	The alert level.
Description	The description about the alert contents.
Updated At	The updated time of the alert information.

6.6.1.10.11. Relationship of service dependency

This report displays the dependencies among server roles. Use the global filter to display the data of a specific cluster in the list.

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Dependent Service	The service on which the server role depends.
Dependent Server Role	The server role on which the server role depends.
Dependent Cluster	The cluster to which the dependent server role belongs.
Dependency in Final Status	Whether the dependent server role reaches the final status.

6.6.1.10.12. Check report of network topology

This report checks if network devices and machines have wirecheck alerts.

Check Report of Network Topology

Checks if network devices have wirecheck alerts.

Item	Description
Cluster	The cluster name.
Network Instance	The name of the network device.
Level	The alert level.
Description	The description about the alert information.

Check Report of Server Topology

Checks if servers (machines) have wirecheck alerts.

Item	Description
Cluster	The cluster name.
Machine Name	The server (machine) name.
Level	The alert level.
Description	The description about the alert information.

6.6.1.10.13. Clone report of machines

This report displays the clone progress and status of machines.

Clone Progress of Machines

Item	Description
Project	The project name.
Cluster	The cluster name.
Machine Name	The machine name.
Machine Status	The running status of the machine.
Clone Progress	The progress of the current clone process.

Clone Status of Machines

Item	Description
Project	The project name.
Cluster	The cluster name.
Machine Name	The machine name.

Item	Description
Machine Action	The action performed by the machine, such as the clone action.
Machine Action Status	The status of the action performed by the machine.
Machine Status	The running status of the machine.
Level	Whether the clone action performed by the machine is normal.
Clone Status	The current status of the clone action performed by the machine.

6.6.1.10.14. Auto healing/install approval pending report

The list structure is the same as the machine RMA approval pending list, whereas this view is used for the approval during the installation. For more information, see Machine RMA approval pending list.

6.6.1.10.15. Machine power on or off statuses of clusters

After a cluster starts or shuts down machines, you can view the related information in this report.

Cluster Running Statuses

If a cluster is starting or shutting down machines, the corresponding data is available in this list. No data indicates that no cluster has machines shut down.

Item	Description
Project	The project name.
Cluster	The cluster name.
Action Name	The startup or shutdown action that is being performed by the cluster.
Action Status	The status of the action.

Server Role Power On or Off Statuses

Displays the power on or off statuses of server roles in the cluster selected in the **Cluster Running Statuses** section.

Select a row in the **Cluster Running Statuses** section to display the information of the corresponding cluster in the list.

Item	Description
Cluster	The cluster name.
Server Role	The server role name.

Item	Description
Action Name	The startup or shutdown action that is being performed by the server role.
Action Status	The status of the action.

Statuses on Machines

Displays the running status of the selected server role on machines.

Select a row in the **Server Role Power On or Off Statuses** section to display the information of the corresponding server role in the list.

Item	Description
Cluster	The cluster name.
Server Role	The server role name.
Machine Name	The machine name.
Server Role Status	The running status of the server role.
Server Role Action	The action currently performed by the server role.
Server Role Action Status	The status of the action.
Error Message	The exception message.

Machine Statuses

Displays the running statuses of machines in the selected cluster.

Select a row in the **Statuses on Machines** section to display the information of the corresponding machine in the list.

Item	Description
Cluster	The cluster name.
Machine Name	The machine name.
IP	The IP address of the machine.
Machine Status	The running status of the machine.
Machine Action	The action currently performed by the machine.
Machine Action Status	The action status of the machine.
Error Message	The exception message.

6.6.2. New console

6.6.2.1. Introduction to Apsara Infrastructure Management Framework

This topic describes the features and terms of Apsara Infrastructure Management Framework.

6.6.2.1.1. What is Apsara Infrastructure Management Framework?

Apsara Infrastructure Management Framework is a distributed data center management system. It can manage applications within clusters that contain multiple machines and provide basic features such as deployment, upgrade, scale-in, scale-out, and configuration change.

Apsara Infrastructure Management Framework also provides data monitoring and report analysis features to facilitate end-to-end operations and maintenance (O&M) and management. In large-scale distributed scenarios, Apsara Infrastructure Management Framework offers automatic O&M to improve O&M efficiency and system availability.

Apsara Infrastructure Management Framework is composed of TianjiMaster and TianjiClient. TianjiClient is installed as an agent on a machine. TianjiMaster delivers the received commands to TianjiClient. Apsara Infrastructure Management Framework uses components to implement different features and provides users with the APIServer and console.

6.6.2.1.2. Features

This topic describes the core features of Apsara Infrastructure Management Framework.

Apsara Infrastructure Management Framework provides the following core features:

- Initializes networks within a data center.
- Manages server installation and maintenance processes.
- Deploys, scales, and upgrades cloud services.
- Manages cloud service configurations.
- Applies for cloud service resources.
- Repairs software and hardware faults.
- Monitors software and hardware infrastructure and business processes.

6.6.2.1.3. Terms

This topic describes the basic terms related to Apsara Infrastructure Management Framework.

project

A group of clusters. A project provides services for users.

cluster

A group of physical machines. A cluster provides services logically and is used to deploy software of a project.

A cluster can only belong to a single project. Multiple services can be deployed within a cluster.

service

A group of software programs used to provide an independent set of features. A service is composed of one or more server roles. A service can be deployed within multiple clusters to provide service capabilities. For example, pangu, fuxi, and nuwa are all services.

service instance

A service that is deployed within a cluster.

server role

One or more indivisible feature units of a service. A server role is composed of one or more applications. If a service is deployed within a cluster, all server roles of the service must be deployed on machines within the same cluster. Multiple server roles, such as PanguMaster and TianjiClient, can be deployed on the same machine.

service role instance

A service role that is deployed on a machine. A service role can be deployed on multiple machines.

application

A process component contained in a server role. Each application works independently. Applications are the minimum units that can be deployed and upgraded in Apsara Infrastructure Management Framework, and can be deployed on each machine. Typically, an application is an executable software program or Docker container.

If a server role is deployed on a machine, all applications in the server role must be deployed on the machine.

Rolling

A process in which Apsara Infrastructure Management Framework upgrades services and modifies cluster configurations based on the configurations updated by users.

service configuration template

A template that contains the same service configurations. A service configuration template can make it easy to write the same configurations to different clusters, and applies to large-scale deployment and upgrade scenarios.

associated service template

A file named template.conf in service configurations. The file declares that a specific version of a service configuration template is used by a service instance.

service deployment

An action that deploys a service from scratch within a cluster.

desired state

A state in which all hardware and software on each machine of a cluster work normally and all software programs are in the desired versions.

dependency

A dependency relationship between server roles in a service. Tasks are executed or configurations are upgraded based on the dependency relationship. For example, assume that A depends on B. In this case, A is downloaded after B is downloaded and upgraded after B is upgraded. By default, the dependency of configuration upgrade does not take effect.

upgrade

A way to change the current state of a service to the desired state. After a user submits a version change request, Apsara Infrastructure Management Framework can upgrade the service version to the desired version. An upgrade is performed on each server role, and aims to upgrade all machines to the desired version.

Before an upgrade starts, the current and desired states of a cluster are the same. When a user submits a version change request, the current state remains unchanged, but the desired state changes. A rolling task is generated to gradually approximate the current state to the desired state. When the upgrade ends, the current state is exactly the same as the desired state.

6.6.2.2. Log on to the Apsara Infrastructure Management Framework console

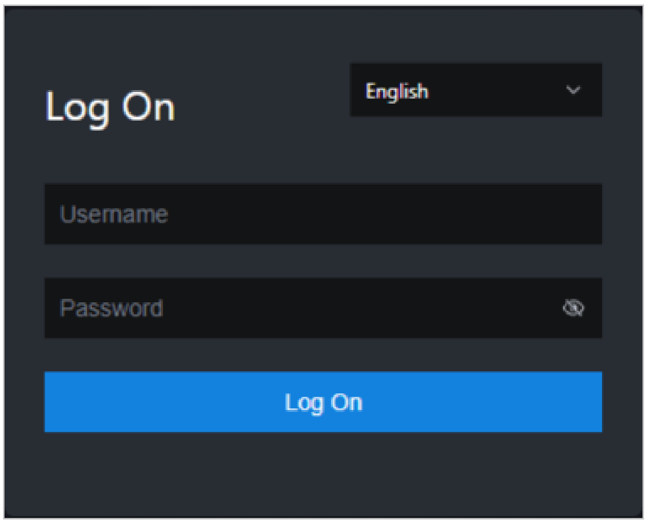
This topic describes how to log on to the Apsara Infrastructure Management Framework console.

Prerequisites

- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.
- The endpoint of the Apsara Uni-manager Operations Console is in the following format: *ops.asconsole.intranet-domain-id*.com.
- A browser is installed. We recommend that you use the Google Chrome browser.

Procedure

1. Open your browser.
2. In the address bar, enter the endpoint *ops.asconsole.intranet-domain-id*.com. Press the Enter key.



> Note
>
> You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

> Note
>
> Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username. For security reasons, your password must meet the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password is 10 to 20 characters in length.

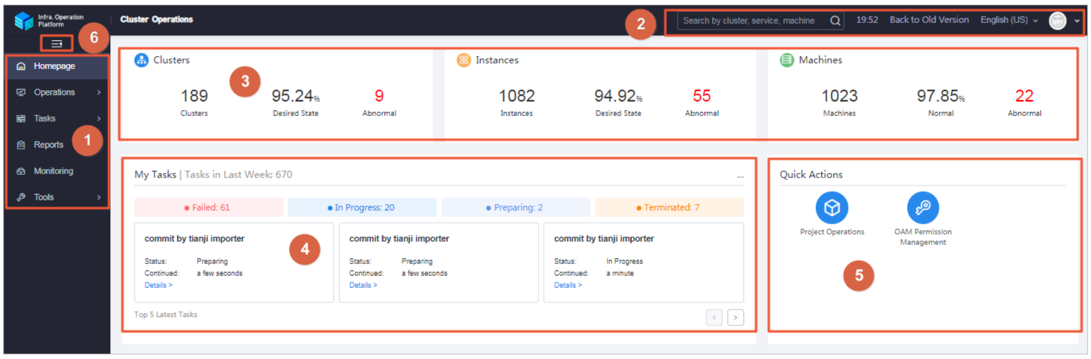
4. Click **Log On**.
5. In the top navigation bar, click **O&M**.
6. In the left-side navigation pane, choose **Product Management**>**Products**.
7. In the **Apsara Stack O&M** section, choose **Basic O&M**>**Apsara Infrastructure Management Framework**.

6.6.2.3. Instructions for the homepage

After you log on to the Apsara Infrastructure Management Framework console, the homepage appears. This topic describes the basic operations and features available on the homepage.

Log on to the Apsara Infrastructure Management Framework console. The homepage appears, as shown in the following figure.

Homepage of the Apsara Infrastructure Management Framework console



The following table describes the functional sections on the homepage.

Description of functional sections

No.	Section	Description
①	Left-side navigation pane	• **Operations**: the quick entrance to operations & maintenance (O&M) operations, which allows you to find operations and their objects. This menu consists of the following submenus: ◦ **Project Operations**: allows you to manage projects based on your project permissions. ◦ **Cluster Operations**: allows you to perform O&M and management operations on clusters based on your project permissions. For example, you can view the status of clusters. ◦ **Service Operations**: allows you to to manage services based on your service permissions. For example, you can view the service list. ◦ **Machine Operations**: allows you to perform O&M and management operations on all machines. For example, you can view the status of machines. • **Tasks**: Rolling tasks are generated after you modify configurations in the system. This menu allows you to view the running tasks, task history, and deployment of clusters, services, and server roles in all projects. • **Reports**: allows you to view monitoring data in tables and find specific reports by using fuzzy search. • **Monitoring**: monitors metrics during system operations and sends alert notifications for abnormal conditions. This menu allows you to view the alert status, modify alert rules, and search alert history. • **Tools**: provides tools such as machine O&M, IDC shutdown, and clone progress.

No.	Section	Description
②	Top navigation bar	- Search box: supports global search. You can enter a keyword in the search box to search for clusters, services, and machines. - The following information is displayed when you move the pointer over the time: ◦ **TJDB Sync Time**: the time when the data on the current page is generated. ◦ **Desired State Calc Time**: the time when the desired-state data on the current page is calculated. The system processes data as fast as it can after the data is generated. Latency exists because Apsara Infrastructure Management Framework is an asynchronous system. Time information helps explain why data on the current page is generated and determine whether the system is faulty. - **Back to Old Version**: allows you to return to the old version of the Apsara Infrastructure Management Framework console. - **English (US)**: the current display language of the console. You can select another language from the drop-down list. - Profile picture: allows you to select **Exit** from the drop-down list to log out of your account.
③	Status bar of global resources	Displays the overview of global resources. - **Cluster**: displays the total number of clusters, the percentage of clusters that have reached the desired state, and the number of abnormal clusters. - **Service Instances**: displays the total number of instances, the percentage of instances that have reached the desired state, and the number of abnormal instances. - **Machine**: displays the total number of machines, the percentage of machines in the Normal state, and the number of abnormal machines. You can move the pointer over each section and then click **Details** to go to the Cluster Operations, Service Operations, or Machine Operations page.
④	Task status bar	Displays the information of tasks submitted within the last week. You can click the number next to a task state to go to the My Tasks page and view the task details. The top 5 latest tasks are displayed in the lower part of the section. You can click **Details** corresponding to each task to view the task details.
⑤	Quick actions	Displays links of the following common quick actions: - **Project Operations**: allows you to go to the Project Operation page. - **OAM Permission Management**: allows you to go to the Operation Administrator Manager (OAM) console. OAM is a centralized permission management platform in the ASO console.

No.	Section	Description
⑥	Show/hide button	Allows you to show or hide the left-side navigation pane to narrow or enlarge the workspace.

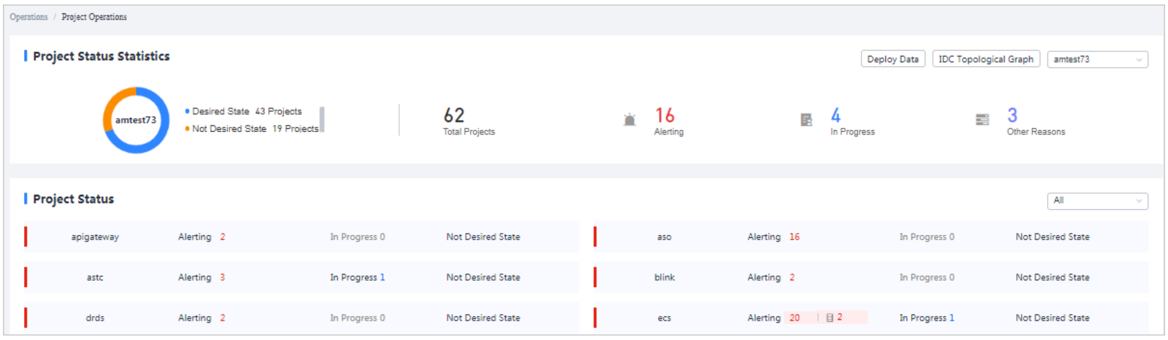
6.6.2.4. Operations

6.6.2.4.1. Project operations

This topic describes how to query a project and view its details.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations > Project Operations**.



Operations / Project Operations

Project Status Statistics

Deploy Data | IDC Topological Graph | amtest73

amtest73
- Desired State 43 Projects
- Not Desired State 19 Projects

62 Total Projects | 16 Alerting | 4 In Progress | 3 Other Reasons

Project Status

All

apigateway	Alerting 2	In Progress 0	Not Desired State	aso	Alerting 16	In Progress 0	Not Desired State
astc	Alerting 3	In Progress 1	Not Desired State	blink	Alerting 2	In Progress 0	Not Desired State
drds	Alerting 2	In Progress 0	Not Desired State	ecs	Alerting 20 | 2	In Progress 1	Not Desired State

3. On the Project Operations page, perform the following operations:
   - Query a project

     In the upper-right corner of the **Project Status** section, enter the name of a project in the search box to search for the project. The search results include the number of alerts, the number of tasks in progress, and whether the project reaches the desired state.

   - View project details
     - Click the number next to **Alerting** corresponding to a project. In the Alert Information dialog box, view the metric name, metric type, and alert source. Click the alert source to view service details.
     - Click the number next to **In Progress** corresponding to a project. In the Tasks dialog box, view details about service upgrade and machine change.

6.6.2.4.2. Cluster operations

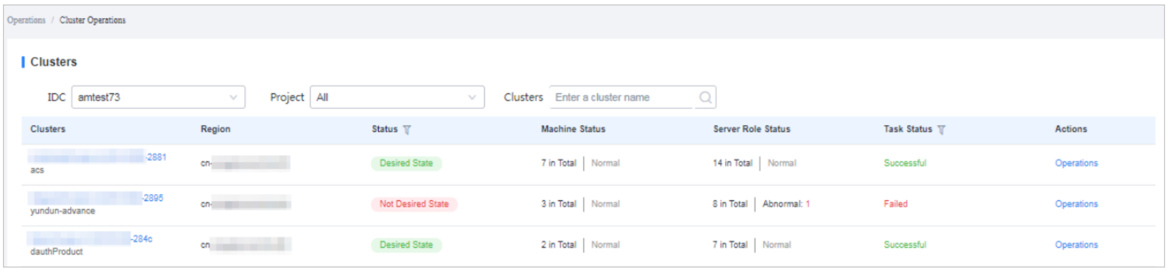
This topic describes the actions about cluster operations.

6.6.2.4.2.1. View the cluster list

This topic describes how to view all clusters and their information.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Use one of the following methods to go to the cluster list:
   - On the **Home** page, move the pointer over the **Cluster** section and click Details in the upper-right corner.
   - In the left-side navigation pane, choose **Operations** > **Cluster Operations**.



Operations / Cluster Operations

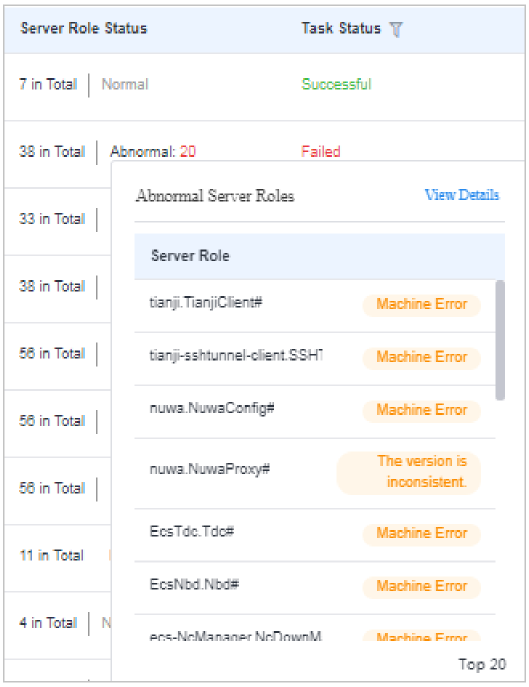
Clusters

IDC amtest73 Project All Clusters Enter a cluster name

Clusters	Region	Status	Machine Status	Server Role Status	Task Status	Actions
[redacted]-2881 acs	cn-[redacted]	Desired State	7 in Total | Normal	14 in Total | Normal	Successful	Operations
[redacted]-2895 yundun-advance	cn-[redacted]	Not Desired State	3 in Total | Normal	8 in Total | Abnormal: 1	Failed	Operations
[redacted]-284c dauthProduct	cn[redacted]	Desired State	2 in Total | Normal	7 in Total | Normal	Successful	Operations

The following table describes the information displayed in the cluster list.

Parameter	Description
Cluster	The name of the cluster. Click the cluster name to view the cluster details.
Region	The region where the cluster is deployed.
Status	Specifies whether the cluster reaches the desired state. Click the ⊽ icon to filter clusters. - Desired State: The cluster has reached the desired state. - Not Desired State: The cluster has reached the desired state for the first time but a server role has not reached the desired state due to undefined reasons.
Machine Status	The number of machines within the cluster and the machine status. Click the machine status to go to the Machines tab of the Cluster Details page.

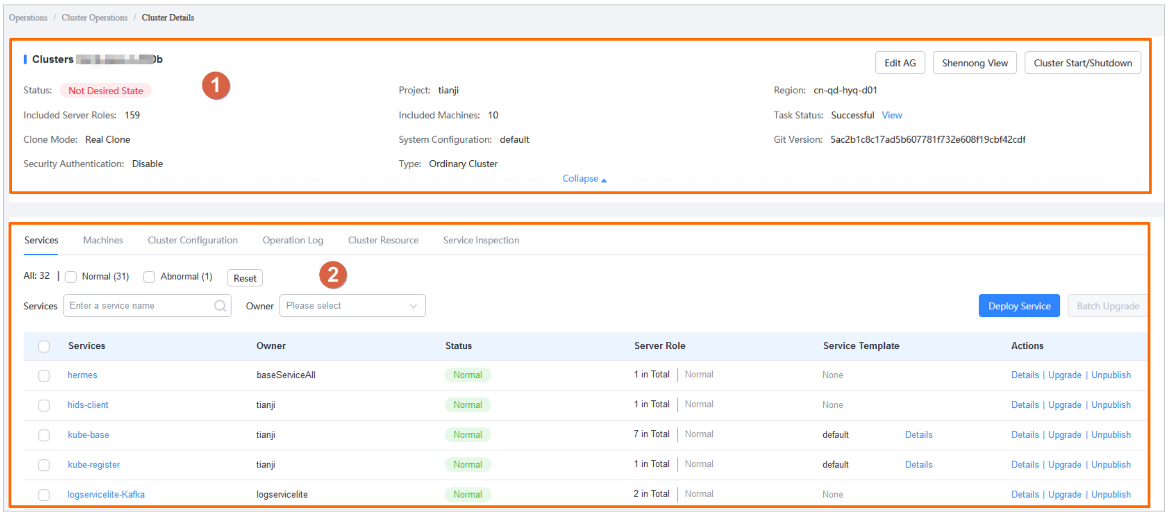
Parameter	Description
Server Role Status	The number of server roles within the cluster and the server role status. Click a server role status to go to the Services tab of the Cluster Details page. Click **Abnormal** in the Server Role Status column to view all the abnormal server roles in the cluster in the displayed dialog box. Click **View Details** in the upper-right corner of the dialog box to go to the Services tab of the Cluster Details page.  Server Role Status · Task Status 7 in Total · Normal · Successful 38 in Total · Abnormal: 20 · Failed 33 in Total 38 in Total 56 in Total 56 in Total 56 in Total 11 in Total 4 in Total Abnormal Server Roles · View Details Server Role tianji.TianjiClient# · Machine Error tianji-sshtunnel-client.SSHT · Machine Error nuwa.NuwaConfig# · Machine Error nuwa.NuwaProxy# · The version is inconsistent. EcsTdc.Tdc# · Machine Error EcsNbd.Nbd# · Machine Error ecs-NcManager.NcDownM · Machine Error Top 20
Task Status	The status of the task related to the cluster. Click the ▽ icon to filter clusters. Click the task status to view the task details.
Actions	The available operations. Click **Operations** to go to the **Cluster Details** page.

6.6.2.4.2.2. View details of a cluster

This topic describes how to view details of a cluster.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
3. (Optional)Select a project from the drop-down list or enter a cluster name to search for the cluster.
4. Click the cluster name or click **Operations** in the **Actions** column to go to the **Cluster Details** page.



Operations / Cluster Operations / Cluster Details

Clusters [redacted]b

Status: Not Desired State

Project: tianji

Region: cn-qd-hyq-d01

Included Server Roles: 159

Included Machines: 10

Task Status: Successful View

Clone Mode: Real Clone

System Configuration: default

Git Version: 5ac2b1c8c17ad5b607781f732e608f19cbf42cdf

Security Authentication: Disable

Type: Ordinary Cluster

All: 32 | □ Normal (31) □ Abnormal (1) Reset

Services: Enter a service name   Owner: Please select

□	Services	Owner	Status	Server Role	Service Template	Actions
□	hermes	baseServiceAll	Normal	1 in Total | Normal	None	Details | Upgrade | Unpublish
□	hids-client	tianji	Normal	1 in Total | Normal	None	Details | Upgrade | Unpublish
□	kube-base	tianji	Normal	7 in Total | Normal	default Details	Details | Upgrade | Unpublish
□	kube-register	tianji	Normal	1 in Total | Normal	default Details	Details | Upgrade | Unpublish
□	logservicelite-Kafka	logservicelite	Normal	2 in Total | Normal	None	Details | Upgrade | Unpublish

Section	Parameter	Description
①	**Status**	○ **Desired State**: All clusters in a project have reached the desired state. ○ **Not Desired State**: A project has reached the desired state for the first time but a server role has not reached the desired state due to undefined reasons.
	Project	The project to which the cluster belongs.
	Region	The region where the cluster is deployed.
	Included Server Roles	The number of server roles included in the cluster.
	Included Machines	The number of machines included in the cluster.
	Task Status	The status of the task. Click **View** to view the task details. ○ **Successful**: The task is successful. ○ **Preparing**: Data is being synchronized and the task is not started. ○ **In Progress**: The cluster has a changing task. ○ **Paused**: The task is paused. ○ **Failed**: This task failed. ○ **Terminated**: The task is manually terminated.
	Clone Mode	○ **Pseudo-clone**: The system is not cloned when a machine is added to the cluster. ○ **Real Clone**: The system is cloned when a machine is added to the cluster.

Section	Parameter	Description
	System Configuration	The name of the system service template used by the cluster.
	Git Version	The change version to which the cluster belongs.
	Security Authentication	The access control among processes. By default, security authentication is disabled in non-production environments. You can enable or disable security authentication to meet your business requirements.
	Type	○ **Ordinary Cluster**: an operations unit of machine groups, where multiple services can be deployed. ○ **Virtual Cluster**: an operations unit of services, which can manage versions of software on machines within several physical clusters in a centralized manner. ○ **RDS**: a type of cluster that renders special cgroup configurations based on some rules. ○ **NETFRAME**: a type of cluster that renders special configurations for special scenarios of Server Load Balancer (SLB). ○ **T4**: a type of cluster that renders special configurations for the mixed deployment of e-commerce. Apsara Stack provides only ordinary clusters.
②	**Services**	The status of each service within the cluster. You can also upgrade or unpublish a service. ○ **Normal**: The service works normally. ○ **Not Deployed**: The service is not deployed on machines. ○ **Changing**: Some server roles in the service are changing. ○ **Operating**: No server role is changing, but a server role is performing operations and maintenance (O&M) operations. ○ **Abnormal**: No server role is changing or the machines where server roles are deployed are not performing O&M operations. However, the server role status is **not good** or the version that the service runs on the machines is different from the desired state configuration.
	Machines	The running status and monitoring status of each machine within the cluster. You can also view details of server roles that are deployed on each machine.
	Cluster Configuration	The configuration file used within the cluster.
	Operation Logs	The operation logs. You can also view the version differences.

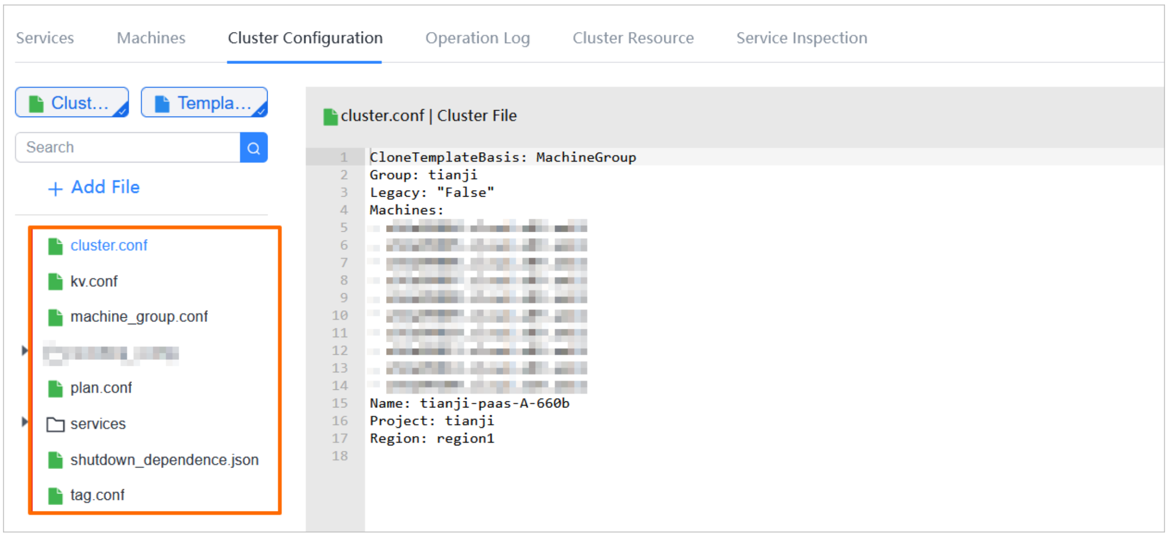
Section	Parameter	Description
	Cluster Resources	The details of resources that can be filtered.
	Service Inspection	The inspection information of each service within the cluster.

6.6.2.4.2.3. View configuration information of a cluster

This topic describes how to view configuration files and folders of a cluster.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Use one of the following methods to go to the **Cluster Configuration** tab to view configuration files and folders.
   - Enter a cluster name in the search box in the upper-right corner of the page. Click **Operations** next to the found cluster. On the Cluster Details page, click the **Cluster Configuration** tab.
   - In the left-side navigation pane, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find a cluster and click **Operations** in the **Actions** column. On the Cluster Details page, click the **Cluster Configuration** tab.



```
CloneTemplateBasis: MachineGroup
Group: tianji
Legacy: "False"
Machines:
[redacted]
Name: tianji-paas-A-660b
Project: tianji
Region: region1
```

The following table describes configuration files and folders of a cluster.

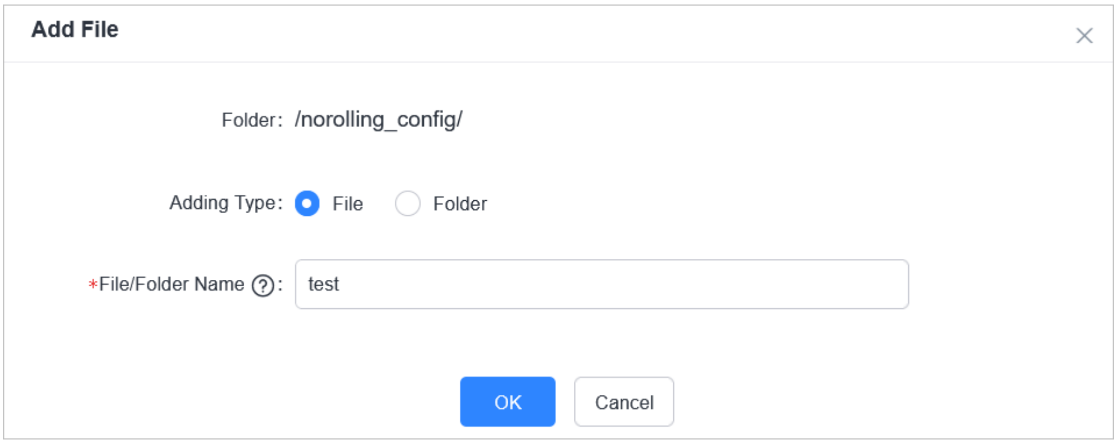
Parameter	Description
cluster.conf	The configuration file of the cluster, including the cluster name, cluster type, and machines.
kv.conf	The file that stores the values used to replace template placeholders when configurations are rendered.
machine_group.conf	The file that stores information of machine groups within a cluster.

Parameter	Description
plan.conf	The file that defines dependencies between services and configuration upgrade parameters.
services	The folder that stores configurations of each service.
shutdown_dependence.json	The shutdown dependency file.
tag.conf	The file that stores the tags used to calculate tag expressions when configurations are rendered.

3. On the **Cluster Configuration** tab, move the pointer over a folder, click the ⚙ icon next to the folder name, and then select **Add File** to add a configuration file.

   > ? **Note** You can also click **Add File** below the search box to add a file or folder to the directory.

   i. In the **Add File** dialog box, enter a file or folder name and click **OK**.



Add File

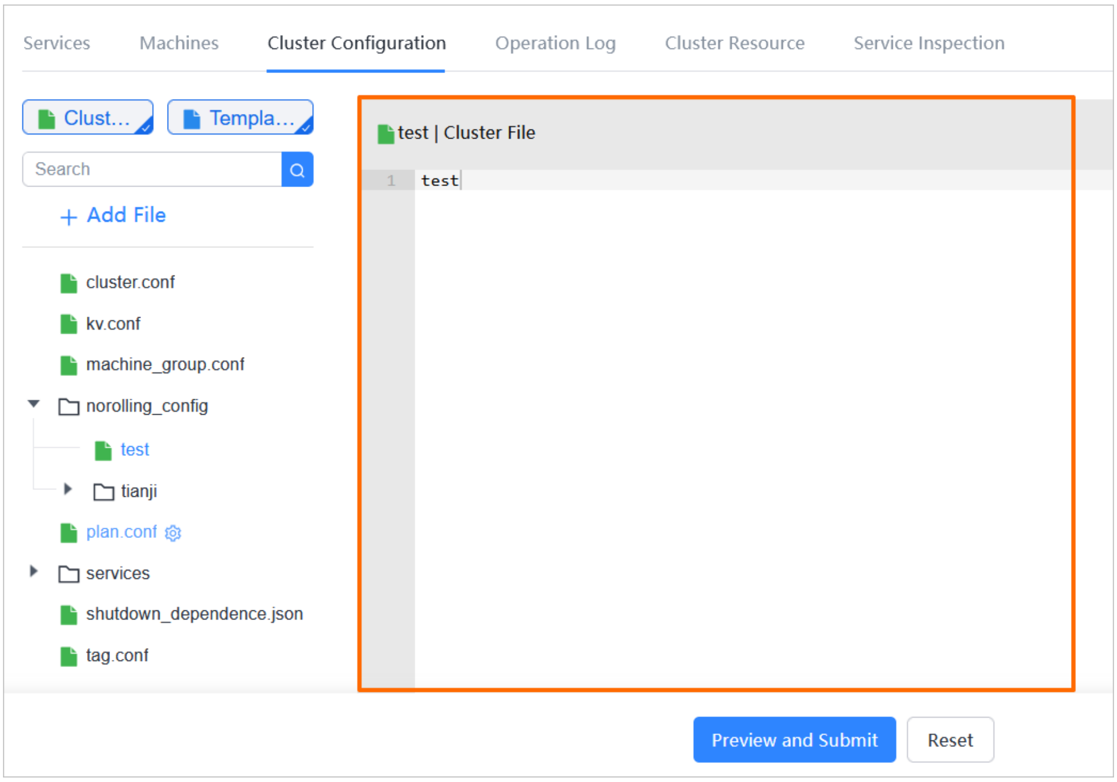
Folder: /norolling_config/

Adding Type: ● File ○ Folder

*File/Folder Name ?: test

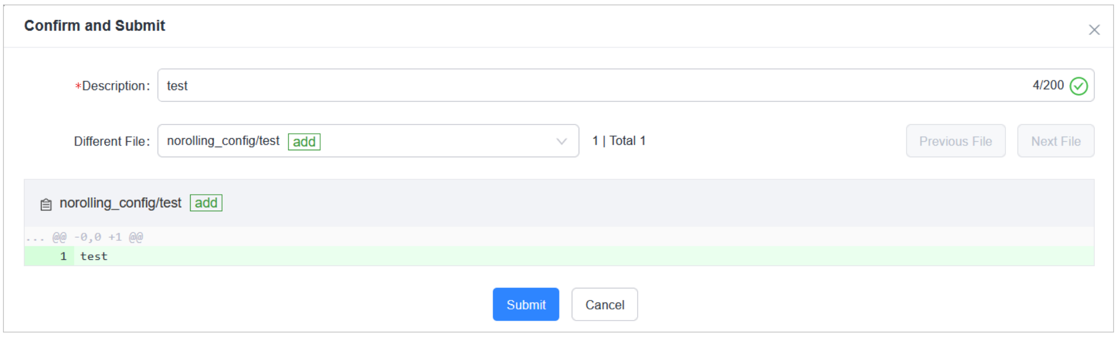
> ? **Note** After you enter a folder name and click **OK**, the folder is added.

ii. Enter configuration file information into the **Cluster File** text editor. Click **Preview and Submit**.



```
test
```

iii. In the **Confirm and Submit** dialog box, enter **Description** and click **Submit**.



*Description: test 4/200

Different File: norolling_config/test add 1 | Total 1

norolling_config/test add

```
... @@ -0,0 +1 @@
1 test
```

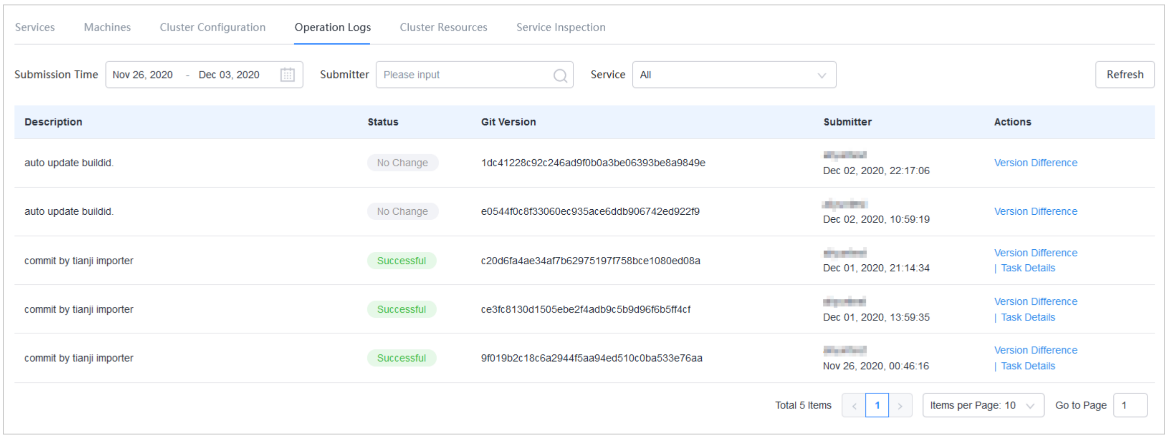
The configuration file is added. You can click the **Operation Logs** tab to view related records.

6.6.2.4.2.4. View operations logs

This topic describes how to view differences between Git versions from operation logs.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Use one of the following methods to go to the operation logs of a cluster:
   - Enter a cluster name in the search box in the upper-right corner of the page. Click **Operations** next to the found cluster. On the Cluster Details page, click the **Operation Logs** tab.
   - In the left-side navigation pane, choose **Operations > Cluster Operations**. On the **Cluster Operations** page, find a cluster and click **Operations** in the **Actions** column. On the Cluster Details page, click the **Operation Logs** tab.



Description	Status	Git Version	Submitter	Actions
auto update buildid.	No Change	1dc41228c92c246ad9f0b0a3be06393be8a9849e	[redacted] Dec 02, 2020, 22:17:06	Version Difference
auto update buildid.	No Change	e0544f0c8f33060ec935ace6ddb906742ed922f9	[redacted] Dec 02, 2020, 10:59:19	Version Difference
commit by tianji importer	Successful	c20d6fa4ae34af7b62975197f758bce1080ed08a	[redacted] Dec 01, 2020, 21:14:34	Version Difference | Task Details
commit by tianji importer	Successful	ce3fc8130d1505ebe2f4adb9c5b9d96f6b5ff4cf	[redacted] Dec 01, 2020, 13:59:35	Version Difference | Task Details
commit by tianji importer	Successful	9f019b2c18c6a2944f5aa94ed510c0ba533e76aa	[redacted] Nov 26, 2020, 00:46:16	Version Difference | Task Details

3. View the version differences on the **Operation Logs** tab.
   i. Find the operation log that you want to view and click **Version Difference** in the **Actions** column.
   ii. Set **Configuration Type** to **Show Configuration** or **Cluster Configuration**.
      - **Show Configuration**: displays the cluster configuration merged with the template configuration.
      - **Cluster Configuration**: displays the cluster configuration.
         - Cluster configuration description: Each cluster contains its dedicated configurations, such as the list of machines.
         - Template configuration description: A template that has the same configurations can be used to deploy a service to multiple clusters.
   iii. Select a basic version below **Configuration Type**. Then, a difference file is displayed in the lower part of the page.
   iv. Select a difference file from the **Difference File** drop-down list to view the content of each difference file.

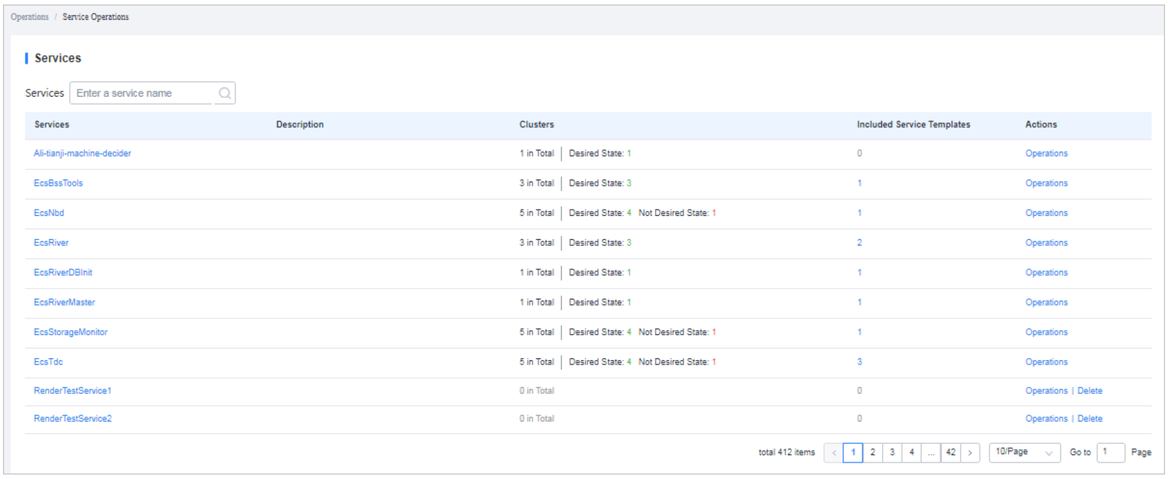
6.6.2.4.3. Service operations

6.6.2.4.3.1. View the service list

This topic describes how to view all services and their information.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Use one of the following methods to go to the service list:
   - On the **Home** page, move the pointer over the **Service Instances** section and click Details in the upper-right corner.
   - In the left-side navigation pane, choose **Operations > Service Operations**.



Services	Description	Clusters	Included Service Templates	Actions
Ali-tianji-machine-decider		1 in Total | Desired State: 1	0	Operations
EcsBssTools		3 in Total | Desired State: 3	1	Operations
EcsNbd		5 in Total | Desired State: 4 Not Desired State: 1	1	Operations
EcsRiver		3 in Total | Desired State: 3	2	Operations
EcsRiverDBInit		1 in Total | Desired State: 1	1	Operations
EcsRiverMaster		1 in Total | Desired State: 1	1	Operations
EcsStorageMonitor		5 in Total | Desired State: 4 Not Desired State: 1	1	Operations
EcsTdc		5 in Total | Desired State: 4 Not Desired State: 1	3	Operations
RenderTestService1		0 in Total	0	Operations | Delete
RenderTestService2		0 in Total	0	Operations | Delete

The following table describes the information displayed in the service list.

Parameter	Description
Service	The name of the service. Click the service name to view the service details.
Clusters	The number of clusters where the service is deployed and the cluster status.
Included Service Templates	The number of service templates that are included in the service.
Actions	○ Click **Operations** to go to the Service Details page. ○ Click **Delete** to delete the service. **Note** A service can be deleted only when the number of clusters where the service is deployed is 0.

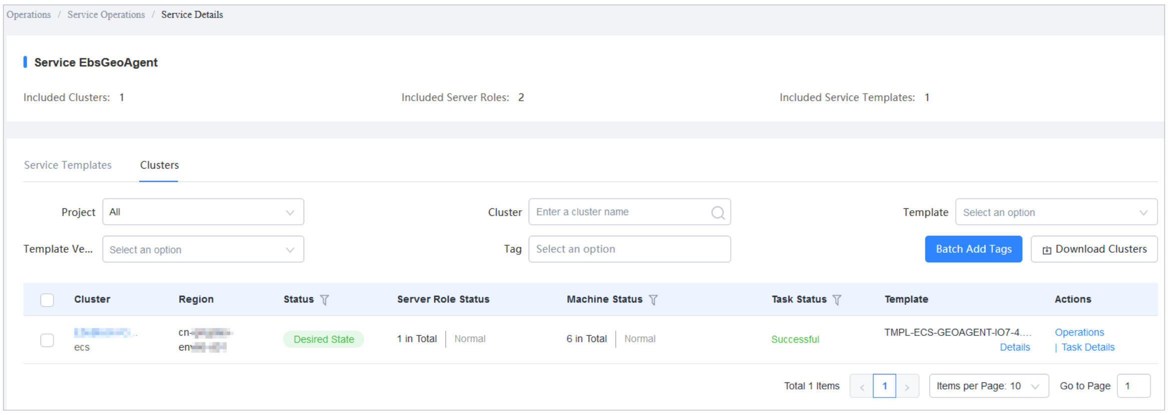
3. (Optional)Enter a service name in the search box to search for the service.

6.6.2.4.3.2. View details of a server role

This topic describes how to view details of a server role.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations** > **Service Operations**.
3. (Optional)Enter a service name in the search box to search for the service.
4. Click the service name or click **Operations** in the **Actions** column.
5. On the **Clusters** tab, click a state in the **Server Role Status** column to view the server roles included in a cluster.


Operations / Service Operations / Service Details

Service EbsGeoAgent

Included Clusters: 1 Included Server Roles: 2 Included Service Templates: 1

Service Templates Clusters

Project: All
Cluster: Enter a cluster name
Template: Select an option
Template Ve...: Select an option
Tag: Select an option

☐	Cluster	Region	Status	Server Role Status	Machine Status	Task Status	Template	Actions
☐	[redacted] ecs	cn-[redacted] en[redacted]	Desired State	1 in Total | Normal	6 in Total | Normal	Successful	TMPL-ECS-GEOAGENT-IO7-4.... Details	Operations | Task Details

Total 1 Items ‹ 1 › Items per Page: 10 Go to Page 1

6. Select the server role that you want to view.
   - Click the **Machines** tab to view details of the server role.

Parameter	Description
Machine	The machine where the server role is deployed. Click the machine name to view the machine details.
Actions	▪ Click **Metric** to view the server role, machine, and system service metrics. ▪ Click **Applications** to view application versions. ▪ Click **Terminal** to log on to the machine and perform operations. ▪ Click **Restart** to restart the server role.

   - Click the **Upgrade History** tab. Click **Details** in the **Actions** column to view details of a historical task.

6.6.2.4.3.3. Block hardware alerts

This topic describes how to block hardware alerts.

Background information

You must block hardware alerts in the following scenarios:

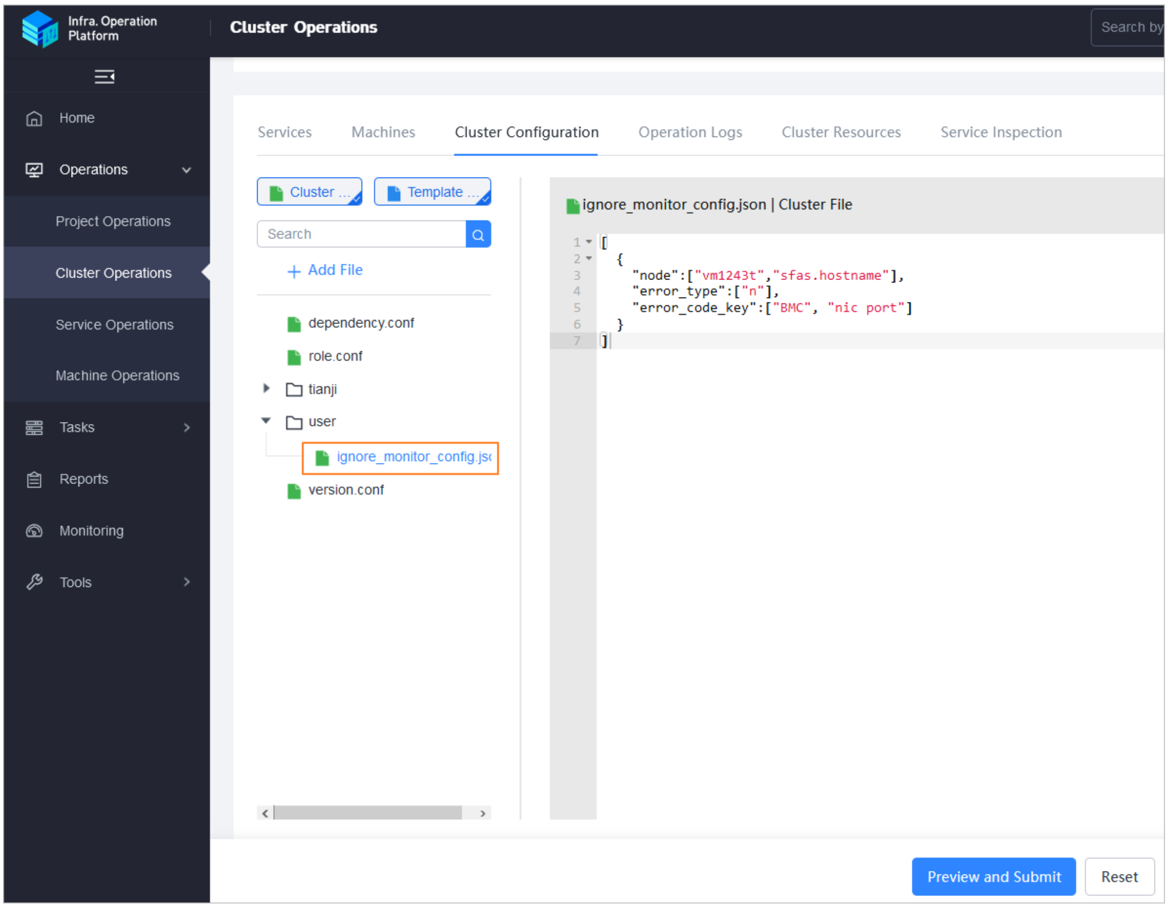
- Alerts are triggered improperly by hardware. In this case, you must block the alerts, and then cancel the block operation after no alerts are reported.
- Upgrades fail to reach the desired state due to hardware faults, and the hardware faults cannot be rectified at this time. In this case, you must block the alerts, and then cancel the block operation after the desired state is reached.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations** > **Service Operations**.
3. In the search box, enter **cruiser** to search for the cruiser service.
4. Find the cruiser service and click **Operations** in the **Actions** column.
5. Click the **Clusters** tab.

6. Click **Operations** in the **Actions** column corresponding to a cluster.

7. Click the **Cluster Configuration** tab. Open the `/user/ignore_monitor_config.json` file in **Cluster File**. Modify the configuration file.



```
[
  {
    "node":["vm1243t","sfas.hostname"],
    "error_type":["n"],
    "error_code_key":["BMC", "nic port"]
  }
]
```

The following table describes parameters in the configuration file.

Parameter	Description	Remarks
node	The name of the machine where alerts are blocked. If you want to block alerts on all machines, set the parameter to `"all"`.	◦ All the node, error_type, and error_code_key parameters are in an array format. ◦ The node parameter is required. ◦ At least one of the error_type and error_code_key parameters is required.
error_type	The type of the fault that triggers alerts. Valid values: ◦ 0: LogicDrive fault ◦ 1: hard disk fault ◦ 2: memory fault	

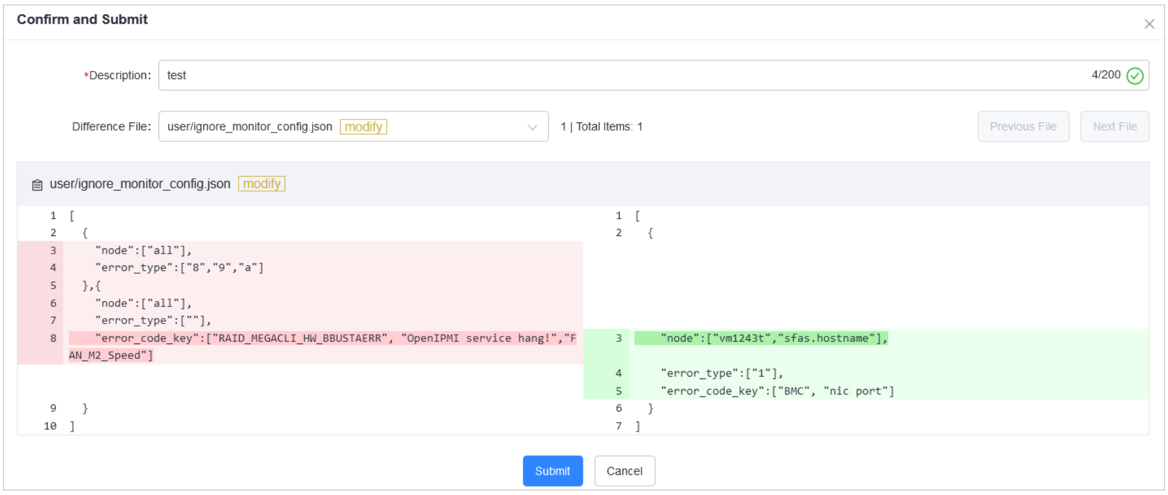
Parameter	Description	Remarks
error_code_key	The keyword used to block alerts. The keyword can be the error code or information.	

Example:

```
{
  "node":["vm1243t", "sfas.hostname"],
  "error_type":["1"]
  "error_code_key":["BMC", "nic port"]
 }
```

In the preceding example, the alerts caused by hard disk faults are blocked on the vm1243t and sfas.hostname machines. The error information includes BMC and NIC port.

8. Click **Preview and Submit**.
9. In the **Confirm and Submit** dialog box, enter the description and click **Submit**.



Confirm and Submit

*Description: test 4/200

Difference File: user/ignore_monitor_config.json modify 1 | Total Items: 1

user/ignore_monitor_config.json modify

```
[
  {
    "node":["all"],
    "error_type":["8","9","a"]
  },{
    "node":["all"],
    "error_type":[""],
    "error_code_key":["RAID_MEGACLI_HW_BBUSTAERR", "OpenIPMI service hang!","FAN_M2_Speed"]
  }
]
```

```
[
  {
    "node":["vm1243t","sfas.hostname"],
    "error_type":["1"],
    "error_code_key":["BMC", "nic port"]
  }
]
```

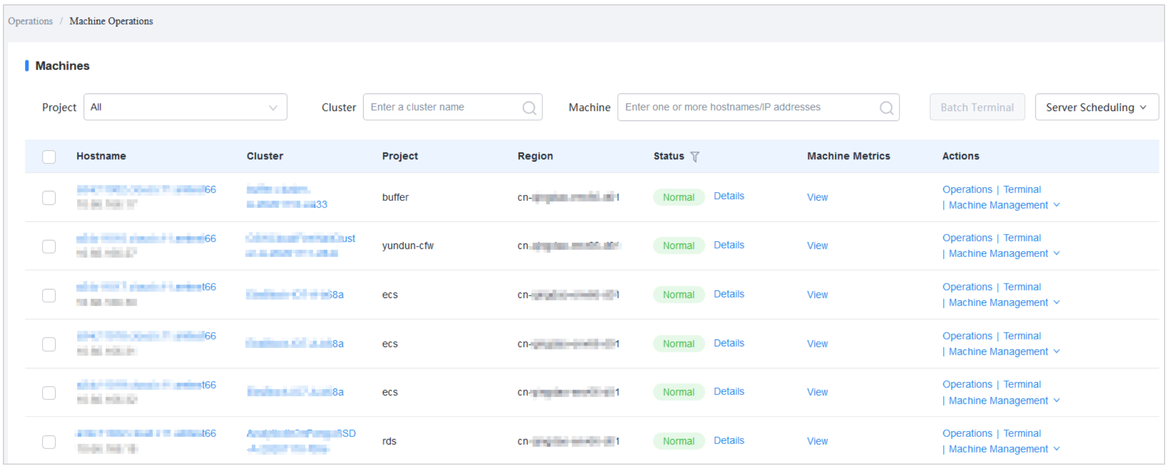
10. Click the **Operation Logs** tab to view related records.

6.6.2.4.4. Machine operations

This topic describes how to view the statistics of all machines.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Use one of the following methods to go to the machine list:
   - On the **Home** page, move the pointer over the **Machine** section and click Details in the upper-right corner.
   - In the left-side navigation pane, choose **Operations > Machine Operations**.
3. (Optional)Select a project from the drop-down list or enter a cluster or machine name to search for the machine.



Operations / Machine Operations

Machines

Project All | Cluster Enter a cluster name | Machine Enter one or more hostnames/IP addresses | Batch Terminal | Server Scheduling

□	Hostname	Cluster	Project	Region	Status	Machine Metrics	Actions
□	[redacted]	[redacted]	buffer	[redacted]	Normal Details	View	Operations | Terminal | Machine Management
□	[redacted]	[redacted]	yundun-cfw	[redacted]	Normal Details	View	Operations | Terminal | Machine Management
□	[redacted]	[redacted]	ecs	[redacted]	Normal Details	View	Operations | Terminal | Machine Management
□	[redacted]	[redacted]	ecs	[redacted]	Normal Details	View	Operations | Terminal | Machine Management
□	[redacted]	[redacted]	ecs	[redacted]	Normal Details	View	Operations | Terminal | Machine Management
□	[redacted]	[redacted]	rds	[redacted]	Normal Details	View	Operations | Terminal | Machine Management

Parameter	Description
Hostname	The hostname of the machine. Click a hostname to go to the Machine Details page.
Cluster	The cluster where the machine is deployed. Click a cluster name to go to the Cluster Details page.
Status	The status of the machine. Click the ▽ icon to filter machines. Click **Details**. Then, the **Status Details of Machine** dialog box appears.
Machine Metrics	The metrics of the machine. Click **View**. Then, the **Metrics** dialog box appears. Metrics are displayed on the **Server Role Metric**, **Machine Metrics**, and **System Service Monitor** tabs. You can view the status and update time of each metric. Enter a keyword in one of the search boxes in the upper-right corner to search for a server role or metric. You can also select the status in the upper-left corner to filter metrics.
Actions	○ Click **Operations** to go to the Machine Details page. ○ Click **Terminal** to log on to the machine and perform operations. You can select multiple machines and then click **Batch Terminal** in the upper-right corner to log on to multiple machines at a time. ○ Click **Machine Management** to perform an out-of-band restart operation on the machine.

6.6.2.5. View tasks

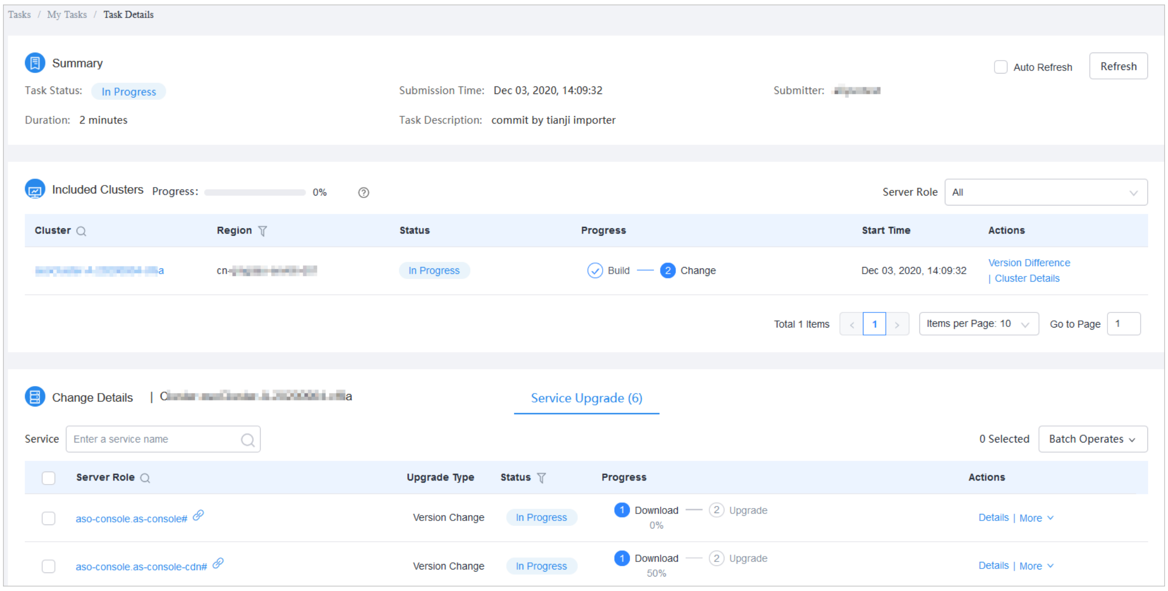
This topic describes how to view the submitted tasks and their statuses.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Use one of the following methods to go to the task list:

  - In the left-side navigation pane, choose **Tasks** > **My Tasks**.
  - In the left-side navigation pane, choose **Tasks** > **Related Tasks**.

3. (Optional) Click the ▽ icon in the **Status** column to filter tasks.
4. Find the task that you want to view and click the task name or **Details** in the **Actions** column.
5. View the status and progress of each cluster and server role on the **Task Details** page.



Tasks / My Tasks / Task Details

Summary

□ Auto Refresh Refresh

Task Status: In Progress

Submission Time: Dec 03, 2020, 14:09:32

Submitter: [redacted]

Duration: 2 minutes

Task Description: commit by tianji importer

Included Clusters Progress: 0%

Server Role: All

Cluster	Region	Status	Progress	Start Time	Actions
[redacted]a	cn-[redacted]	In Progress	✓ Build — 2 Change	Dec 03, 2020, 14:09:32	Version Difference | Cluster Details

Total 1 Items ‹ 1 › Items per Page: 10 Go to Page 1

Change Details | C[redacted]a

Service Upgrade (6)

Service: Enter a service name

0 Selected Batch Operates

□	Server Role	Upgrade Type	Status	Progress	Actions
□	aso-console.as-console#	Version Change	In Progress	1 Download — 2 Upgrade 0%	Details | More
□	aso-console.as-console-cdn#	Version Change	In Progress	1 Download — 2 Upgrade 50%	Details | More

6.6.2.6. Reports

6.6.2.6.1. View reports

This topic describes how to view report data.

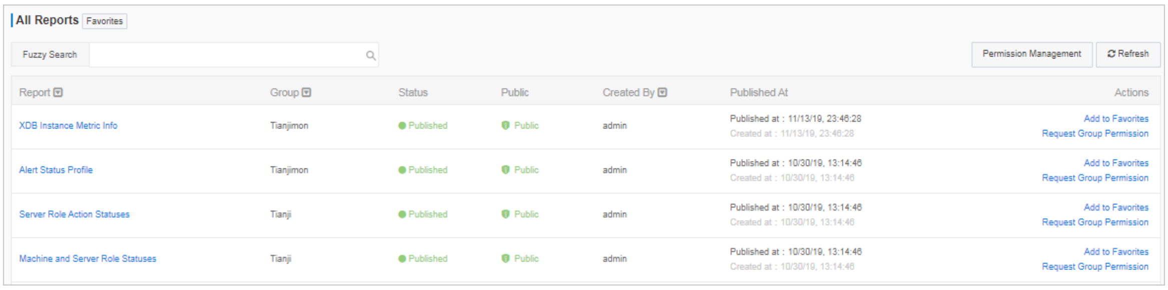
Context

The following reports are available in the Apsara Infrastructure Management Framework console:

- System reports: include default and common reports in the system.
- All reports: include system reports and custom reports.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, click **Reports**. On the Reports page, click **Go** to go to the All Reports page.



All Reports Favorites

Fuzzy Search

Permission Management Refresh

Report	Group	Status	Public	Created By	Published At	Actions
XDB Instance Metric Info	Tianjimon	● Published	Public	admin	Published at : 11/13/19, 23:46:28 Created at : 11/13/19, 23:46:28	Add to Favorites Request Group Permission
Alert Status Profile	Tianjimon	● Published	Public	admin	Published at : 10/30/19, 13:14:46 Created at : 10/30/19, 13:14:46	Add to Favorites Request Group Permission
Server Role Action Statuses	Tianji	● Published	Public	admin	Published at : 10/30/19, 13:14:46 Created at : 10/30/19, 13:14:46	Add to Favorites Request Group Permission
Machine and Server Role Statuses	Tianji	● Published	Public	admin	Published at : 10/30/19, 13:14:46 Created at : 10/30/19, 13:14:46	Add to Favorites Request Group Permission

The following table describes information about reports.

Parameter	Description
Report	The name of the report. Move the pointer over the down arrow next to Report and search by report name.
Group	The group to which the report belongs. Move the pointer over the down arrow next to Group and search by group name.
Status	Specifies whether the report is published. ○ Published ○ Not Published
Public	Specifies whether the report is public. ○ Public: visible to all logon users. ○ Private: visible only to the current logon user.
Created By	The person who creates the report.
Published At	The time when the report is created and published.
Actions	○ Click **Add to Favorites** to add the report to your favorites. Then, you can view the report by choosing **Reports > Favorites** in the top navigation bar. ○ Click **Request Group Permission** to go to the Operation Administrator Manager (OAM) console. You can then configure groups and permissions. For more information, see *OAM* in *Operations and Maintenance Guide*.

3. (Optional)Enter a report name in the search box to search for the report.
4. Click the report name to go to the corresponding report details page.For more information about reports, see Appendix.

6.6.2.6.2. Add a report to favorites

This topic describes how to add frequently used reports to favorites. Then, you can find them on the Home or Favorites page.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, click **Reports**. On the Reports page, click **Go** to go to the All Reports page.
3. (Optional)Search for a report in the search box.
4. Click **Add to Favorites** in the **Actions** column corresponding to the report.
5. In the **Add to Favorites** dialog box, enter tags for the report.

6. Click **Add to Favorites**.

6.6.2.7. Monitoring center

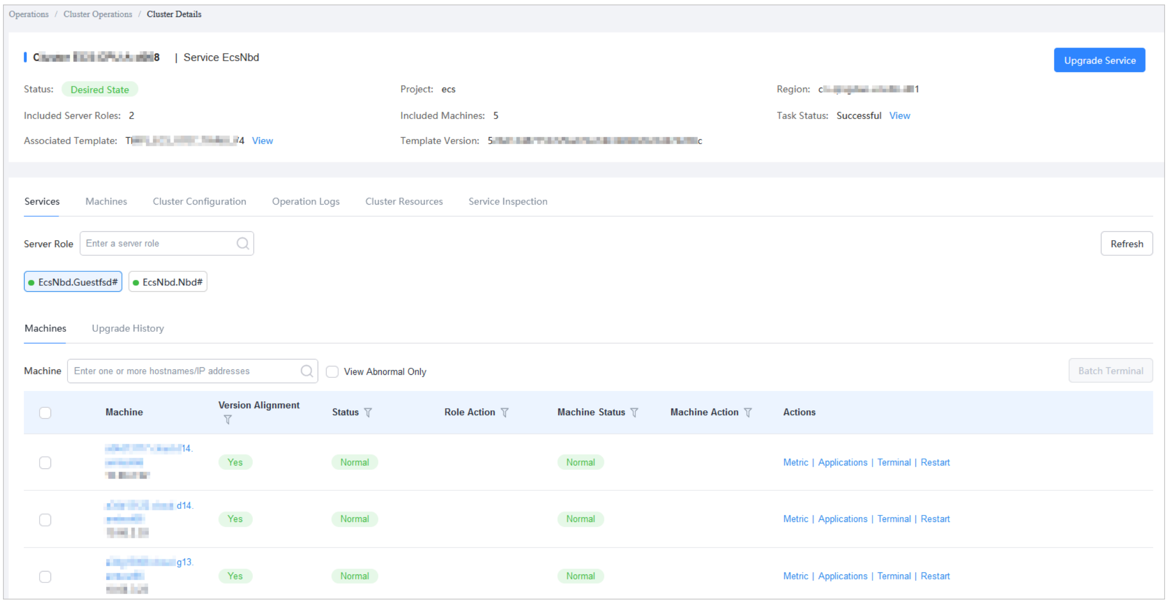
You can view the alert status, alert rules, and alert history in the monitoring center.

6.6.2.7.1. View the status of a metric

This topic describes how to view the status of a metric.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations > Service Operations**.
3. (Optional)Enter a service name in the search box to search for the service.
4. Click Operations in the Actions column. On the Service Details page, click the **Clusters** tab.
5. Find the cluster that you want to view and click **Operations** in the **Actions** column.
6. On the **Services** tab, select a server role and click **Metric** in the **Actions** column corresponding to a machine to view the server role, machine, and system service metrics.



Operations / Cluster Operations / Cluster Details

C[redacted]8 | Service EcsNbd

Upgrade Service

Status: Desired State

Project: ecs

Region: c[redacted]1

Included Server Roles: 2

Included Machines: 5

Task Status: Successful View

Associated Template: T[redacted]4 View

Template Version: 5[redacted]c

Services | Machines | Cluster Configuration | Operation Logs | Cluster Resources | Service Inspection

Server Role: Enter a server role

Refresh

● EcsNbd.Guestfsd# ● EcsNbd.Nbd#

Machines | Upgrade History

Machine: Enter one or more hostnames/IP addresses

□ View Abnormal Only

Batch Terminal

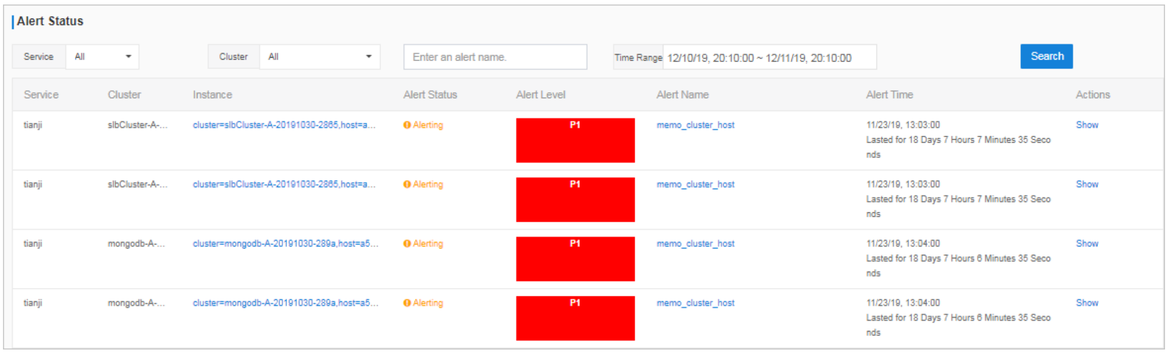
□	Machine	Version Alignment	Status	Role Action	Machine Status	Machine Action	Actions
□	[redacted]14. [redacted] [redacted]	Yes	Normal		Normal		Metric | Applications | Terminal | Restart
□	[redacted]d14. [redacted] [redacted]	Yes	Normal		Normal		Metric | Applications | Terminal | Restart
□	[redacted]g13. [redacted] [redacted]	Yes	Normal		Normal		Metric | Applications | Terminal | Restart

6.6.2.7.2. View the alert status

This topic describes how to view the alerts related to different services and the alert details.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, click **Monitoring**. On the Monitoring page, click **Go** to go to the Alert Status page.
3. In the top navigation bar, choose **Monitoring > Alert Status**.



Alert Status

Service All | Cluster All | Enter an alert name. | Time Range 12/10/19, 20:10:00 ~ 12/11/19, 20:10:00 | Search

Service	Cluster	Instance	Alert Status	Alert Level	Alert Name	Alert Time	Actions
tianji	slbCluster-A-...	cluster=slbCluster-A-20191030-2865,host=a...	Alerting	P1	memo_cluster_host	11/23/19, 13:03:00 Lasted for 18 Days 7 Hours 7 Minutes 35 Seconds	Show
tianji	slbCluster-A-...	cluster=slbCluster-A-20191030-2865,host=a...	Alerting	P1	memo_cluster_host	11/23/19, 13:03:00 Lasted for 18 Days 7 Hours 7 Minutes 35 Seconds	Show
tianji	mongodb-A-...	cluster=mongodb-A-20191030-289a,host=a5...	Alerting	P1	memo_cluster_host	11/23/19, 13:04:00 Lasted for 18 Days 7 Hours 6 Minutes 35 Seconds	Show
tianji	mongodb-A-...	cluster=mongodb-A-20191030-289a,host=a5...	Alerting	P1	memo_cluster_host	11/23/19, 13:04:00 Lasted for 18 Days 7 Hours 6 Minutes 35 Seconds	Show

4. (Optional)Search for an alert by service name, cluster name, alert time range, or alert name.
5. View alert details on the **Alert Status** page. The following table describes the related parameters.

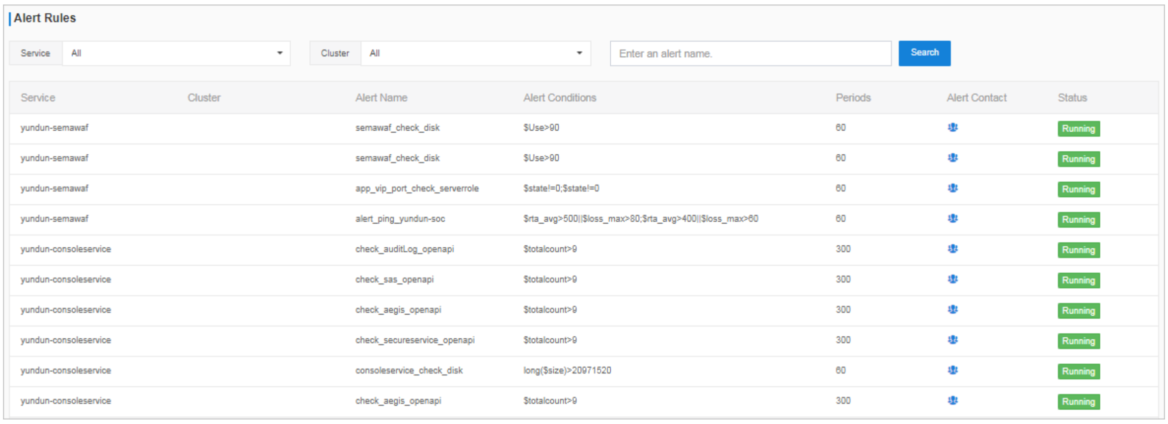
Parameter	Description
Service	The name of the service.
Cluster	The name of the cluster where the service is deployed.
Instance	The name of the monitored instance. Click the name of an instance to view the alert history of the instance.
Alert Status	The state of the alert. Two alert states are available, which are **Normal** and **Alerting**.
Alert Level	The level of the alert. Alerts are divided into five levels in descending order of severity: ○ P0: an alert that has been cleared ○ P1: an urgent alert ○ P2: a major alert ○ P3: a minor alert ○ P4: a reminder alert
Alert Name	The name of the alert. Click the name of an alert to view alert rule details.
Alert Time	The time when the alert is triggered and how long the alert lasts.
Actions	The available operations. Click **Show** to view the data before and after the alert time.

6.6.2.7.3. View alert rules

This topic describes how to view the alert rules of a service.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, click **Monitoring**. On the Monitoring page, click **Go** to go to the Alert Status page.
3. In the top navigation bar, choose **Monitoring > Alert Rules**.



Alert Rules

Service	Cluster	Alert Name	Alert Conditions	Periods	Alert Contact	Status
yundun-semawaf		semawaf_check_disk	$Use>90	60	👥	Running
yundun-semawaf		semawaf_check_disk	$Use>90	60	👥	Running
yundun-semawaf		app_vip_port_check_serverrole	$state!=0;$state!=0	60	👥	Running
yundun-semawaf		alert_ping_yundun-soc	$rta_avg>500\|\|$loss_max>80;$rta_avg>400\|\|$loss_max>60	60	👥	Running
yundun-consoleservice		check_auditLog_openapi	$totalcount>9	300	👥	Running
yundun-consoleservice		check_sas_openapi	$totalcount>9	300	👥	Running
yundun-consoleservice		check_aegis_openapi	$totalcount>9	300	👥	Running
yundun-consoleservice		check_secureservice_openapi	$totalcount>9	300	👥	Running
yundun-consoleservice		consoleservice_check_disk	long($size)>20971520	60	👥	Running
yundun-consoleservice		check_aegis_openapi	$totalcount>9	300	👥	Running

4. (Optional)Search for alert rules by service name, cluster name, or alert name.
5. View alert rules on the **Alert Rules** page. The following table describes the related parameters.

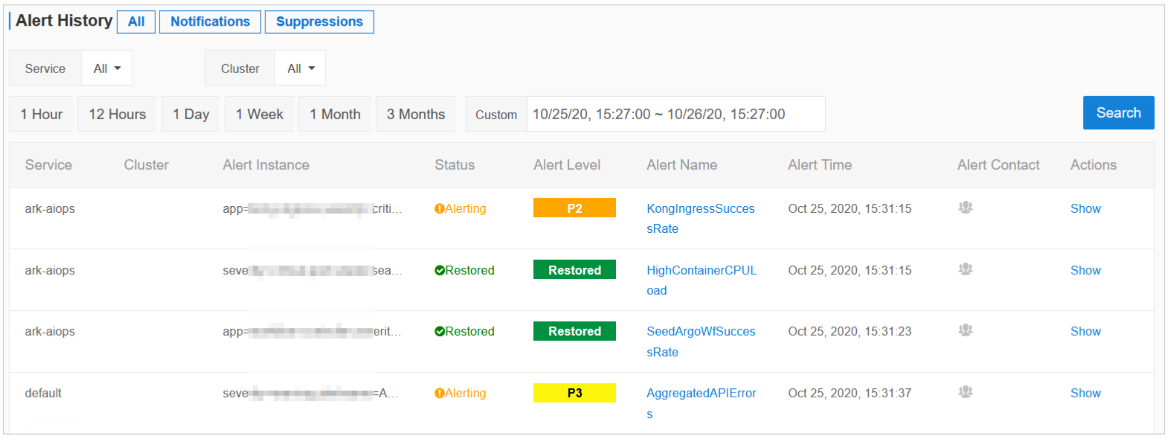
Parameter	Description
Service	The name of the service.
Cluster	The name of the cluster where the service is deployed.
Alert Name	The name of the alert.
Alert Conditions	The conditions that trigger the alert.
Periods	The frequency at which the alert rule is executed.
Alert Contact	The groups and members to notify when the alert is triggered.
Status	The status of the alert rule. ○ **Running**: Click it to stop the alert rule. ○ **Stopped**: Click it to execute the alert rule.

6.6.2.7.4. View the alert history

This topic describes how to view the historical alerts related to different services and the alert details.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, click **Monitoring**. On the Monitoring page, click **Go** to go to the Alert Status page.
3. In the top navigation bar, choose **Monitoring > Alert History**.



Alert History | All | Notifications | Suppressions

Service: All ▾ Cluster: All ▾

1 Hour | 12 Hours | 1 Day | 1 Week | 1 Month | 3 Months | Custom 10/25/20, 15:27:00 ~ 10/26/20, 15:27:00 | Search

Service	Cluster	Alert Instance	Status	Alert Level	Alert Name	Alert Time	Alert Contact	Actions
ark-aiops		app=[redacted]criti...	Alerting	P2	KongIngressSuccessRate	Oct 25, 2020, 15:31:15		Show
ark-aiops		seve[redacted]sea...	Restored	Restored	HighContainerCPULoad	Oct 25, 2020, 15:31:15		Show
ark-aiops		app=[redacted]erit...	Restored	Restored	SeedArgoWfSuccessRate	Oct 25, 2020, 15:31:23		Show
default		seve[redacted]=A...	Alerting	P3	AggregatedAPIErrors	Oct 25, 2020, 15:31:37		Show

4. (Optional)Search for an alert by service name, cluster name, alert cycle, or alert time range.
5. View the alert history on the **Alert History** page. The following table describes the related parameters.

Parameter	Description
Service	The name of the service to which the alert belongs.
Cluster	The name of the cluster where the service is deployed.
Alert Instance	The name of the instance where the alert is triggered.
Status	The state of the alert. Two alert states are available, which are **Normal** and **Alerting**.
Alert Level	The level of the alert. Alerts are divided into five levels in descending order of severity: ○ P0: an alert that has been cleared ○ P1: an urgent alert ○ P2: a major alert ○ P3: a minor alert ○ P4: a reminder alert
Alert Name	The name of the alert. Click the name of an alert to view alert rule details.
Alert Time	The time when the alert is triggered.
Alert Contact	The groups and members to notify when the alert is triggered.
Actions	The available operations. Click **Show** to view the data before and after the alert time.

6.6.2.8. Tools

6.6.2.8.1. Use machine operations tools

This topic describes how to use machine operations tools in typical scenarios.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Tools > Operation Tools > Machine Tools**. On the Machine Tools page, click **Go** to go to the Operation Tools page.
3. Select a scenario from the Operation Scene drop-down list.

Scenario	Description	Actions
Scene 1. NC Scale-out (with existing machines)	Scales out an SRG of the worker type.	Select a cluster from the Target Cluster drop-down list and an SRG from the Target SRG drop-down list. Select the machines to scale out in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.
Scene 2. Host Scale-out (with existing machines)	Scales out DockerHost#Buffer of a cluster.	Select a cluster from the Target Cluster drop-down list. Select the machines to scale out in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.
Scene 3. NC Scale-in	Scales in an SRG of the worker type.	Select a cluster from the Target Cluster drop-down list and an SRG from the Target SRG drop-down list. Select the machines to scale in in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.
Scene 4. Host Scale-in	Scales in DockerHost#Buffer of a cluster.	Select a cluster from the Target Cluster drop-down list. Select the machines to scale in in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.

Scenario	Description	Actions
Scene 5. VM Migration	Migrates virtual machines (VMs) from a host to another host.	Select a source host from the Source Host drop-down list and a destination host from the Destination Host drop-down list. Select the VMs to migrate in the left-side section, click Select> to add them to the right-side section, and then click **Submit**. In the message that appears, click **Confirm**.
Scene 6. Host Switching	Switches a standby host to the primary host.	Select a source host from the Source Host drop-down list and a destination host from the Destination Host drop-down list. Click **Submit**. In the message that appears, click **Confirm**.

6.6.2.8.2. Shut down a data center

This topic describes how to shut down up to 25 machines within all clusters of a data center in scenarios such as vehicle-mounted devices.

Prerequisites

- The total number of machines within all clusters of a data center cannot exceed 25.
- Your browser is connected with the machines on which Apsara Infrastructure Management Framework is deployed over a smooth network. If a proxy is required to log on to the Apsara Infrastructure Management Framework console, the proxy is not configured on a machine that you want to shut down.
- Your browser remains active while the machines are being shut down.
- Data related to operations such as scaling is not retained within the default cluster before the machines are shut down.

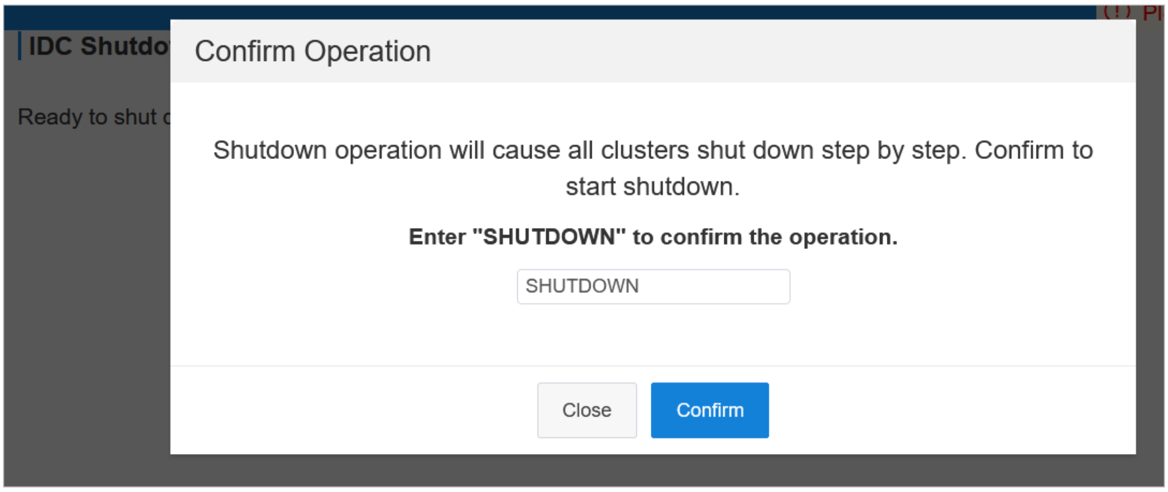
Context

When you shut down a data center, business clusters are shut down first, and then the base cluster is shut down.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Tools > IDC Shutdown**. In the right-side workspace, click **Go**.
3. On the **IDC Shutdown** page, click **Start Shutdown**.
4. In the **Confirm Operation** message, enter *SHUTDOWN* and click **Confirm**.

> Warning
>
> - The data center shutdown operation shuts down all services and machines and thus cause business interruption.
> - Backend services must communicate with the frontend shutdown page during the data center shutdown process. Do not close the shutdown page until the shutdown is complete.



IDC Shutdo

Ready to shut d

(!) Pl

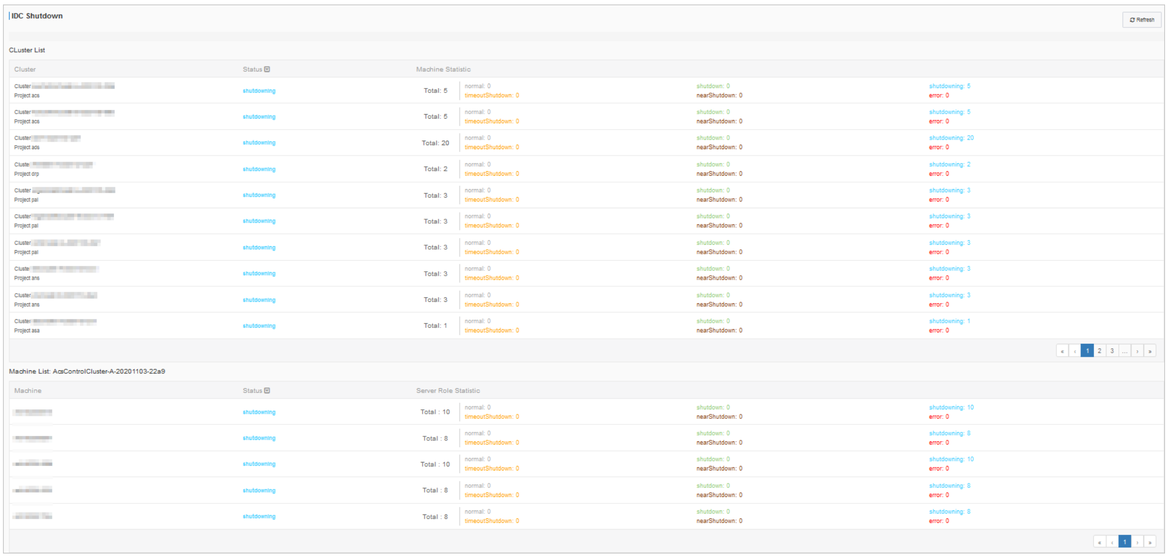
Confirm Operation

Shutdown operation will cause all clusters shut down step by step. Confirm to start shutdown.

Enter "SHUTDOWN" to confirm the operation.

SHUTDOWN

5. View the data center shutdown progress and the statuses of clusters, machines, and server roles.



IDC Shutdown

CLuster List

Cluster	Status	Machine Statistic			
Cluster [redacted] Project acs	shutdowning	Total: 5	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 5 error: 0
Cluster [redacted] Project acs	shutdowning	Total: 5	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 5 error: 0
Cluster [redacted] Project ads	shutdowning	Total: 20	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 20 error: 0
Cluste [redacted] Project drp	shutdowning	Total: 2	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 2 error: 0
Cluster [redacted] Project pal	shutdowning	Total: 3	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 3 error: 0
Cluster [redacted] Project pal	shutdowning	Total: 3	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 3 error: 0
Cluster [redacted] Project pal	shutdowning	Total: 3	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 3 error: 0
Cluste [redacted] Project ans	shutdowning	Total: 3	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 3 error: 0
Cluster [redacted] Project ans	shutdowning	Total: 3	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 3 error: 0
Cluster [redacted] Project asa	shutdowning	Total: 1	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 1 error: 0

Machine List: AcsControlCluster-A-20201103-22a9

Machine	Status	Server Role Statistic			
[redacted]	shutdowning	Total : 10	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 10 error: 0
[redacted]	shutdowning	Total : 8	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 8 error: 0
[redacted]	shutdowning	Total : 10	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 10 error: 0
[redacted]	shutdowning	Total : 8	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 8 error: 0
[redacted]	shutdowning	Total : 8	normal: 0 timeoutShutdown: 0	shutdown: 0 nearShutdown: 0	shutdowning: 8 error: 0

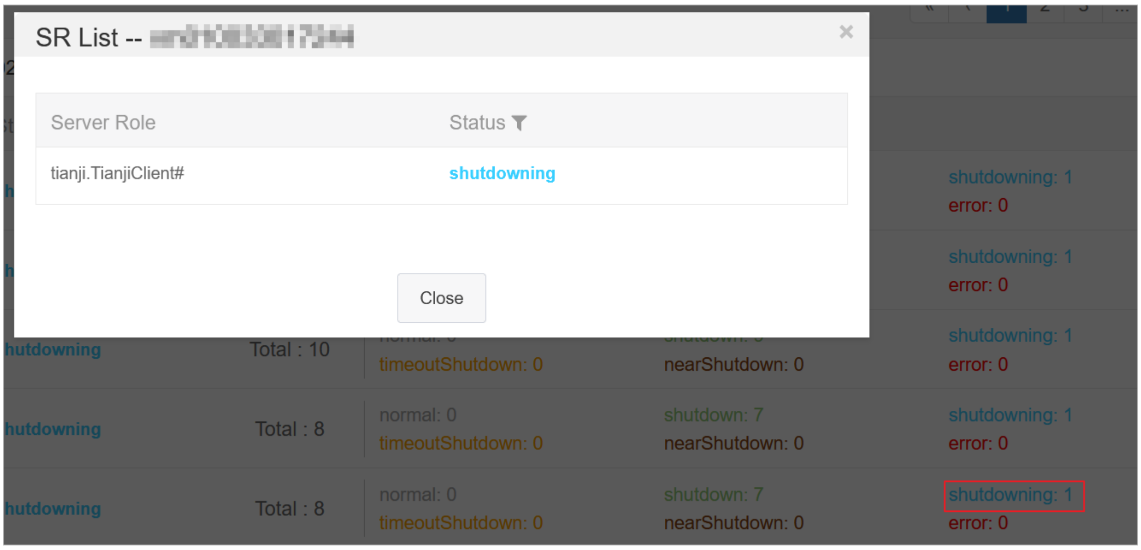
It takes a long time to shut down all clusters and machines within an environment. You can view the shutdown progress on the **IDC Shutdown** page. The following statuses are available for clusters, machines, and server roles:

- **normal**: A cluster, machine, or server role is running normally.
- **shutdown**: A cluster, machine, or server role is shut down.
- **shutdowning**: A cluster, machine, or server role is being shut down.
- **timeoutShutdown**: The shutdown of a cluster, machine, or server role timed out.
- **nearShutdown**: A cluster, machine, or server role is about to be shut down.

- **error**: An error occurred while a cluster, machine, or server role is being shut down.

You can perform the following operations:

- View the data center shutdown progress: In the upper part of the **IDC Shutdown** page, view the data center shutdown progress.
- View the cluster status: In the **Cluster List** section, view the status of each cluster, the total number of machines within each cluster, and the number of machines in each state.
- View the machine status: In the **Cluster List** section, click a state corresponding to a cluster. In the **Machine List** section, view all machines in the corresponding state within the cluster, the total number of server roles on each machine, and the number of server roles in each state.
- View the server role status: In the **Machine List** section, click a state corresponding to a machine. In the **SR List--xxx** message, view all server roles in the corresponding state on the machine.



SR List -- [redacted]

Server Role	Status
tianji.TianjiClient#	shutdowning

> **Note**
>
> In the left-side navigation pane, click **Go**. On the **All Reports** page, enter the entire or part of **Machine Power On or Off Statuses of Clusters** in the **Fuzzy Search** search box. In the search results, click **Machine Power On or Off Statuses of Clusters** to view the status of each server role.

- Filter clusters or machines: In the **Cluster List** or **Machine List** section, click the filter icon in the **Status** column and select a state to filter all clusters or machines in the corresponding state.
- Refresh data: Click **Refresh** in the upper-right corner to refresh data.

If all clusters in the **Cluster List** section are displayed in the **shutdown** state, the data center shutdown operation succeeds. After the base cluster is shut down, the OPS1 server is also shut down. Then, the Apsara Infrastructure Management Framework console is inaccessible.

6. After all base machines are shut down and inaccessible, go to the data center and confirm that all machines are powered off.

What's next

If you want to use the machines in the future, power on each machine one by one in the data center and wait until all services reach the desired state.

6.6.2.8.3. View the clone progress

This topic describes how to go to the OS Provision console (Corner Stone) and check the progress, status, and errors about machine installation.

Prerequisites

The username and password used to log on to the OP Provision console are obtained from delivery personnel.

Context

Apsara Infrastructure Management Framework provides a quick entry to the OS Provision console, which allows you to view details about machine installation. You can then obtain the progress and status about machine installation and then locate the installation faults.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Tools > Clone Progress**.
3. On the logon page of the OS Provision console, enter **Username** and **Password**, and then click **Submit**.

6.6.2.9. Appendix

6.6.2.9.1. Project component info report

This report displays the name and status for each type of project components, including services, server roles, and machines.

Item	Description
Project	The project name.
Cluster	The name of a cluster in the project.
Service	The name of a service in the cluster.
Server Role	The name of a server role in the service.
Server Role Status	The running status of the server role on the machine.
Server Role Action	The action that the server role performs on the machine. Data is available only when Apsara Infrastructure Management Framework asks the server role to perform certain actions, such as rolling and restart actions.
Machine Name	The hostname of the machine.
IP	The IP address of the machine.
Machine Status	The running status of the machine.

Item	Description
Machine Action	The action that Apsara Infrastructure Management Framework asks the machine to perform, such as the clone action.

6.6.2.9.2. IP list

This report displays the IP addresses of physical machines and Docker applications.

IP List of Physical Machines

Item	Description
Project	The project name.
Cluster	The cluster name.
Machine Name	The hostname of the machine.
IP	The IP address of the machine.

IP List of Docker Applications

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Machine Name	The hostname of the machine.
Docker Host	The Docker hostname.
Docker IP	The Docker IP address.

6.6.2.9.3. Machine info report

This report displays the statuses of machines and server roles on the machines.

Machine Status

Displays all the machines currently managed by Apsara Infrastructure Management Framework and their corresponding statuses. In the **Global Filter** section at the top of the page, select the project, cluster, and machine from the **project**, **cluster**, and **machine** drop-down lists, and then click **Filter** on the right to filter the data.

Item	Description
Machine Name	The machine name.
IP	The IP address of the machine.
Machine Status	The machine status.
Machine Action	The action currently performed by the machine.
Machine Action Status	The action status.
Status Description	The description about the machine status.

Expected Server Role List

Select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The machine name.
Server Role	The name of the expected server role on the machine.

Abnormal Monitoring Status

Select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The machine name.
Monitored Item	The name of the monitored item.
Level	The level of the monitored item.
Description	The description of the monitored item contents.
Updated At	The updated time of the monitored item.

Server Role Version and Status on Machine

Select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The machine name.
Server Role	The server role name.
Server Role Status	The status of the server role.

Item	Description
Target Version	The expected version of the server role on the machine.
Current Version	The current version of the server role on the machine.
Status Description	The description about the status.
Error Message	The exception message of the server role.

Monitoring Status

Select a row in the **Machine Status** section to display the corresponding information in this list.

Item	Description
Machine Name	The machine name.
Server Role	The server role name.
Monitored Item	The name of the monitored item.
Level	The level of the monitored item.
Description	The description of the monitored item contents.
Updated At	The updated time of the monitored item.

6.6.2.9.4. Rolling info report

This report displays the running and completed rolling tasks and the task-related status.

Choose a rolling action

This list only displays the running rolling tasks. If no rolling task is running, no data is available in the list.

Item	Description
Cluster	The cluster name.
Git Version	The version of change that triggers the rolling task.
Description	The description about the change entered by a user when the user submits the change.
Start Time	The start time of the rolling task.
End Time	The end time of the rolling task.
Submitted By	The ID of the user who submits the change.
Rolling Task Status	The current status of the rolling task.

Item	Description
Submitted At	The time when the change is submitted.

Server Role in Job

Select a rolling task in the **Choose a rolling action** section to display the rolling status of server roles related to the selected task. If no rolling task is selected, the server role statuses of all historical rolling tasks are displayed.

Item	Description
Server Role	The server role name.
Server Role Status	The rolling status of the server role.
Error Message	The exception message of the rolling task.
Git Version	The version of change to which the rolling task belongs.
Start Time	The start time of the rolling task.
End Time	The end time of the rolling task.
Approve Rate	The proportion of machines that have the rolling task approved by the decider.
Failure Rate	The proportion of machines that have the rolling task failed.
Success Rate	The proportion of machines that have the rolling task succeeded.

Server Role Rolling Build Information

The source version and target version of each application under the server role in the rolling process.

Item	Description
App	The name of the application that requires rolling in the server role.
Server Role	The server role to which the application belongs.
From Build	The version before the upgrade.
To Build	The version after the upgrade.

Server Role Statuses on Machines

Select a server role in the **Server Role in Job** section to display the deployment status of this server role on the machine.

Item	Description
Machine Name	The name of the machine on which the server role is deployed.
Expected Version	The target version of the rolling.
Actual Version	The current version.
State	The status of the server role.
Action Name	The Apsara Infrastructure Management Framework action currently performed by the server role.
Action Status	The action status.

6.6.2.9.5. Machine RMA approval pending list

Some Apsara Infrastructure Management Framework actions (such as restart) on machines and server roles can be triggered by users, but this type of actions must be reviewed and approved. This report is used to process the actions that must be reviewed and approved.

Machine

Displays the basic information of pending approval machines.

Item	Description
Project	The project name.
Cluster	The cluster name.
Hostname	The hostname of the machine.
IP	The IP address of the machine.
State	The running status of the machine.
Action Name	The action on the machine.
Action Status	The status of the action on the machine.
Actions	The approval button.

Machine Serverrole

Displays the information of server roles on the pending approval machines.

Item	Description
Project	The project name.
Cluster	The cluster name.
Hostname	The hostname of the machine.
IP	The IP address of the machine.
Serverrole	The server role name.
State	The running status of the server role.
Action Name	The action on the server role.
Action Status	The status of the action on the server role.
Actions	The approval button.

Machine Component

Displays the hard disk information of pending approval machines.

Item	Description
Project	The project name.
Cluster	The cluster name.
Hostname	The hostname of the machine.
Component	The hard disk on the machine.
State	The running status of the hard disk.
Action Name	The action on the hard disk.
Action Status	The status of the action on the hard disk.
Actions	The approval button.

6.6.2.9.6. Registration vars of services

This report displays values of all service registration variables.

Item	Description
Service	The service name.
Service Registration	The service registration variable.

Item	Description
Cluster	The cluster name.
Update Time	The updated time.

6.6.2.9.7. Virtual machine mappings

Use the global filter to display the virtual machines of a specific cluster.

Displays the information of virtual machines in the cluster. Data is available only when virtual machines are deployed in the cluster.

Item	Description
Project	The project name.
Cluster	The cluster name.
VM	The hostname of the virtual machine.
Currently Deployed On	The hostname of the physical machine on which the virtual machine is currently deployed.
Target Deployed On	The hostname of the physical machine on which the virtual machine is expected to be deployed.

6.6.2.9.8. Service inspector report

Use the global filter to display the service inspection reports of a specific cluster.

Service Inspector: Data is available only for services with inspection configured.

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Description	The contents of the inspection report.
Level	The level of the inspection report.

6.6.2.9.9. Resource application report

In the **Global Filter** section, select the project, cluster, and machine from the **project**, **cluster**, and **machine** drop-down lists and then click **Filter** on the right to display the corresponding resource application data.

Change Mappings

Item	Description
Project	The project name.
Cluster	The cluster name.
Version	The version where the change occurs.
Resource Process Status	The resource application status in the version.
Msg	The exception message.
Begintime	The start time of the change analysis.
Endtime	The end time of the change analysis.

Changed Resource List

Item	Description
Res	The resource ID.
Type	The resource type.
Name	The resource name.
Owner	The application to which the resource belongs.
Parameters	The resource parameters.
Ins	The resource instance name.
Instance ID	The resource instance ID.

Resource Status

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
APP	The application of the server role.
Name	The resource name.

Item	Description
Type	The resource type.
Status	The resource application status.
Parameters	The resource parameters.
Result	The resource application result.
Res	The resource ID.
Reprocess Status	The status of the interaction with Business Foundation System during the VIP resource application.
Reprocess Msg	The error message of the interaction with Business Foundation System during the VIP resource application.
Reprocess Result	The result of the interaction with Business Foundation System during the VIP resource application.
Refer Version List	The version that uses the resource.
Error Msg	The exception message.

6.6.2.9.10. Statuses of project components

This report displays the status of all server roles in an abnormal status on machines of the project, and the monitoring information (alert information reported by the server role to Apsara Infrastructure Management Framework monitor) of server roles and machines.

Error State Component Table

Only displays the information of server roles that are not in GOOD status and server roles to be upgraded.

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Machine Name	The machine name.
Need Upgrade	Whether the current version reaches the final status.
Server Role Status	The current status of the server role.

Item	Description
Machine Status	The current status of the machine.

Server Role Alert Information

Select a row in the **Error State Component Table** section to display the corresponding information in the list.

Item	Description
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Machine Name	The machine name.
Monitored Item	The monitored item name of the server role.
Level	The alert level.
Description	The description about the alert contents.
Updated At	The updated time of the alert information.

Machine Alert Information

Select a row in the **Error State Component Table** section to display the corresponding information in the list.

Item	Description
Cluster	The cluster name.
Machine Name	The machine name.
Monitored Item	The monitored item name of the server role.
Level	The alert level.
Description	The description about the alert contents.
Updated At	The updated time of the alert information.

Service Inspector Information

Select a row in the **Error State Component Table** section to display the corresponding information in the list.

Item	Description
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Monitored Item	The monitored item name of the server role.
Level	The alert level.
Description	The description about the alert contents.
Updated At	The updated time of the alert information.

6.6.2.9.11. Relationship of service dependency

This report displays the dependencies among server roles. Use the global filter to display the data of a specific cluster in the list.

Item	Description
Project	The project name.
Cluster	The cluster name.
Service	The service name.
Server Role	The server role name.
Dependent Service	The service on which the server role depends.
Dependent Server Role	The server role on which the server role depends.
Dependent Cluster	The cluster to which the dependent server role belongs.
Dependency in Final Status	Whether the dependent server role reaches the final status.

6.6.2.9.12. Check report of network topology

This report checks if network devices and machines have wirecheck alerts.

Check Report of Network Topology

Checks if network devices have wirecheck alerts.

Item	Description
Cluster	The cluster name.
Network Instance	The name of the network device.
Level	The alert level.
Description	The description about the alert information.

Check Report of Server Topology

Checks if servers (machines) have wirecheck alerts.

Item	Description
Cluster	The cluster name.
Machine Name	The server (machine) name.
Level	The alert level.
Description	The description about the alert information.

6.6.2.9.13. Clone report of machines

This report displays the clone progress and status of machines.

Clone Progress of Machines

Item	Description
Project	The project name.
Cluster	The cluster name.
Machine Name	The machine name.
Machine Status	The running status of the machine.
Clone Progress	The progress of the current clone process.

Clone Status of Machines

Item	Description
Project	The project name.
Cluster	The cluster name.
Machine Name	The machine name.

Item	Description
Machine Action	The action performed by the machine, such as the clone action.
Machine Action Status	The status of the action performed by the machine.
Machine Status	The running status of the machine.
Level	Whether the clone action performed by the machine is normal.
Clone Status	The current status of the clone action performed by the machine.

6.6.2.9.14. Auto healing/install approval pending report

The list structure is the same as the machine RMA approval pending list, whereas this view is used for the approval during the installation. For more information, see Machine RMA approval pending list.

6.6.2.9.15. Machine power on or off statuses of clusters

After a cluster starts or shuts down machines, you can view the related information in this report.

Cluster Running Statuses

If a cluster is starting or shutting down machines, the corresponding data is available in this list. No data indicates that no cluster has machines shut down.

Item	Description
Project	The project name.
Cluster	The cluster name.
Action Name	The startup or shutdown action that is being performed by the cluster.
Action Status	The status of the action.

Server Role Power On or Off Statuses

Displays the power on or off statuses of server roles in the cluster selected in the **Cluster Running Statuses** section.

Select a row in the **Cluster Running Statuses** section to display the information of the corresponding cluster in the list.

Item	Description
Cluster	The cluster name.
Server Role	The server role name.
Action Name	The startup or shutdown action that is being performed by the server role.

Item	Description
Action Status	The status of the action.

Statuses on Machines

Displays the running status of the selected server role on machines.

Select a row in the **Server Role Power On or Off Statuses** section to display the information of the corresponding server role in the list.

Item	Description
Cluster	The cluster name.
Server Role	The server role name.
Machine Name	The machine name.
Server Role Status	The running status of the server role.
Server Role Action	The action currently performed by the server role.
Server Role Action Status	The status of the action.
Error Message	The exception message.

Machine Statuses

Displays the running statuses of machines in the selected cluster.

Select a row in the **Statuses on Machines** section to display the information of the corresponding machine in the list.

Item	Description
Cluster	The cluster name.
Machine Name	The machine name.
IP	The IP address of the machine.
Machine Status	The running status of the machine.
Machine Action	The action currently performed by the machine.
Machine Action Status	The action status of the machine.
Error Message	The exception message.

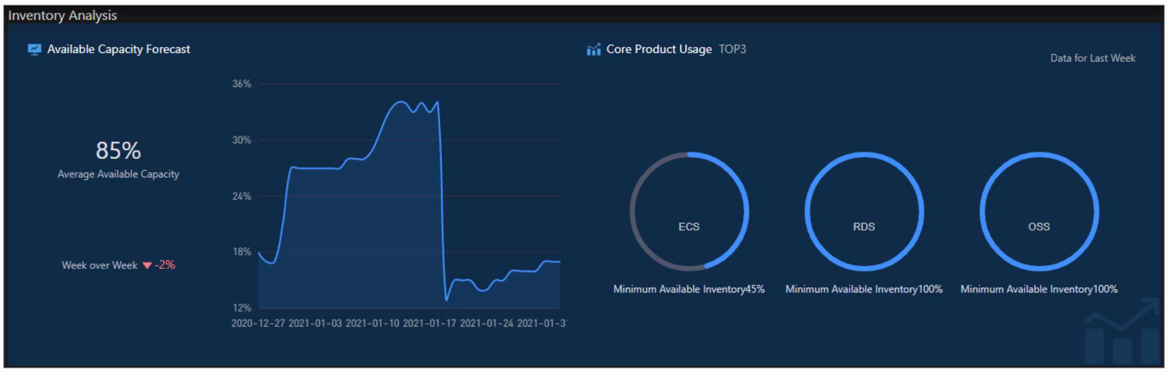
7.Analysis

7.1. Inventory analysis

The Inventory Analysis module allows you to predict capacity trends and perform operations based on the available product inventory and usage habits.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Analysis**.
3. On the **Inventory Analysis** page, view the cloud product inventory.



   - In the **Inventory Analysis** section, view the average available inventory, changing trends, and core product usage.
   - In the **Product available capacity forecast** section, view the inventory of items related to a single product.
     - Click **Days**, **Weeks**, or **Months** to view the predicted available capacity of the product within the specified time range.
     - Click an inventory item under a product name to view the corresponding product inventory.
     - Move the pointer over a curve. Inventory information at a specific time point is displayed.

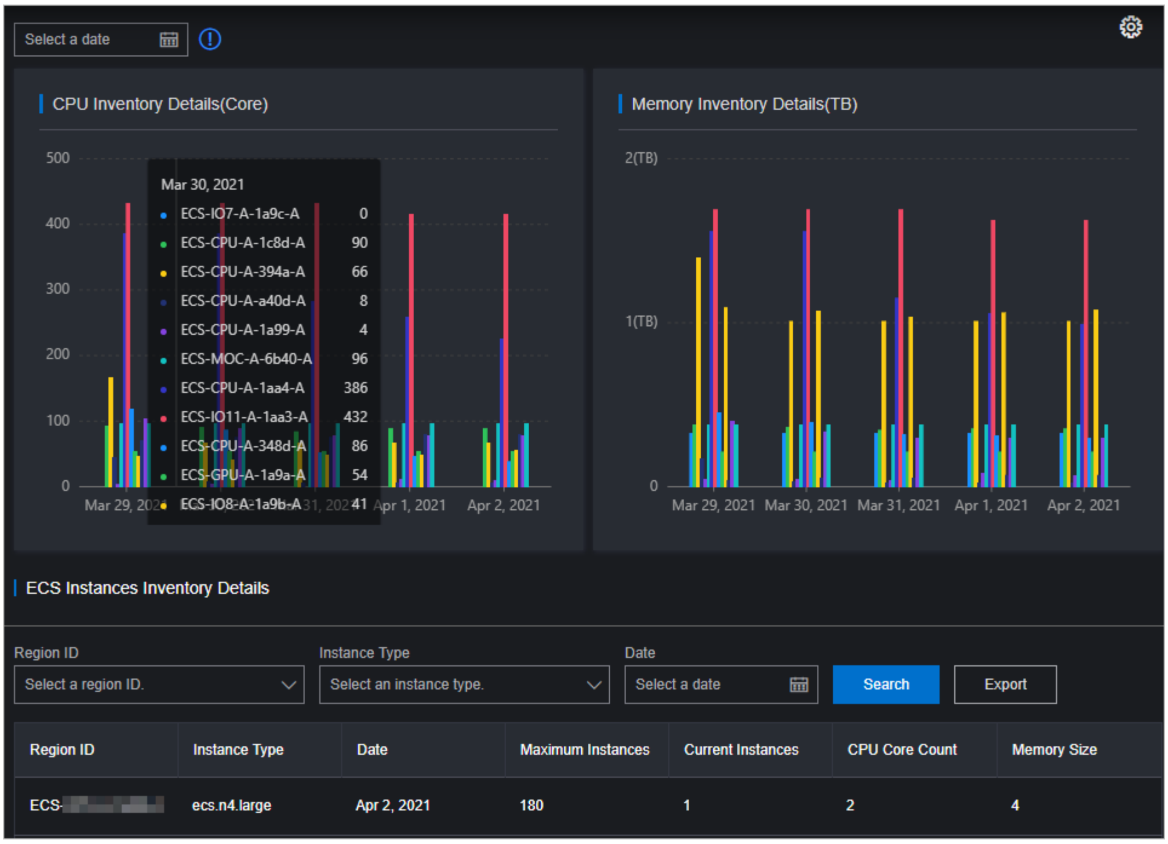
7.2. View the ECS inventory

By viewing the Elastic Computing Service (ECS) inventory, you can query the usage and availability of ECS resources to perform O&M operations more efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Analysis**.
3. In the left-side navigation pane, click **ECS**.
4. Select a date in the upper part of the page and view the ECS inventory.

> **Note** You can click the ⚙ icon in the upper-right corner of the page to specify a zone and configure thresholds.



Mar 30, 2021

● ECS-IO7-A-1a9c-A	0
● ECS-CPU-A-1c8d-A	90
● ECS-CPU-A-394a-A	66
● ECS-CPU-A-a40d-A	8
● ECS-CPU-A-1a99-A	4
● ECS-MOC-A-6b40-A	96
● ECS-CPU-A-1aa4-A	386
● ECS-IO11-A-1aa3-A	432
● ECS-CPU-A-348d-A	86
● ECS-GPU-A-1a9a-A	54
● ECS-IO8-A-1a9b-A	41

ECS Instances Inventory Details

Region ID: Select a region ID.
Instance Type: Select an instance type.
Date: Select a date
Search
Export

Region ID	Instance Type	Date	Maximum Instances	Current Instances	CPU Core Count	Memory Size
ECS-[redacted]	ecs.n4.large	Apr 2, 2021	180	1	2	4

- The **CPU Inventory Details (Core)** and **Memory Inventory Details (TB)** sections show the usage and availability of CPU (core) and memory (TB) of all ECS instance families for the last five days.
- The **ECS Instances Inventory Details** section shows the inventory details of specified ECS instance type at the specified date on multiple pages by **Region ID**, **Instance Type**, and **Date**, as well as the CPU and memory configurations corresponding to each instance of this type.

5. (Optional)Query data by specifying **Region ID**, **Instance Type**, and **Date** in the **ECS Instances Inventory Details** section, and then click **Export** to export the ECS inventory details to your computer.

7.3. View the SLB inventory

By viewing the Server Load Balancer (SLB) inventory, you can query the usage and availability of SLB resources to perform O&M operations more efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Analysis**.
3. In the left-side navigation pane, click **SLB**.

> **Note** You can click the ⚙ icon in the upper-right corner to configure the thresholds.

4. View the SLB inventory.

- The Internal VIP Used Inventory and Public VIP Used Inventory sections show the amount and percentage of internal and public VIP inventory that are being used.
- The Network Card Traffic section shows the inbound and outbound network card traffic.
- The **SLB Inventory Details** section shows the SLB inventory details on multiple pages by **Type** and **Date**.

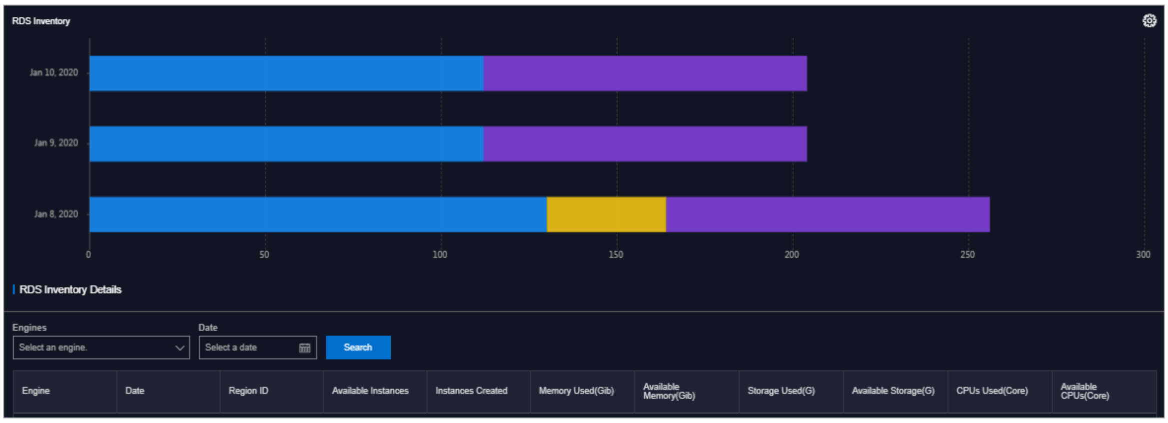
7.4. View the RDS inventory

By viewing the Relational Database Service (RDS) inventory, you can query the usage and availability of RDS resources to perform O&M operations efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Analysis**.
3. In the left-side navigation pane, click **RDS**.

> ? **Note** You can click the ⚙ icon in the upper-right corner to configure inventory thresholds for each engine.



Engine	Date	Region ID	Available Instances	Instances Created	Memory Used(Gib)	Available Memory(Gib)	Storage Used(G)	Available Storage(G)	CPUs Used(Core)	Available CPUs(Core)

4. View the RDS inventory.
   - The **RDS Inventory** section shows the inventories of different types of RDS instances for the last five days. Different colors represent different types of RDS instances.
   - The **RDS Inventory Details** section shows the RDS inventory details on multiple pages by **Engines** and **Date**.

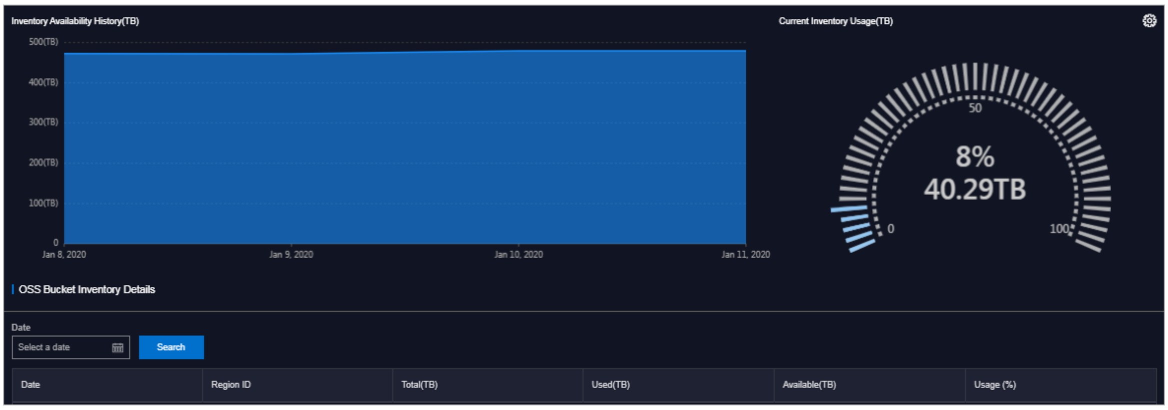
7.5. View the OSS inventory

By viewing the Object Storage Service (OSS) inventory, you can query the usage and availability of OSS resources to perform O&M operations more efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Analysis**.
3. In the left-side navigation pane, click **OSS**.

> ⓘ **Note** You can click the ⚙ icon in the upper-right corner of the page to configure the thresholds.



4. View the OSS inventory.
   - The **Inventory Availability History (TB)** section shows the available OSS resources for the last five days.
   - The **Current Inventory Usage (TB)** section shows the amount and percentage of OSS resources that are being used.
   - The **OSS Bucket Inventory Details** section shows the OSS inventory details on multiple pages by **Date**.

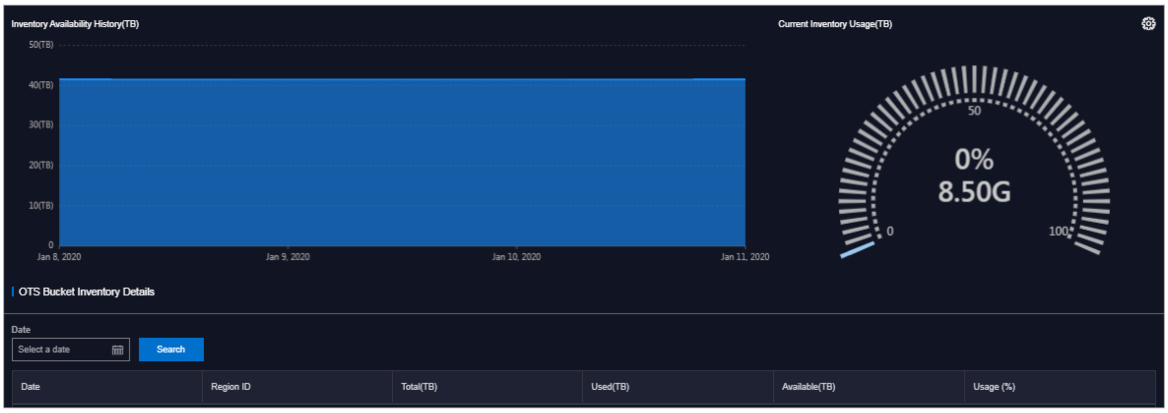
7.6. View the Tablestore inventory

By viewing the Tablestore inventory, you can query the usage and availability of Tablestore resources to perform O&M operations efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Analysis**.
3. In the left-side navigation pane, click **OTS**.

> ⓘ **Note** You can click the ⚙ icon in the upper-right corner and configure the global quota.



4. View the Tablestore inventory.
   - The **Inventory Availability History (TB)** section shows the available Tablestore inventory for the last five days.
   - The **Current Inventory Usage (TB)** section shows the amount and percentage of Tablestore inventory that are in use.
   - The **OTS Bucket Inventory Details** section shows the Tablestore inventory details on multiple pages by **Date**.

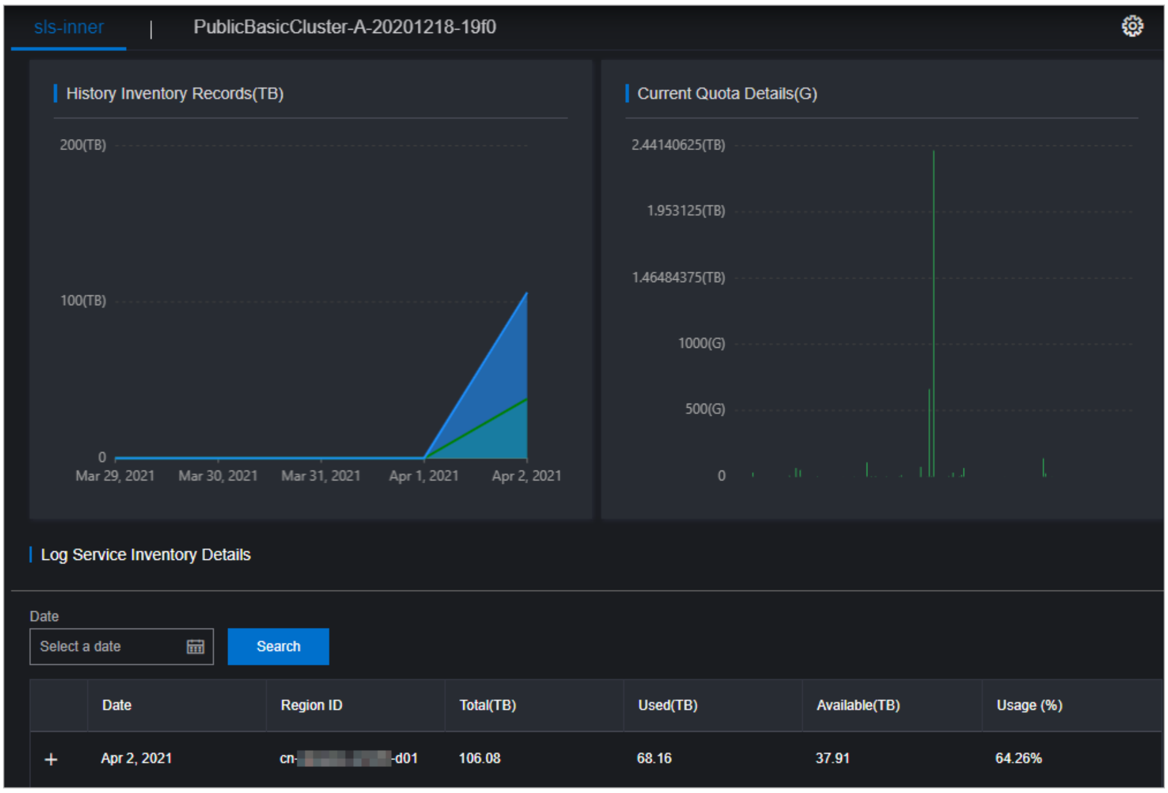
7.7. View the Log Service inventory

By viewing the Log Service inventory, you can query the usage and availability of Log Service resources to perform O&M operations efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Diagnose**.
3. In the left-side navigation pane, click **SLS**.

> **Note** You can click the ⚙ icon in the upper-right corner of the page to configure the inventory thresholds and global quota.



	Date	Region ID	Total(TB)	Used(TB)	Available(TB)	Usage (%)
+	Apr 2, 2021	cn-[redacted]-d01	106.08	68.16	37.91	64.26%

4. On the **sls-inner** tab, view the Log Service inventory details.
   - The **History Inventory Records (TB)** section shows the available and total Log Service inventory for the last five days.

- The **Current Quota Details (G)** section shows the amount and percentage of Log Service inventory that are currently in use.
- The **Log Service Inventory Details** section shows the Log Service inventory details on multiple pages by **Date**.

5. Click the **PublicBasicCluster-XXX** tab to view details about the Log Service inventory for which that you have applied.
   - The **Inventory Availability History (TB)** section shows the available Log Service inventory for the last five days.
   - The **Current Inventory Usage (TB)** section shows the amount and percentage of Log Service inventory that are currently in use.
   - The **SLS Bucket Inventory Details** section shows the Log Service inventory details in multiple pages by **Date**.

7.8. View the EBS inventory

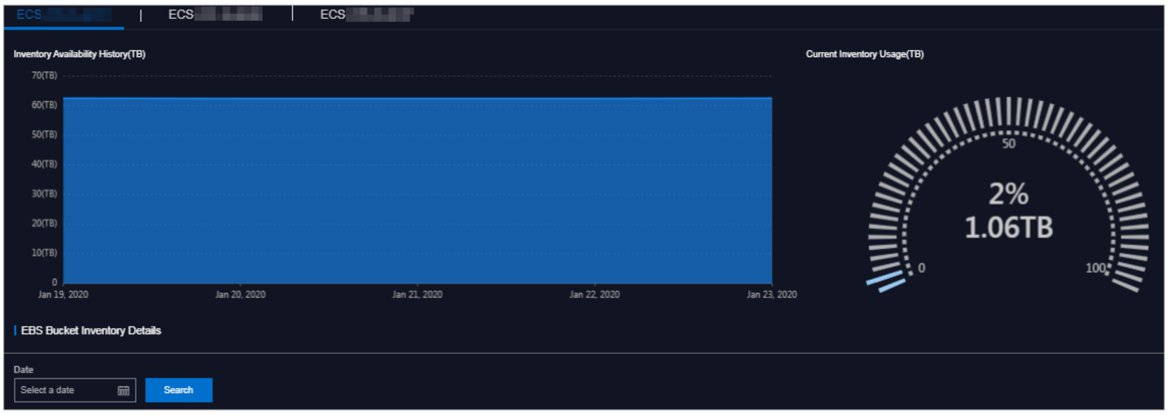
By viewing the Elastic Block Storage (EBS) inventory, you can query the usage and availability of EBS resources to perform O&M operations efficiently.

Context

> **Note** EBS is the Apsara Distributed File System storage provided for ECS by the base, and ECS IO clusters are used for Apsara Distributed File System storage. Therefore, you can view the EBS inventory in ECS IO clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Analysis**.
3. In the left-side navigation pane, click **EBS**.



4. If multiple ECS IO clusters exist in the environment, click the tab of each ECS IO cluster to view the EBS inventory.
   - The **Inventory Availability History (TB)** section shows the available EBS inventory for the last five days.
   - The **Current Inventory Usage (TB)** section shows the amount and percentage of EBS inventory that are being used.

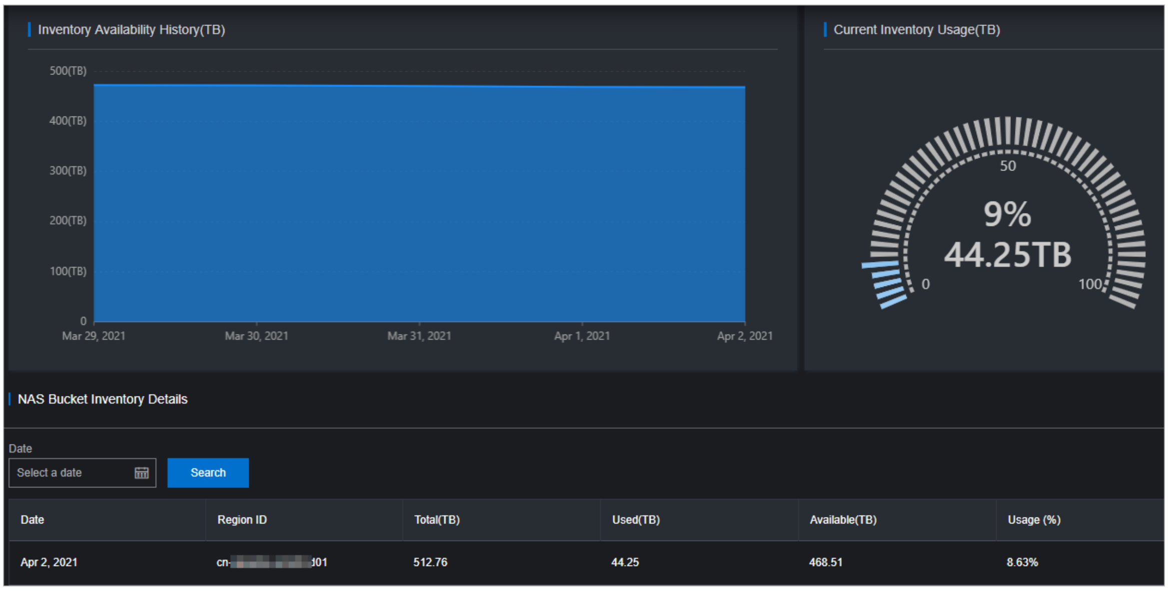
- The **EBS Bucket Inventory Details** section shows the EBS inventory details on multiple pages by Date.

7.9. View the NAS inventory

By viewing the Apsara File Storage NAS inventory, you can query the usage and availability of NAS resources to perform O&M operations efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Analysis**.
3. In the left-side navigation pane, click **NAS**.



NAS Bucket Inventory Details

Date

Date	Region ID	Total(TB)	Used(TB)	Available(TB)	Usage (%)
Apr 2, 2021	cn-[redacted]01	512.76	44.25	468.51	8.63%

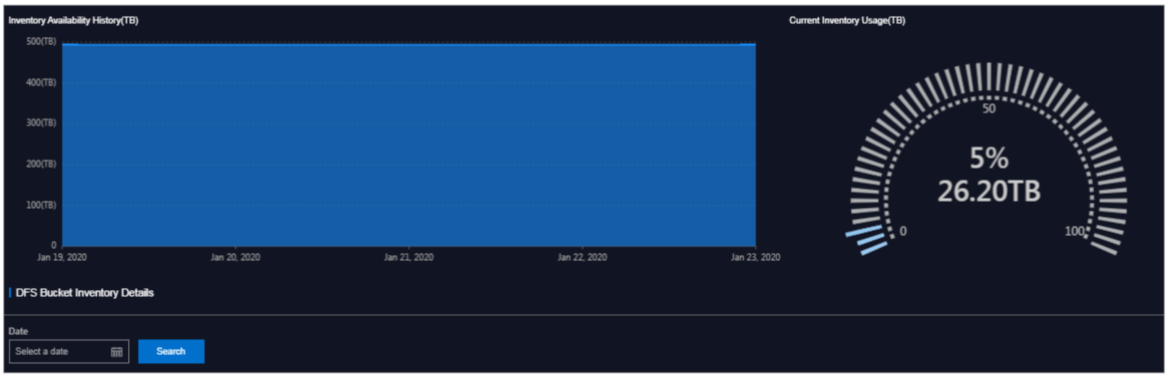
4. View the NAS inventory.
   - The **Inventory Availability History (TB)** section shows the available NAS inventory for the last five days.
   - The **Current Inventory Usage (TB)** section shows the amount and percentage of NAS inventory that are being used.
   - The **NAS Bucket Inventory Details** section shows the NAS inventory details on multiple pages by date.

7.10. View the DFS inventory

By viewing the DFS inventory, you can query the usage and availability of HDFS resources to perform O&M operations efficiently.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **Analysis**.
3. In the left-side navigation pane, click **DFS**.



4. View the DFS inventory.
   - The **Inventory Availability History (TB)** section shows the available DFS inventory for the last five days.
   - The **Current Inventory Usage (TB)** section shows the amount and percentage of DFS inventory that are being used.
   - The **DFS Bucket Inventory Details** section shows the DFS inventory details on multiple pages by **Date**.

8.Network operations

8.1. Apsara Network Intelligence

8.1.1. What is Apsara Network Intelligence?

Apsara Network Intelligence is a system that can analyze network traffic. It provides data to facilitate resource planning, diagnostic functions, monitoring, system management, and user profiling.

You can use Apsara Network Intelligence to:

- Manage cloud service types.
- Query VPC and SLB instance details with a single click.
- Configure reverse access to cloud services.
- Configure leased lines by using graphical interfaces and set up primary and secondary routes.
- Query the tunnel VIPs of cloud services.
- Create Layer 4 listeners.

8.1.2. Log on to the Apsara Network Intelligence console

This topic describes how to log on to the Apsara Network Intelligence console.

Prerequisites

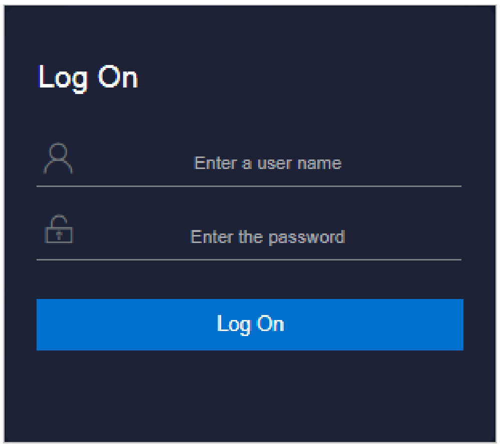
- You must log on to the the Apsara Uni-manager Operations Console to access Apsara Network Intelligence. Before you start, you must obtain the URL, username, and password of the Apsara Uni-manager Operations Console from the engineer that deploys the service.

  The URL of the Apsara Uni-manager Operations Console is in the `*ops*.**asconsole**.*intranet-domain-id*.**com**` format.

- We recommend that you use the Google Chrome browser.

Procedure

1. Open your browser.
2. In the address bar, enter the URL of the Apsara Uni-manager Operations Console: `*ops*.**asconsole**.*intranet-domain-id*.**com**` and press enter.
3. Enter your username and password.



> **Note** You can select a language from the drop-down list in the upper-right corner of the page.

If this is the first time you log on to the Apsara Uni-manager Operations Console, you must change your password as prompted.

For higher security, make sure that the password meets the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password is 10 to 20 characters in length.

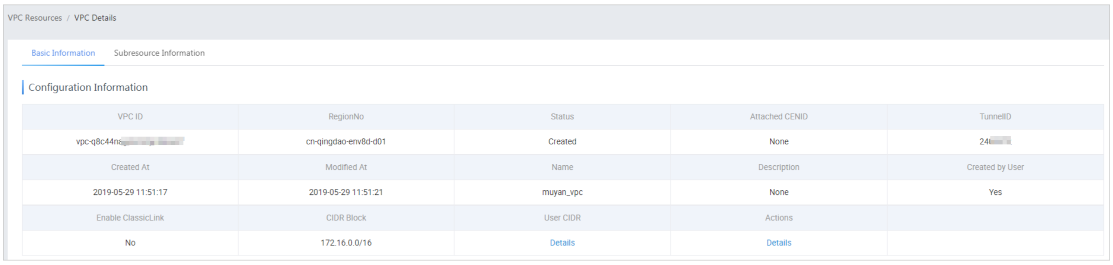
4. Click **Log On** to go to the **Apsara Uni-manager Operations Console** homepage.
5. In the top navigation bar, click **O&M**.
6. In the left-side navigation pane, choose **Product Management > Product List**.
7. In the **Infrastructure as a Service (IaaS)** section, click **Apsara Network Intelligence**.

8.1.3. Query information

You can enter an instance ID to query details of the instance.

Procedure

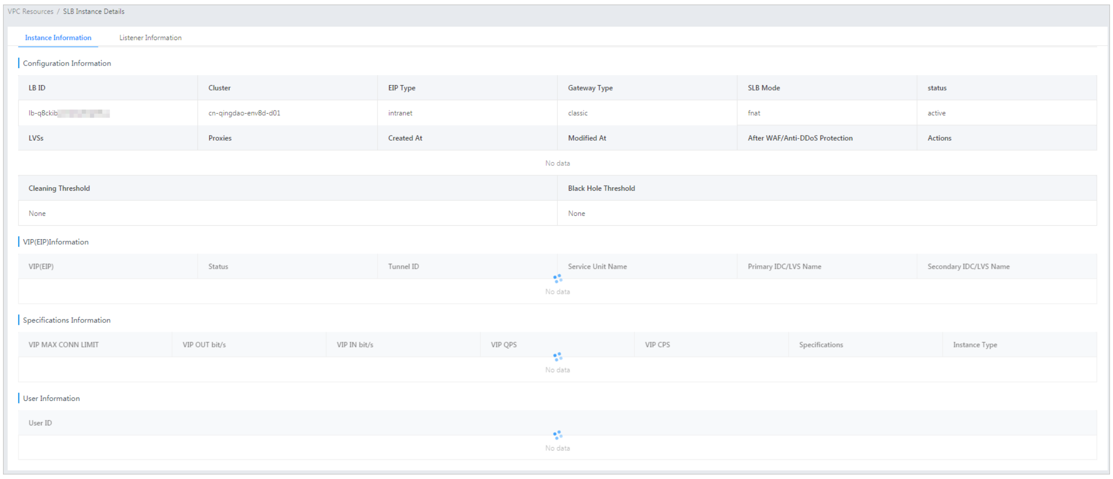
1. Log on to the Apsara Network Intelligence console.
2. Enter the ID of a VPC or an SLB instance to query details.
   - Enter the ID of a VPC to query VPC, VRouter, and VSwitch details.
     - VPC details



Configuration Information

VPC ID	RegionNo	Status	Attached CENID	TunnelID
vpc-q8c44na[redacted]	cn-qingdao-env8d-d01	Created	None	24[redacted]
Created At	Modified At	Name	Description	Created by User
2019-05-29 11:51:17	2019-05-29 11:51:21	muyan_vpc	None	Yes
Enable ClassicLink	CIDR Block	User CIDR	Actions	
No	172.16.0.0/16	Details	Details	

    - Information about VRouters, route tables, router interfaces, and VSwitches .
- Enter the ID of an SLB instance to query instance details.
    - Information about SLB instance configurations, VIPs, specifications, and users



VPC Resources / SLB Instance Details

Instance Information | Listener Information

Configuration Information

LB ID	Cluster	EIP Type	Gateway Type	SLB Mode	status
lb-q8ckib[redacted]	cn-qingdao-env8d-d01	intranet	classic	fnat	active

LVSs	Proxies	Created At	Modified At	After WAF/Anti-DDoS Protection	Actions

No data

Cleaning Threshold	Black Hole Threshold
None	None

VIP(EIP)Information

VIP(EIP)	Status	Tunnel ID	Service Unit Name	Primary IDC/LVS Name	Secondary IDC/LVS Name

No data

Specifications Information

VIP MAX CONN LIMIT	VIP OUT bit/s	VIP IN bit/s	VIP QPS	VIP CPS	Specifications	Instance Type

No data

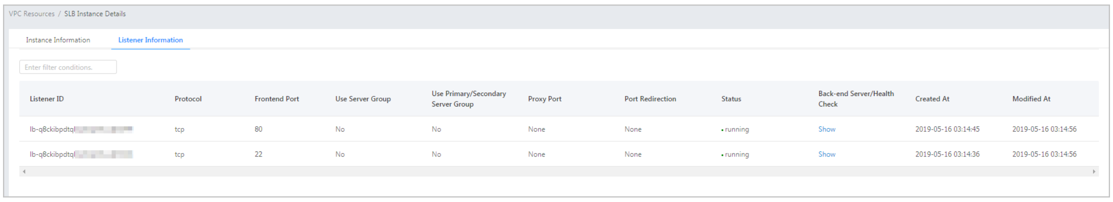
User Information

User ID

No data

    - Listener information

      Click **Show** in the **Back-end Server/Health Check** column to view details on backend servers.



VPC Resources / SLB Instance Details

Instance Information | Listener Information

Enter filter conditions.

Listener ID	Protocol	Frontend Port	Use Server Group	Use Primary/Secondary Server Group	Proxy Port	Port Redirection	Status	Back-end Server/Health Check	Created At	Modified At
lb-q8ckibpdtql[redacted]	tcp	80	No	No	None	None	• running	Show	2019-05-16 03:14:45	2019-05-16 03:14:56
lb-q8ckibpdtql[redacted]	tcp	22	No	No	None	None	• running	Show	2019-05-16 03:14:36	2019-05-16 03:14:56

8.1.4. Manage cloud service instances

You can create a cloud service in a region or query the instance information of a region.

Procedure

1. Log on to the Apsara Network Intelligence console.
2. From the **Products** menu, choose **Virtual Private Cloud > VPC Instance Type Management**.
3. Select the region from the **Select Region** drop-down list for which you want to create a cloud service instance. All cloud service instances in the specified region are displayed.
4. Click **Add** to add a cloud service type.

8.1.5. Tunnel VIP

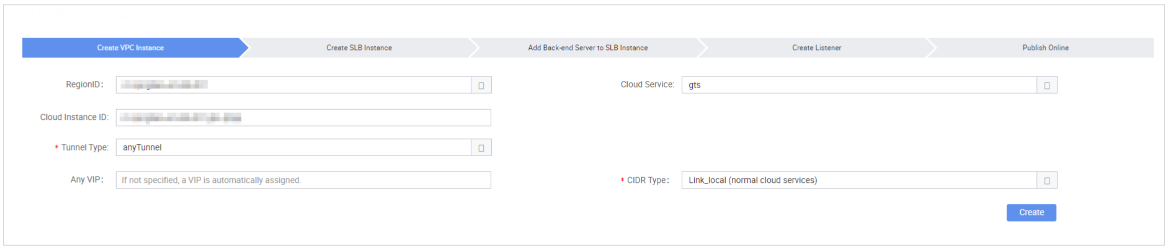
8.1.5.1. Create a Layer-4 listener VIP

You can create Layer-4 listener VIPs to forward traffic for cloud services in your VPC.

Procedure

1. Log on to the Apsara Network Intelligence console.
2. In the top navigation bar, click **Products** and choose **Server Load Balancer > VIP Management**.

3. Click **Create VIP**.
4. In the **Create VPC Instance** step, set the VPC instance parameters.



RegionID: [redacted]

Cloud Instance ID: [redacted]

* Tunnel Type: anyTunnel

Any VIP: If not specified, a VIP is automatically assigned.

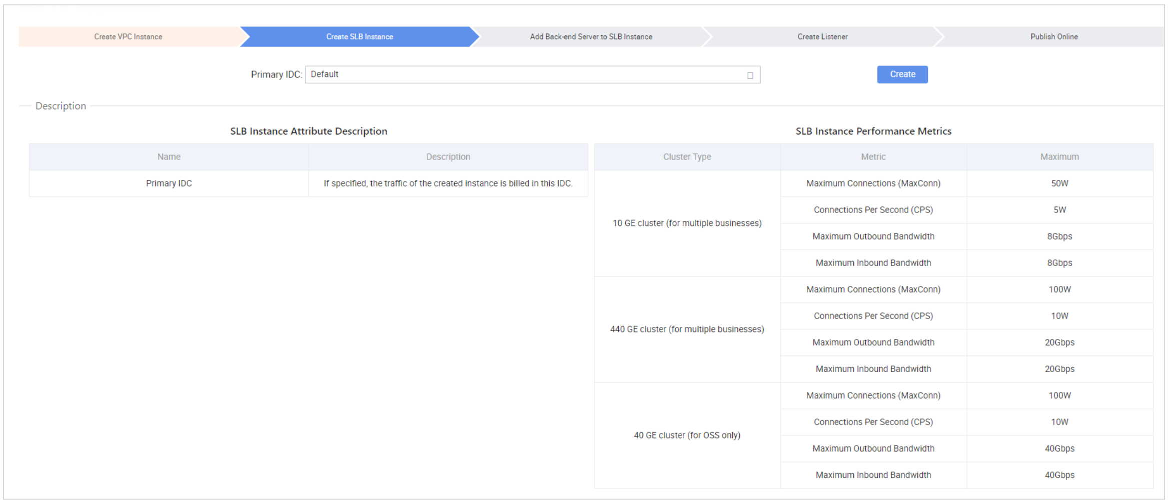
Cloud Service: gts

* CIDR Type: Link_local (normal cloud services)

The following tunnel types are available:

- **singleTunnel**: specifies a single tunnel VIP that allows the Elastic Compute Service (ECS) instances in a single VPC to access external cloud services.
- **anyTunnel**: specifies a tunnel VIP that allows the ECS instances in all VPCs to access a specified cloud service.

5. Click **Create**.
6. In the **Create SLB Instance** step, select a primary data center or use the default data center.



Primary IDC: Default

SLB Instance Attribute Description

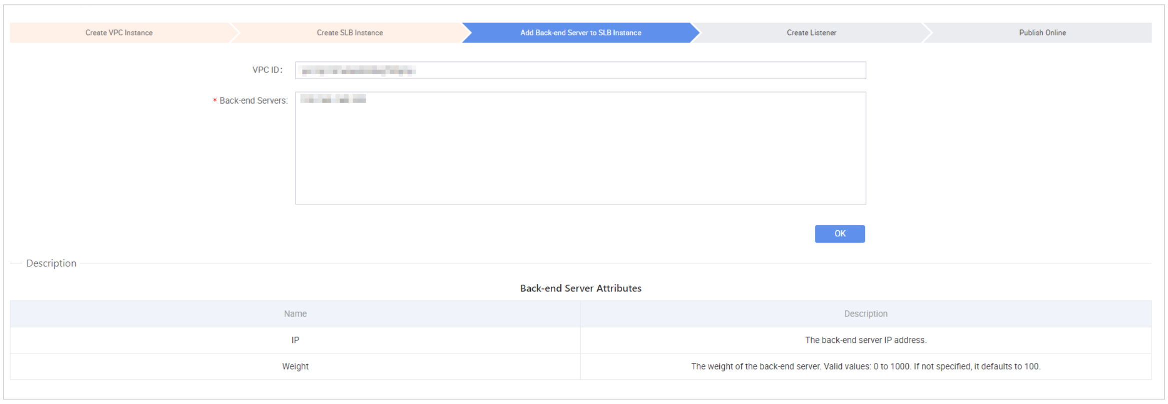
Name	Description
Primary IDC	If specified, the traffic of the created instance is billed in this IDC.

SLB Instance Performance Metrics

Cluster Type	Metric	Maximum
10 GE cluster (for multiple businesses)	Maximum Connections (MaxConn)	50W
	Connections Per Second (CPS)	5W
	Maximum Outbound Bandwidth	8Gbps
	Maximum Inbound Bandwidth	8Gbps
440 GE cluster (for multiple businesses)	Maximum Connections (MaxConn)	100W
	Connections Per Second (CPS)	10W
	Maximum Outbound Bandwidth	20Gbps
	Maximum Inbound Bandwidth	20Gbps
40 GE cluster (for OSS only)	Maximum Connections (MaxConn)	100W
	Connections Per Second (CPS)	10W
	Maximum Outbound Bandwidth	40Gbps
	Maximum Inbound Bandwidth	40Gbps

7. Click **Create**.
8. In the **Add Back-end Server to SLB Instance** step, specify the following information:

- **VPC ID**: Enter the ID of the VPC to which target ECS instances belong. This parameter must be set if the target ECS instances are deployed in a VPC.
- **Back-end Servers**: Specify the backend servers that you want to add. You can specify the server IP address and weight of only one backend server in each line. You can separate an IP address and the weight value with either a space or a comma (,). If no weight value is specified, the default value 100 is used.



VPC ID: [redacted]

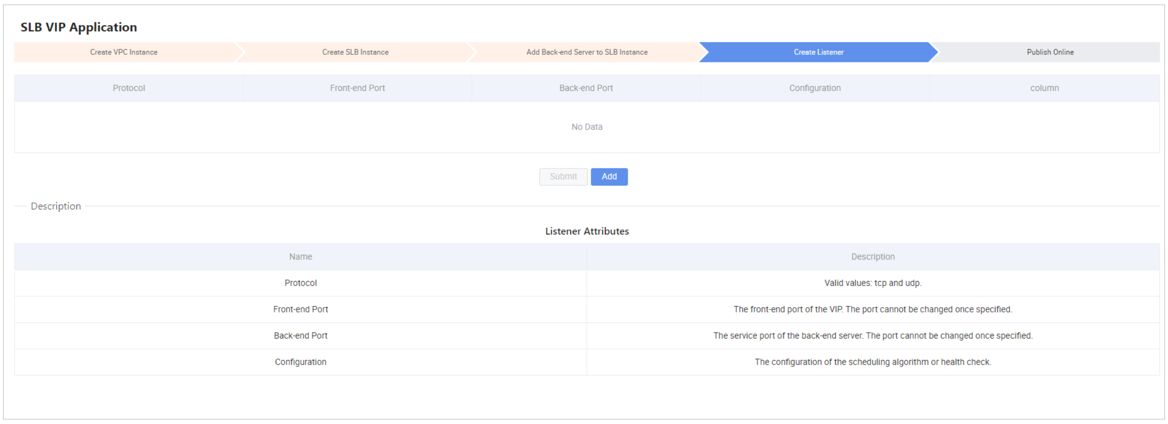
* Back-end Servers: [redacted]

Description

Back-end Server Attributes

Name	Description
IP	The back-end server IP address.
Weight	The weight of the back-end server. Valid values: 0 to 1000. If not specified, it defaults to 100.

9. Click **OK**.
10. In the **Create Listener** step, click **Add** to configure a User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) listener.


SLB VIP Application

Protocol	Front-end Port	Back-end Port	Configuration	column

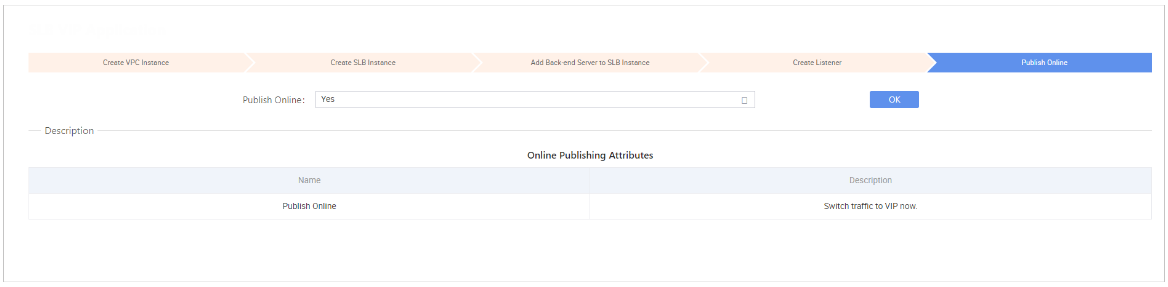
No Data

Description

Listener Attributes

Name	Description
Protocol	Valid values: tcp and udp.
Front-end Port	The front-end port of the VIP. The port cannot be changed once specified.
Back-end Port	The service port of the back-end server. The port cannot be changed once specified.
Configuration	The configuration of the scheduling algorithm or health check.

11. Click **Submit**.
12. In the **Publish Online** step, click **Yes** and then click **OK**.



Publish Online: Yes

Description

Online Publishing Attributes

Name	Description
Publish Online	Switch traffic to VIP now.

Result

The cloud services for which you have created the VIP can forward traffic through the created Layer-4 listener.

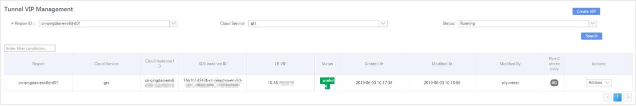
8.1.5.2. Query the tunnel VIP of a cloud service

You can query information such as creation time, connectivity, and VIP for cloud services that have Server Load Balancer (SLB) VIPs.

Procedure

1. Log on to the Apsara Network Intelligence console.

2. From the **Products** menu, choose **Server Load Balancer > VIP Management**.
3. On the **Tunnel VIP Management** page, select Region ID, Cloud Service, and Status. Click **Search**.



Tunnel VIP Management

Create VIP

* Region ID : cn-qingdao-env8d-d01 Cloud Service: gts Status: Running

Search

Enter filter conditions.

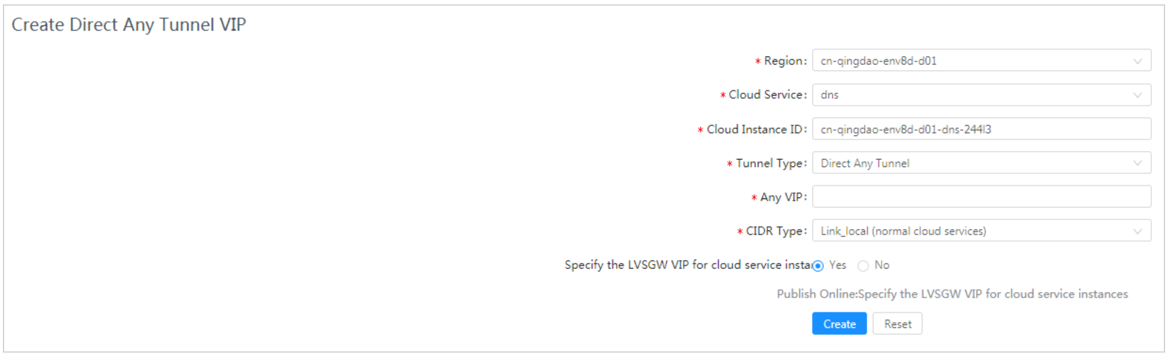
Region	Cloud Service	Cloud Instance ID	SLB Instance ID	LB VIP	Status	Created At	Modified At	Modified By	Port Connectivity	Actions
cn-qingdao-env8d-d01	gts	cn-qingdao-env8 [redacted]	16b1b1d3436-cn-qingdao-env8d- [redacted]	10.68. [redacted]	working	2019-06-03 10:17:38	2019-06-03 10:18:06	aliyuntest	80	Actions

8.1.6. Create a Direct Any Tunnel VIP

You can create Direct Any Tunnel VIPs for cloud services in your VPC to allow traffic forwarding through XGW.

Procedure

1. Log on to the Apsara Network Intelligence console.
2. From the **Products** menu, choose **Server Load Balancer > Direct Any Tunnel VIP Management**.
3. On the **Direct Any Tunnel VIP Management** page, click **Create Direct Any Tunnel VIP**.
4. On the **Create Direct Any Tunnel VIP** page, configure the parameters for the Direct Any Tunnel VIP.



Create Direct Any Tunnel VIP

* Region: cn-qingdao-env8d-d01

* Cloud Service: dns

* Cloud Instance ID: cn-qingdao-env8d-d01-dns-244l3

* Tunnel Type: Direct Any Tunnel

* Any VIP:

* CIDR Type: Link_local (normal cloud services)

Specify the LVSGW VIP for cloud service insta ● Yes ○ No

Publish Online:Specify the LVSGW VIP for cloud service instances

Create Reset

5. Click **Create**. Cloud service instances that have Direct Any Tunnel VIPs can forward traffic through XGW.

8.1.7. Leased line connection

8.1.7.1. Overview

You can connect a VPC to an IDC through a leased line.

Before connecting to a VPC through a leased line, you must confirm the initial CSW configurations meet the following conditions:

- You have uploaded the licenses required for VLAN functions onto the CSWs.
- You have set the management IP address on the loopback 100 interface of each CSW.
- You have configured the CSW uplink interfaces to ensure interoperability with the Layer 3 interfaces used by VPC APIs.
- You have deleted the default configuration of bridge-domain.
- You have enabled NETCONF and STelnet for CSWs. The configuration details are included in the CSW initial configuration template.

- You have configured the service type of CSW interfaces to tunnel.

You must also obtain the following account information:

- BID: specifies the ID of the account group. The BID for Mainland China users is 26842, and the BID for international users is 26888.
- UID: specifies the ID of the account to which the destination VPC belongs.

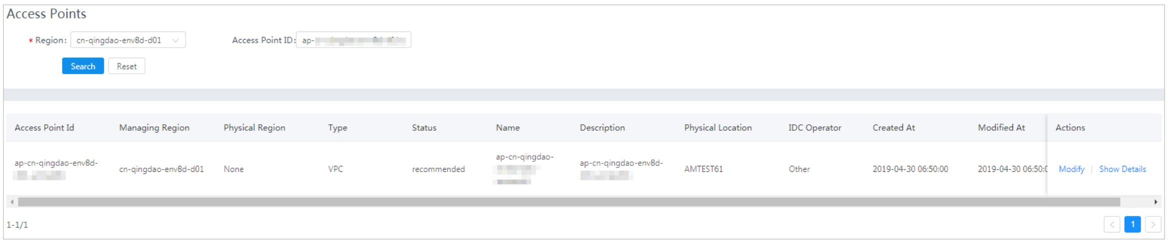
8.1.7.2. Manage access points

Access points are Alibaba Cloud data centers located in different regions. One or more access points are deployed in each region. This topic describes how to query and modify information about access points of a region.

Query an access point

Perform the following operations to query an access point:

1. Log on to the Apsara Network Intelligence console.
2. In the top navigation bar, click **Products** and choose **Express Connect > Daily Operation**.
3. In the left-side navigation pane, choose **Daily Operation > Access Points**.
4. Select the region and enter the ID of the access point that you want to query.
5. Click **Search**.



Access Points

* Region: cn-qingdao-env8d-d01
Access Point ID: ap-[redacted]

Access Point Id	Managing Region	Physical Region	Type	Status	Name	Description	Physical Location	IDC Operator	Created At	Modified At	Actions
ap-cn-qingdao-env8d-[redacted]	cn-qingdao-env8d-d01	None	VPC	recommended	ap-cn-qingdao-[redacted]	ap-cn-qingdao-env8d-[redacted]	AMTEST61	Other	2019-04-30 06:50:00	2019-04-30 06:50:(	Modify | Show Details

1-1/1

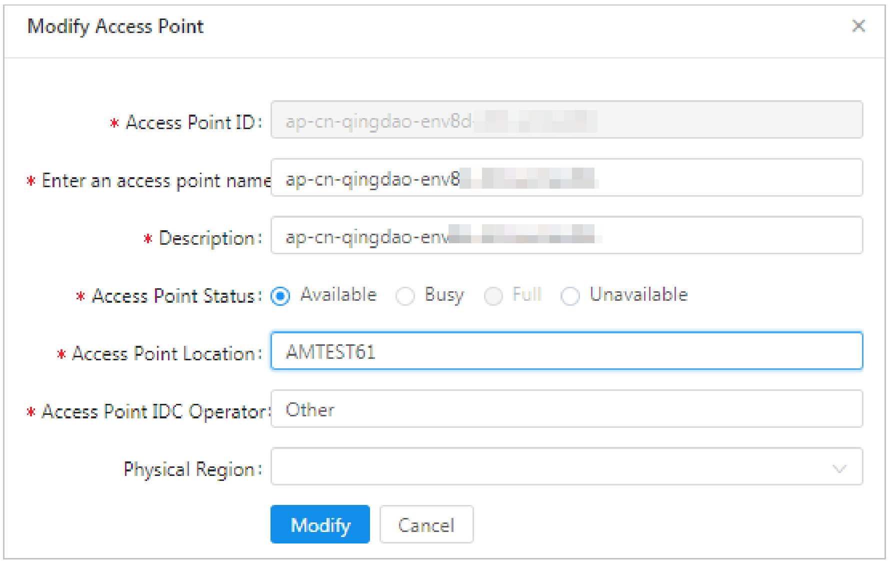
Modify access point information

Perform the following operations to modify the information about an access point:

1. Find the target access point and click **Modify** in the **Actions** column.
2. In the dialog box that appears, modify the information as needed.
3. Click **Modify**.

   Note the following points when you modify access point information:

   - **Access Point Location**: Enter the physical location of the access point. You can set a custom value.
   - **Access Point IDC Operator**: Enter the name of the data center operator.



Modify Access Point

* Access Point ID: ap-cn-qingdao-env8d[redacted]

* Enter an access point name: ap-cn-qingdao-env8[redacted]

* Description: ap-cn-qingdao-env[redacted]

* Access Point Status: ● Available ○ Busy ○ Full ○ Unavailable

* Access Point Location: AMTEST61

* Access Point IDC Operator: Other

Physical Region:

8.1.7.3. Manage access devices

This topic describes how to query and modify information about access devices of a region.

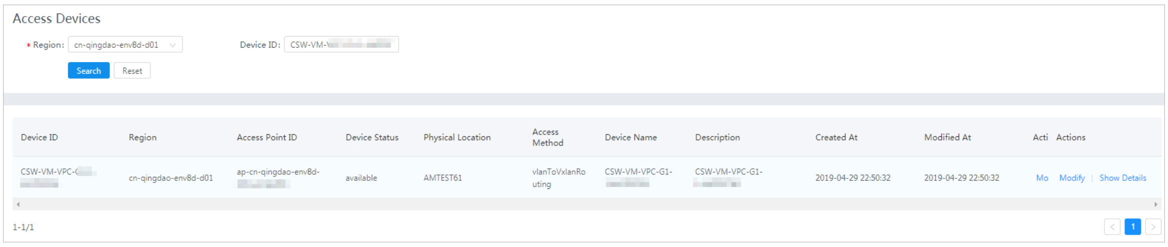
Query an access device

Perform the following operations to query an access device:

1. Log on to the Apsara Network Intelligence console.
2. In the top navigation bar, click **Products** and choose **Express Connect > Daily Operation**.
3. In the left-side navigation pane, choose **Daily Operation > Access Devices**.
4. Select the region and enter the ID of the access device that you want to query.

> **Note** If Device ID is not set, all devices in the specified region are queried.

5. Click **Search**.



Access Devices

* Region: cn-qingdao-env8d-d01

Device ID: CSW-VM-[redacted]

Device ID	Region	Access Point ID	Device Status	Physical Location	Access Method	Device Name	Description	Created At	Modified At	Acti	Actions
CSW-VM-VPC-[redacted]	cn-qingdao-env8d-d01	ap-cn-qingdao-env8d-[redacted]	available	AMTEST61	vlanToVxlanRouting	CSW-VM-VPC-G1-[redacted]	CSW-VM-VPC-G1-[redacted]	2019-04-29 22:50:32	2019-04-29 22:50:32	Mo	Modify | Show Details

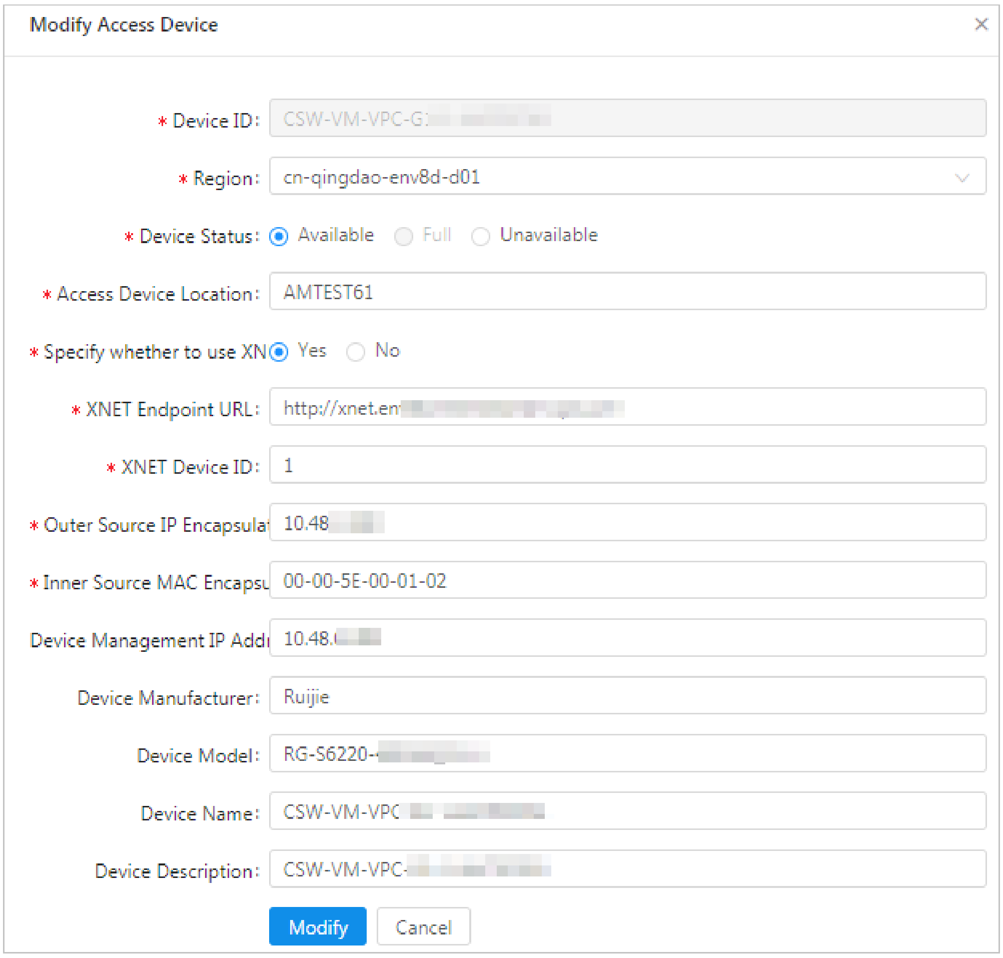
1-1/1

6. Find the target access device and click **Show Details** in the **Actions** column to view details of the access device.

Modify access device information

Perform the following operations to modify the information about an access device:

1. Find the target access device and click **Modify** in the **Actions** column.
2. In the dialog box that appears, modify the device information.



Modify Access Device

* Device ID:	CSW-VM-VPC-G[redacted]
* Region:	cn-qingdao-env8d-d01
* Device Status:	● Available ○ Full ○ Unavailable
* Access Device Location:	AMTEST61
* Specify whether to use XN	● Yes ○ No
* XNET Endpoint URL:	http://xnet.en[redacted]
* XNET Device ID:	1
* Outer Source IP Encapsula	10.48[redacted]
* Inner Source MAC Encapsu	00-00-5E-00-01-02
Device Management IP Addr	10.48.[redacted]
Device Manufacturer:	Ruijie
Device Model:	RG-S6220-[redacted]
Device Name:	CSW-VM-VPC[redacted]
Device Description:	CSW-VM-VPC-[redacted]

3. Click **Modify**.

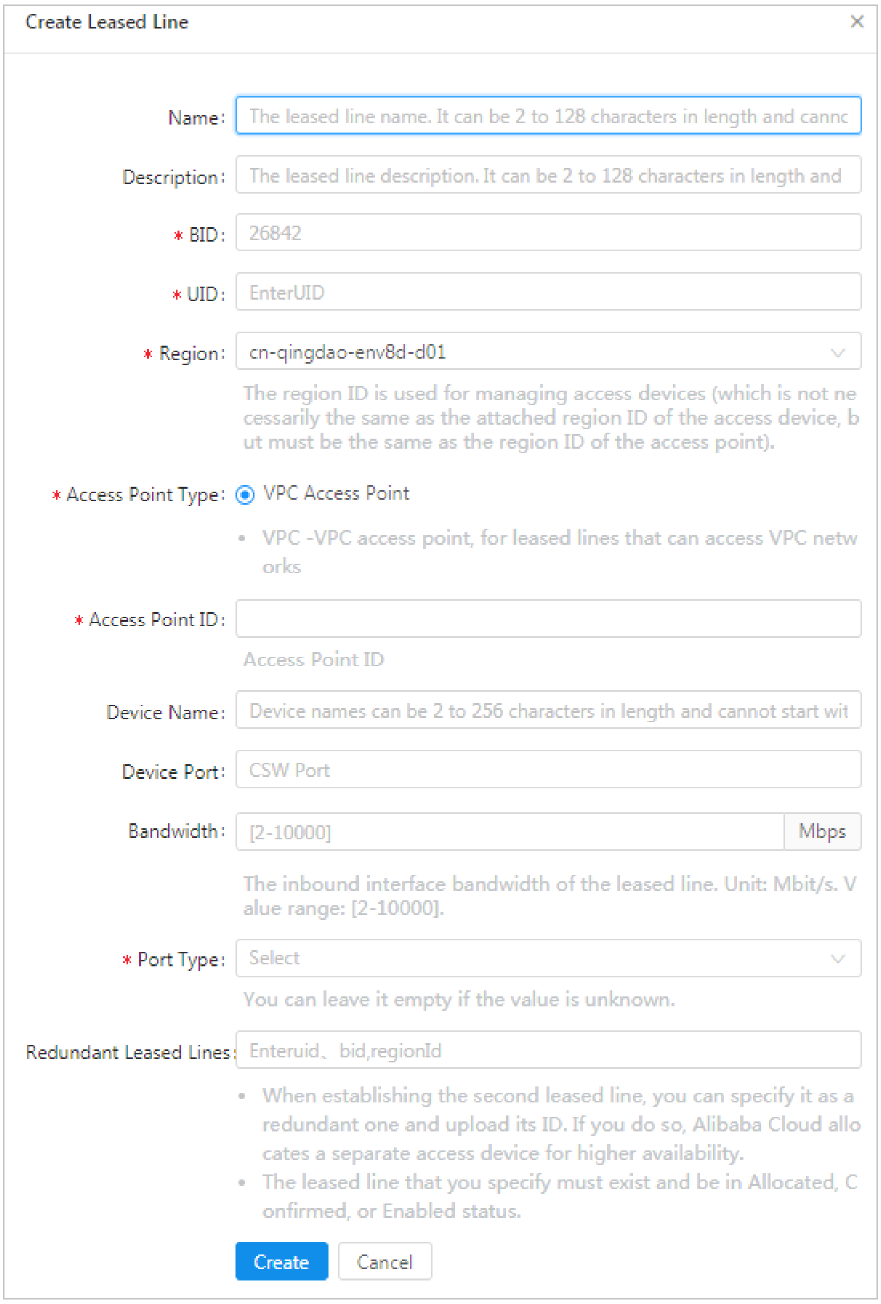
8.1.7.4. Establish a leased line connection

A leased line can be obtained from a telecom operator to establish a physical connection between your data center and an Alibaba Cloud access point. This topic describes how to establish a leased line connection and query leased line information of a region.

Procedure

1. Log on to the Apsara Network Intelligence console.
2. In the top navigation bar, click **Products** and choose **Express Connect > Network Environment Management**.
3. In the left-side navigation pane, choose **Function Modules > Leased Lines**. On the page that appears, click **Create Leased Line**.
4. In the dialog box that appears, configure the leased line and click **Create**. Note the following points when you create a leased line:
   - **Device Name**: Optional. If you set a device name, the device name must be the same as the CSW host name.
   - **Device Port**: Optional. If you set a device port, the device port number must be the same as the CSW port number.
   - **UID**: Enter the ID of the account to which the destination VPC belongs.

- **Access Point ID**: Select the ID of the region where your data center is located.
- **Redundant Leased Lines**: Select a previously obtained leased line as the redundant leased line for the leased line you are creating.



Create Leased Line ×

Name: The leased line name. It can be 2 to 128 characters in length and cannc

Description: The leased line description. It can be 2 to 128 characters in length and

* BID: 26842

* UID: EnterUID

* Region: cn-qingdao-env8d-d01

The region ID is used for managing access devices (which is not necessarily the same as the attached region ID of the access device, but must be the same as the region ID of the access point).

* Access Point Type: ● VPC Access Point

- VPC -VPC access point, for leased lines that can access VPC networks

* Access Point ID:

Access Point ID

Device Name: Device names can be 2 to 256 characters in length and cannot start wit

Device Port: CSW Port

Bandwidth: [2-10000] Mbps

The inbound interface bandwidth of the leased line. Unit: Mbit/s. Value range: [2-10000].

* Port Type: Select

You can leave it empty if the value is unknown.

Redundant Leased Lines: Enteruid、bid,regionId

- When establishing the second leased line, you can specify it as a redundant one and upload its ID. If you do so, Alibaba Cloud allocates a separate access device for higher availability.
- The leased line that you specify must exist and be in Allocated, Confirmed, or Enabled status.

Create | Cancel

When the leased line state is **Confirmed**, the line is created.

5. On the **Leased Lines** page, find the created leased line and choose **Actions > Enable**.

   If the allocation process for a leased line persists for several minutes after you click Enable, choose **Products > Network Controller > Business Foundation System Flow**. On the page that appears, set Instance ID to the leased line ID, set **Step Status** to **All**, and click Search. Check the flow status in the search results. A red flow indicates that the corresponding task has failed. You can click **Resend** to restart the task and then requery the flow status.

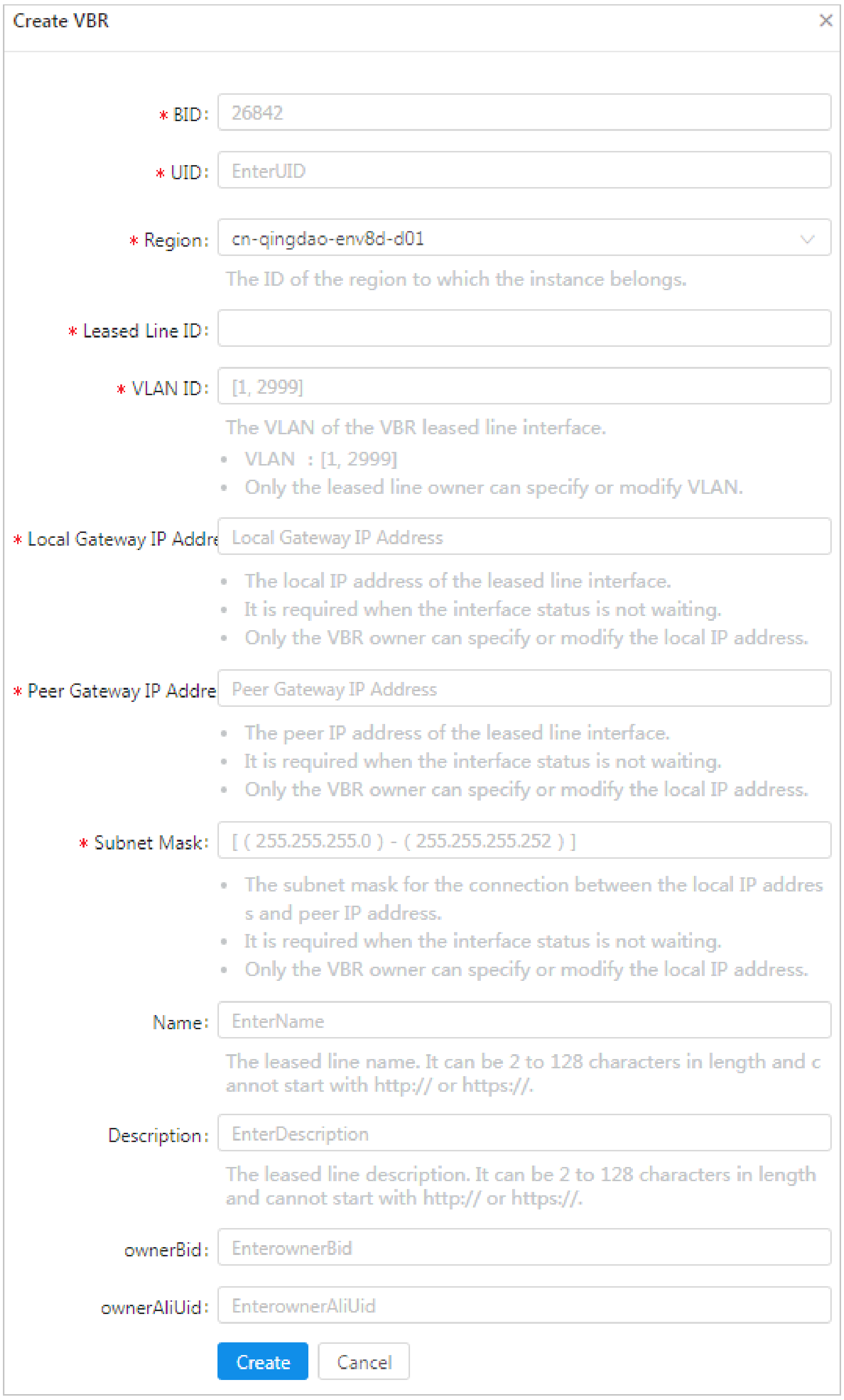
If the second attempt still fails, run the `vpcregiondb -e "select * from xnet_publish_task order by id desc limit 5"` command on the ECS availability group (AG). If an error is returned, you can check service logs in Network Management and Operations to troubleshoot the issue based on the returned error.

8.1.7.5. Create a VBR

A virtual border router (VBR) is a router between customer-premises equipment (CPE) and a VPC, and functions as a data forwarding bridge from a VPC to an on-premises IDC. This topic describes how to create a VBR in a region and query VBR information of the region.

Procedure

1. Log on to the Apsara Network Intelligence console.
2. From the **Products** menu, choose **Express Connect** > **Network Environment Management**.
3. Choose **Network Environment Management** > **VBRs**.
4. Click **Create VBR**.



Create VBR

* BID: 26842

* UID: EnterUID

* Region: cn-qingdao-env8d-d01

The ID of the region to which the instance belongs.

* Leased Line ID:

* VLAN ID: [1, 2999]

The VLAN of the VBR leased line interface.

- VLAN : [1, 2999]
- Only the leased line owner can specify or modify VLAN.

* Local Gateway IP Addre: Local Gateway IP Address

- The local IP address of the leased line interface.
- It is required when the interface status is not waiting.
- Only the VBR owner can specify or modify the local IP address.

* Peer Gateway IP Addre: Peer Gateway IP Address

- The peer IP address of the leased line interface.
- It is required when the interface status is not waiting.
- Only the VBR owner can specify or modify the local IP address.

* Subnet Mask: [(255.255.255.0) - (255.255.255.252)]

- The subnet mask for the connection between the local IP address and peer IP address.
- It is required when the interface status is not waiting.
- Only the VBR owner can specify or modify the local IP address.

Name: EnterName

The leased line name. It can be 2 to 128 characters in length and cannot start with http:// or https://.

Description: EnterDescription

The leased line description. It can be 2 to 128 characters in length and cannot start with http:// or https://.

ownerBid: EnterownerBid

ownerAliUid: EnterownerAliUid

5. Follow the on-screen prompts to configure the VBR parameters.

   The parameters are described as follows:

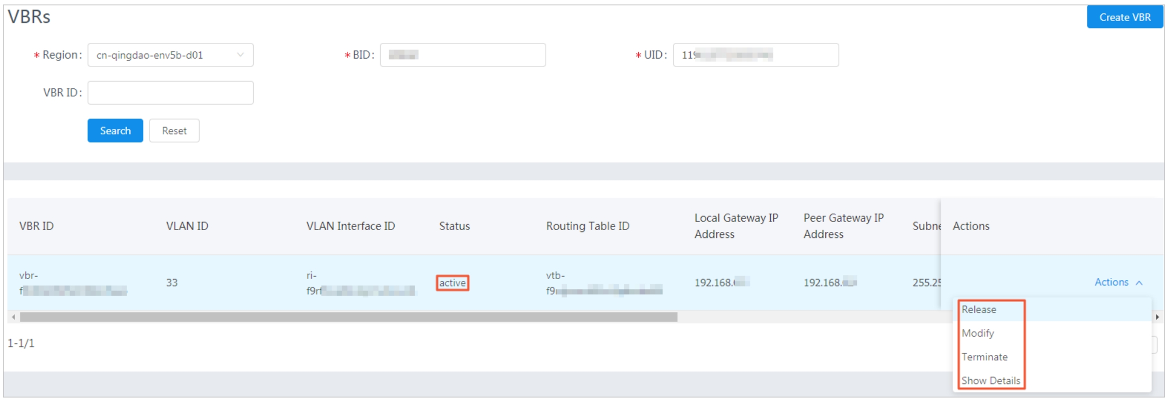
   - **Leased Line ID**: specifies the ID of the leased line that the VBR connects to.
   - **VLAN ID**: specifies the VLAN ID of the VBR. The value ranges from 0 to 2999.

     When creating router interfaces, you can use VLAN IDs to identify subsidiaries or departments that use the leased line, thus implementing Layer 2 network isolation between them.
   - **Local Gateway IP**: specifies the local IP address of the router interface for the leased line.
   - **Peer Gateway IP**: specifies the peer IP address of the router interface for the leased line.

  - **Subnet Mask**: specifies the subnet mask of the leased line between the local IP address and peer IP address.

    Only two IP addresses are required. Therefore, you can enter a longer subnet mask.

6. Click **Create**.
   When the VBR state is **Active**, the VBR is created.



* Region: cn-qingdao-env5b-d01
* BID: [redacted]
* UID: 11[redacted]
VBR ID:

VBR ID	VLAN ID	VLAN Interface ID	Status	Routing Table ID	Local Gateway IP Address	Peer Gateway IP Address	Subne	Actions
vbr- f[redacted]	33	ri- f9r[redacted]	active	vtb- f9[redacted]	192.168.[redacted]	192.168.[redacted]	255.25	Actions

1-1/1

You can click **Release**, **Modify**, **Terminate**, or **Show Details** in the **Actions** column to manage a VBR.

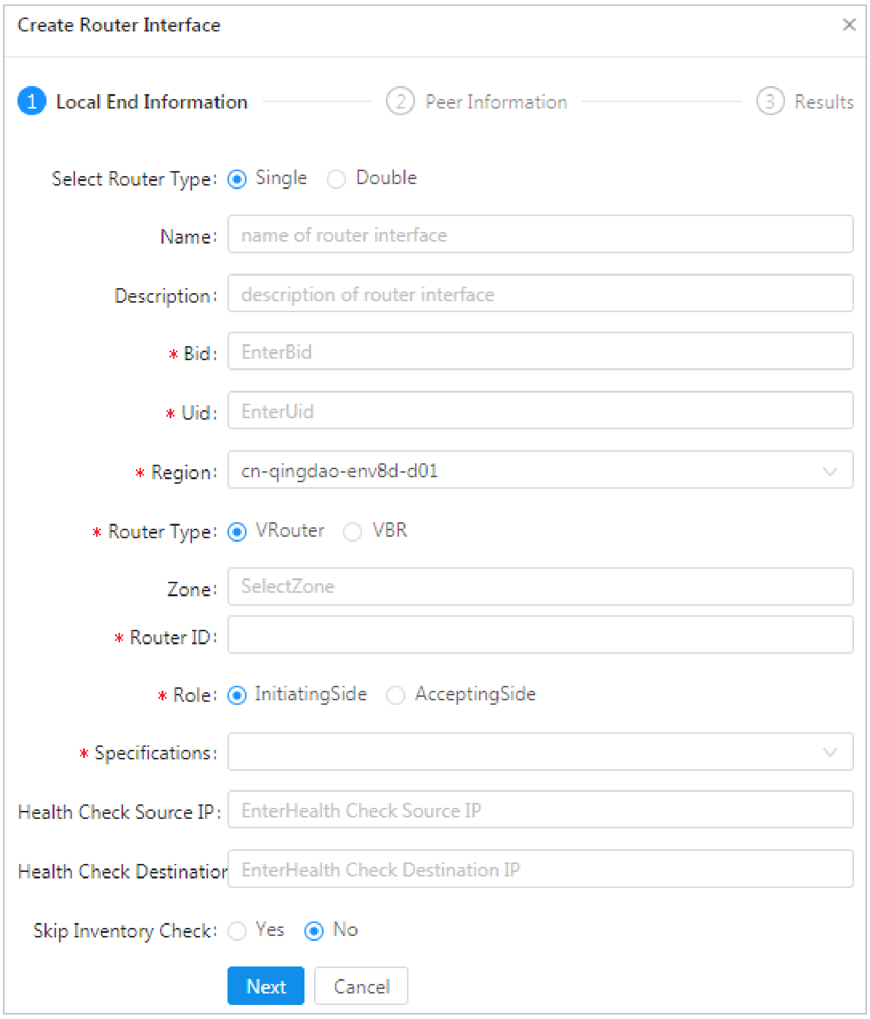
8.1.7.6. Create router interfaces

After you create a VBR, you must create a pair of router interfaces to connect the VBR and VPC. The connection initiator must be the VBR.

Procedure

1. Log on to the Apsara Network Intelligence console.
2. From the **Products** menu, choose **Express Connect** > **Network Environment Management**.
3. Choose **Network Environment Management** > **Router Interfaces**.
4. Click **Create Router Interface**.
5. Configure router interface parameters and click **Submit**.

   Set **Create Router Interface** to **Double**. Configure the local router interface based on the created VBR information, and configure the peer router interface based on the destination VPC information.



Create Router Interface

1 Local End Information — 2 Peer Information — 3 Results

Select Router Type: ● Single ○ Double

Name: name of router interface

Description: description of router interface

* Bid: EnterBid

* Uid: EnterUid

* Region: cn-qingdao-env8d-d01

* Router Type: ● VRouter ○ VBR

Zone: SelectZone

* Router ID:

* Role: ● InitiatingSide ○ AcceptingSide

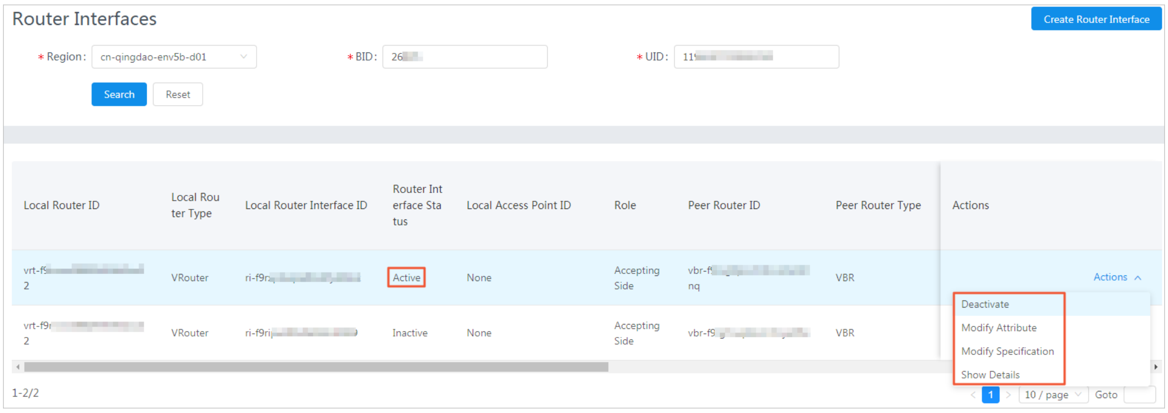
* Specifications:

Health Check Source IP: EnterHealth Check Source IP

Health Check Destinatior EnterHealth Check Destination IP

Skip Inventory Check: ○ Yes ● No

When the router interface state is **Active**, the interface is created.



Router Interfaces

* Region: cn-qingdao-env5b-d01 * BID: 26[redacted] * UID: 11[redacted]

Local Router ID	Local Router Type	Local Router Interface ID	Router Interface Status	Local Access Point ID	Role	Peer Router ID	Peer Router Type	Actions
vrt-f[redacted]2	VRouter	ri-f9r[redacted]	Active	None	Accepting Side	vbr-f[redacted]nq	VBR	Actions
vrt-f9[redacted]2	VRouter	ri-f9ri[redacted]	Inactive	None	Accepting Side	vbr-f9[redacted]	VBR	

1-2/2

8.1.7.7. Create a routing table

A routing table is a list of route entries on a VRouter. This topic describes how to create routing tables in a region and query the routing table information of a region.

Procedure

1. Perform the following steps to add routes on a VBR destined for a VPC and an IDC:

   i. Log on to the Apsara Network Intelligence console.

i. Log on to the Apsara Network Intelligence console.

ii. From the **Products** menu, choose **Express Connect > Network Environment Management**.

iii. Choose **Function Modules > Routing Tables**.

iv. Set search conditions such as Region, BID, UID, Router Type, Routing Table ID, and Router ID, and click **Search** to query routing tables.

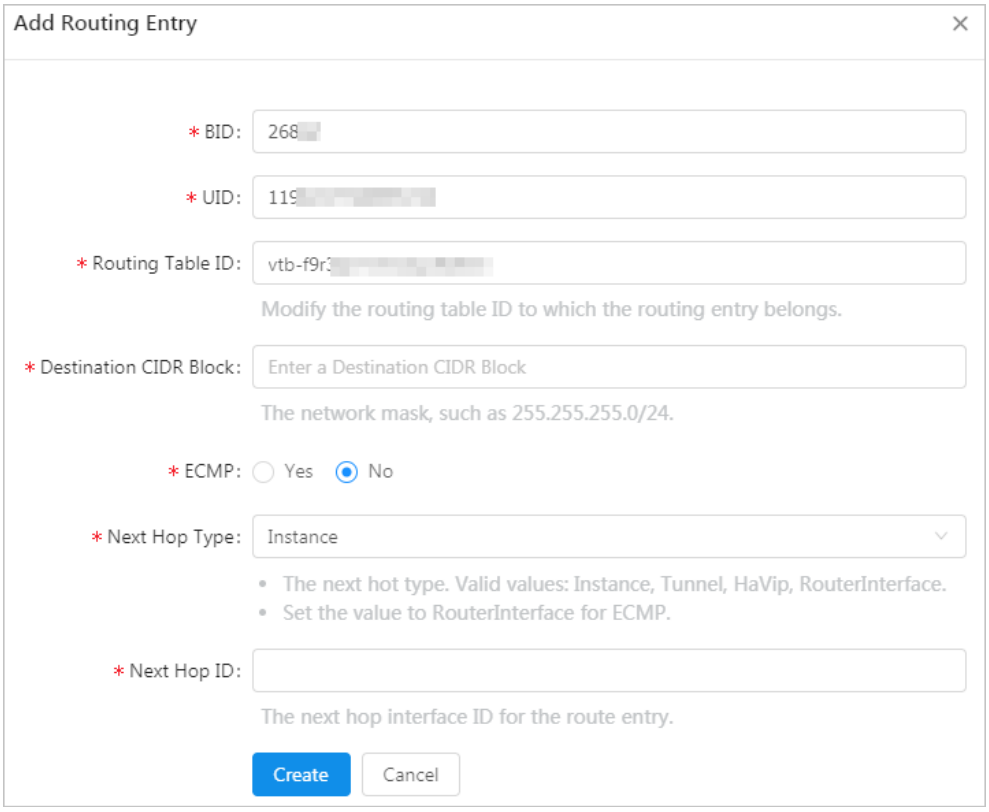
v. Click **Add Route Entry** in the **Actions** column corresponding to a routing table.

vi. Specify a route entry destined for the CIDR block of a destination VPC, and click **Create**.

The parameters are described as follows:

- **Destination CIDR Block**: the destination CIDR block.
- **Next Hop Type**: the next hop type.
- **Next Hop Instance ID**: the ID of the next hop instance for the specified next hop type.

Add a route destined for a destination VPC



Add Routing Entry

* BID:	268[redacted]
* UID:	119[redacted]
* Routing Table ID:	vtb-f9r[redacted] Modify the routing table ID to which the routing entry belongs.
* Destination CIDR Block:	Enter a Destination CIDR Block The network mask, such as 255.255.255.0/24.
* ECMP:	○ Yes ● No
* Next Hop Type:	Instance • The next hot type. Valid values: Instance, Tunnel, HaVip, RouterInterface. • Set the value to RouterInterface for ECMP.
* Next Hop ID:	 The next hop interface ID for the route entry.

vii. Repeat the preceding steps to add a route destined for a target IDC.

> ⓘ **Note** You can navigate to the VBRs page and locate the **VLAN Interface ID** area to obtain next hop router interface information.

2. Add a route destined for the router interface of a VBR in the VPC.

3. On the gateway of the on-premises IDC, configure a route destined for the VPC.

8.1.8. Manage Business Foundation System flows in a VPC

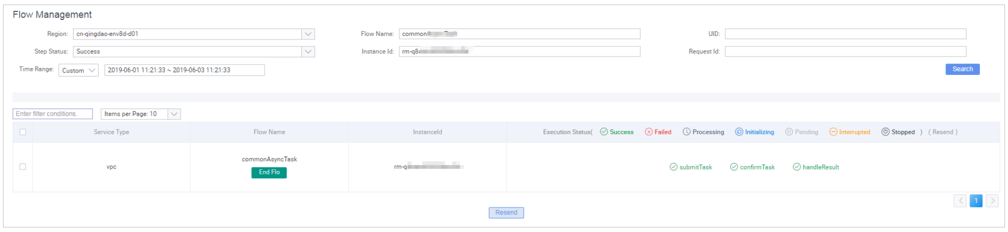
You can view the execution state of tasks in a VPC and restart the tasks as needed.

Procedure

1. Log on to the Apsara Network Intelligence console.
2. From the **Products** menu, choose **Network Controller > Business Foundation System Flow**.
3. Query the flow state of the task you want to view.

   Enter a leased line ID in **Instance ID** and set **Step Status** to **All** to check the flow status. A flow in red indicates that the corresponding step has failed. Click **Resend** to restart the task, and then requery the flow status.

   Flow Management page

   Flow Management

   Region: cn-qingdao-env8d-d01
   Flow Name: common[redacted]
   UID:
   Step Status: Success
   Instance Id: rm-q8[redacted]
   Request Id:
   Time Range: Custom 2019-06-01 11:21:33 ~ 2019-06-03 11:21:33

□	Service Type	Flow Name	InstanceId	Execution Status(✓ Success ⊗ Failed ◷ Processing Initializing Pending Interrupted Stopped) (Resend)
□	vpc	commonAsyncTask End Flo	rm-q[redacted]	✓ submitTask ✓ confirmTask ✓ handleResult

8.1.9. Configure reverse access to cloud services

Cloud services cannot be directly accessed from external networks. You must configure reverse access to allow external networks to access cloud services.

Prerequisites

Log on to the Apsara Uni-manager Operations Console, and obtain the **AccessKey ID** and **AccessKey secret** on the **Personal Information** page.

Procedure

1. Log on to the Apsara Network Intelligence console.
2. In the top navigation bar, click **Products**, and choose **Cloud Service Management > Cloud Service Reverse Access**.
3. Enter the **AccessKey ID** and **AccessKey secret** and click **OK**.
4. On the **Cloud Service Reverse Access** page, click **Create Cloud Service Reverse Access**.
5. On the **Allocate Cloud Service ID** wizard page, select a region and enter a name and description.
6. Click **Continue**. The following information is automatically created and displayed on the **Create Address Pool** wizard page: the application ID of the cloud service that allows reverse access and the address pool that is used for reverse access to the cloud service.
7. Click **Continue**. On the **Add Server Address** wizard page, configure the Elastic Compute Service (ECS) instance to be used for reverse access.
   - **VPC ID**: Enter the ID of a virtual private cloud (VPC) and an ECS instance, or a single-tunnel cloud service instance.

   - **Server IP**: Enter the IP address of the ECS instance to be used for reverse access.

8. Click **Continue**. On the **Create Mapping IP** wizard page, enter the ID of a vSwitch and the mapping IP address of the ECS instance. The IP address is used to allow access from external networks.
9. Click **Continue**. On the **Complete Authorization** wizard page, specify VPC ID, Server IP, and Instance Port for reverse access.

   Separate multiple port numbers with commas (,). For example, `10,20,30`. You can specify up to 10 ports.

8.2. Network Management and Operations

8.2.1. Overview

This topic provides an overview of the Apsara Stack Network Operation Platform (NET). NET is a platform where network construction and O&M activities (including planning, design, construction, delivery, maintenance, changing, scheduling, and offlining) are transformed from **offline procedures** into **online automated processes**.

NET allows you to establish connections between physical network devices by using Secure Shell (SSH), Telnet, Simple Network Management Protocol (SNMP), RESTCONF, or gRPC Remote Procedure Calls (gRPC), and facilitates the creation of subsystems in O&M phases.

NET has the following features:

- Network automation

  The network automation feature allows you to establish connections by using protocols such as SSH, SNMP, and Telnet. You can create template scripts in Python to manage and organize upper-layer O&M systems and businesses.

- Change center

  NET provides a change automation engine that operates based on automation templates. You can use the features of the change center to orchestrate the execution sequence and correlations in the templates based on your business scenarios and O&M experience to formulate standardized and reusable change management plans. Such change management plans can be automatically implemented by the system to improve efficiency and reduce the risk of human errors.

Intended users

Network engineers who are responsible for construction, operation, and engineering change management of IT infrastructure.

8.2.2. Log on to the Network Management and Operations operations console

This topic describes how to log on to the Network Management and Operations console.

Prerequisites

- You must log on to the the Apsara Uni-manager Operations Console to access Network Management and Operations. Before you start, you must obtain the URL, username, and password of the Apsara

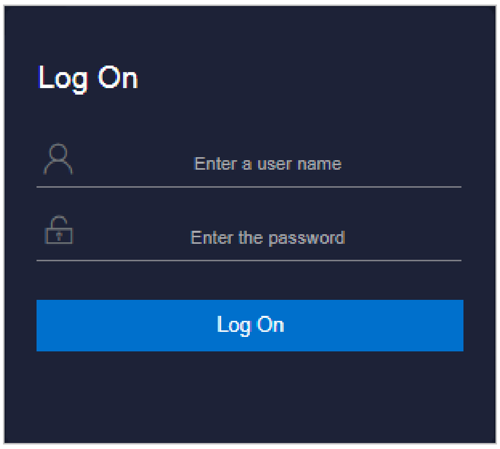
Uni-manager Operations Console from the engineer that deploys the service.

The URL of the Apsara Uni-manager Operations Console is in the `ops.asconsole.intranet-domain-id.com` format.

- We recommend that you use the Google Chrome browser.

Procedure

1. Open your browser.
2. In the address bar, enter the URL of the Apsara Uni-manager Operations Console: `ops.asconsole.intranet-domain-id.com` and press enter.
3. Enter your username and password.

   > Note You can select a language from the drop-down list in the upper-right corner of the page.

   If this is the first time you log on to the Apsara Uni-manager Operations Console, you must change your password as prompted.

   For higher security, make sure that the password meets the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password is 10 to 20 characters in length.
4. Click **Log On** to navigate to the **Apsara Uni-manager Operations Console** homepage.
5. In the top navigation bar, click **O&M**.
6. In the left-side navigation pane, choose **Product Management** > **Product List**.
7. In the **Infrastructure as a Service (IaaS)** section, click **Network Management and Operations**.

8.2.3. Network Automation

8.2.3.1. Manage devices

This topic describes how to query, add, modify, and delete a device. After the NET system is started, the backend services automatically synchronize the data of physical network devices in the planning information to Apsara Infrastructure Management Framework.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Net Automation > Device Management**.The list of network devices appears on the page.
3. You can perform the following operations on physical switches.
   - Query

     Enter device properties and click **Search** to display the filtered results.
   - Modification

     Find the target device and click the ✎ icon in the **Actions** column. On the **Update Device** page, modify the device settings.

     > **Note** If you do not set a user name and password, your Apsara Stack user name and password will be used for task execution. For more information about accounts, contact the O&M personnel.
   - Addition

     Find the target device and click the ❐ icon in the **Actions** column. On the **Add Device** page, add a new device.

     > **Note** The hostname, IP address, and serial number must be globally unique.
   - Deletion

     Find the target device and click the 🗑 icon in the **Actions** column to delete the device.

8.2.3.2. Configure templates

8.2.3.2.1. Overview

This topic provides a brief overview of template configuration on NET. You can create template scripts in Python and configure input parameters.

The following features are supported:

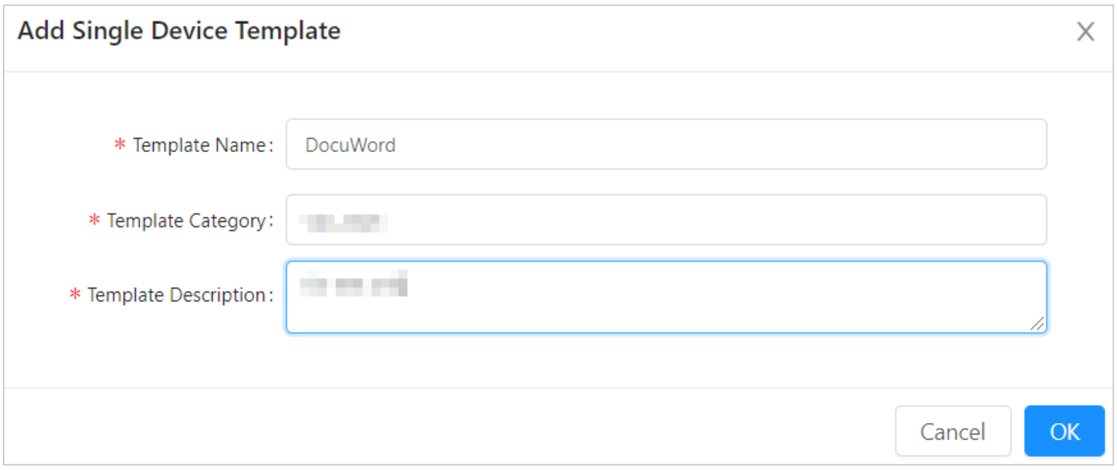
- Using third-party libraries to abstract the capabilities of establishing connections and running command-line interface (CLI) commands to built-in methods (functions).
- Using nested templates to flexibly design device operations and structure business logic.

8.2.3.2.2. Create a device template

This topic describes how to create a device template. Device templates are applied to devices. By default, the system performs device logon and logoff before and after executing the scripts of a device template. The commands contained in a device template are run based on the built-in exec_cli method.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Net Automation > Device Templates**.
3. Add a single device template.
   i. Click **Add Single Device Template**.



Add Single Device Template

* Template Name: DocuWord

* Template Category: [redacted]

* Template Description: [redacted]

   ii. Configure the device template.
   - **Template Name**: Enter a name for the template.
   - **Template Category**: Specify a category for the device template. Device templates can be classified into different categories for merged queries.

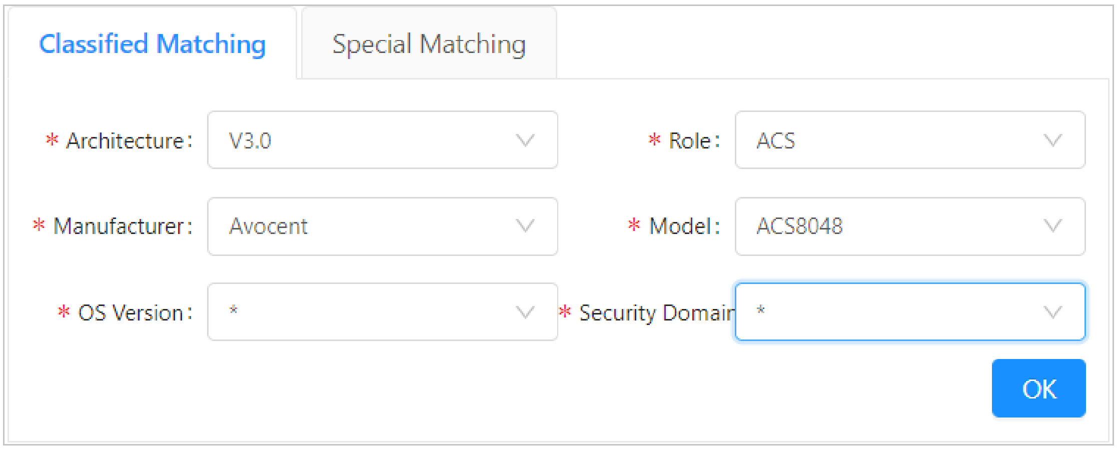
     You can select an existing template category from the drop-down list.

     To create a new template category, enter a name for the category and then click **OK**.
   - **Template Description**: Enter a description for the template.

   iii. Click **OK**.

4. Find the target template and click the ✎ icon in the **Actions** column to add a rule to the template.
   i. Click **Add Template**.

ii. Click the **Classified Matching** tab. You can add rules based on the six tuples of different devices.



* Architecture: V3.0

* Role: ACS

* Manufacturer: Avocent

* Model: ACS8048

* OS Version: *

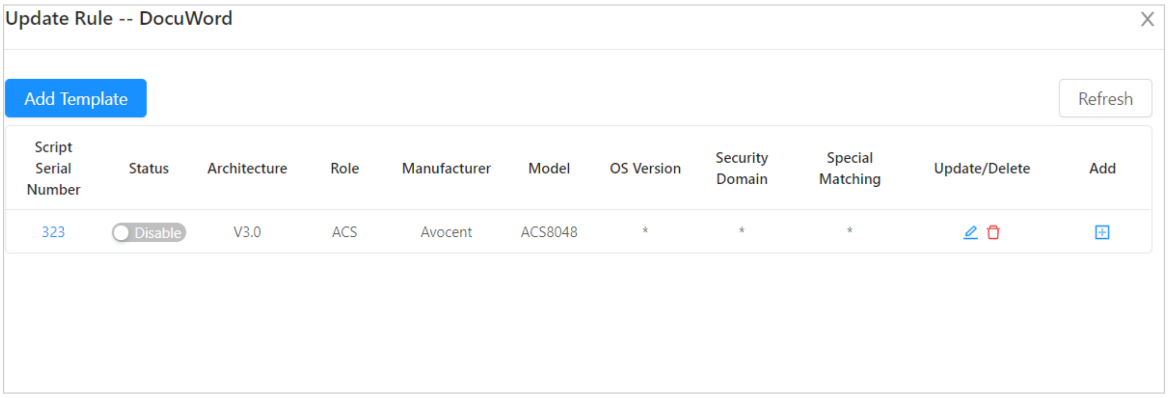
* Security Domain: *

Since configuration commands vary by device model and manufacturer, you can select asterisk (*****) from the drop-down list to denote an absence or omission of information.

> **Note** You can click the **Special Matching** tab and enter the hostnames to which this template is applicable. Multiple hostnames must be separated with line breaks.

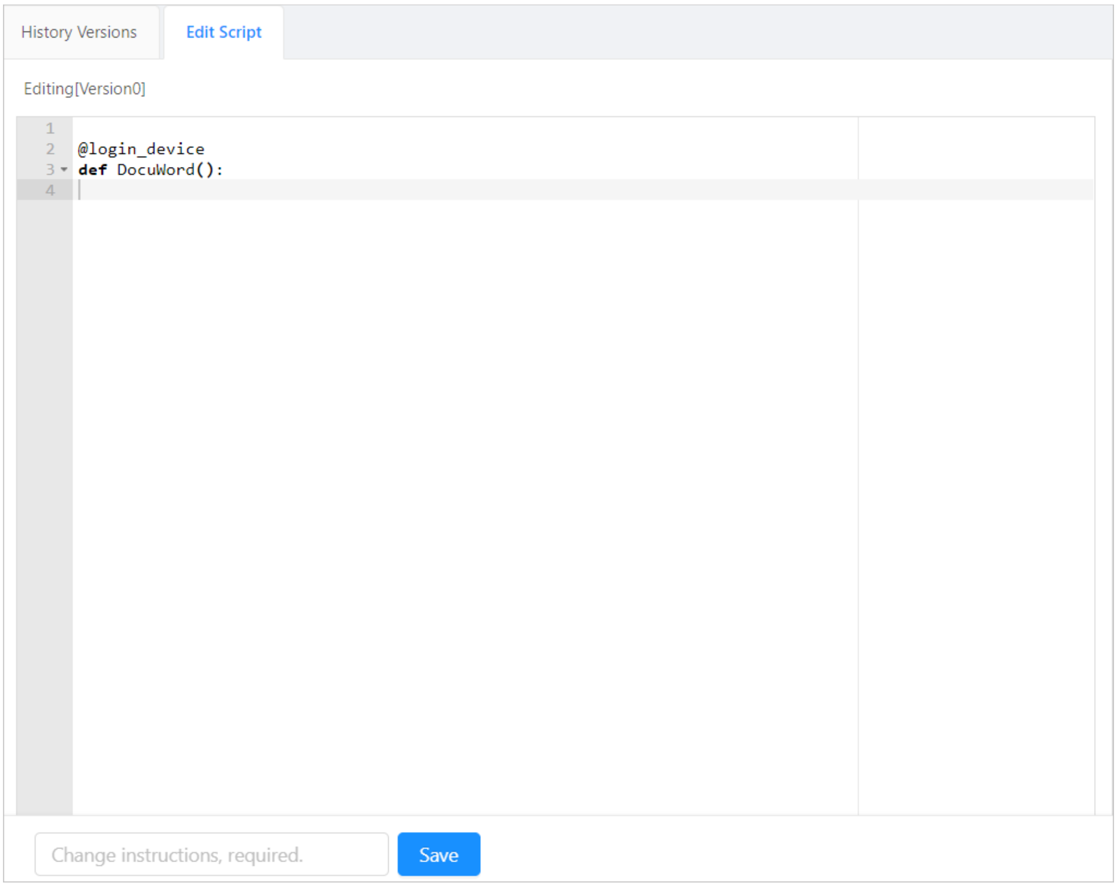
iii. Click **OK**.

5. On the **Update Rule** page, click the serial number of a script to write template code.



Script Serial Number	Status	Architecture	Role	Manufacturer	Model	OS Version	Security Domain	Special Matching	Update/Delete	Add
323	Disable	V3.0	ACS	Avocent	ACS8048	*	*	*		

i. On the **Edit Script** tab, write the script.



```
@login_device
def DocuWord():
```

The login decorator (device_login) and function name (template name) of the device template use default values. You only need to import a library, such as re or JSON, as needed.

The following example illustrates how to query the platform version. The exec cli is a built-in function that can be used directly, which is equivalent to running the `display version` command and returning the version information.

```
import re
@login_device
def get_software_version():
  output = exec_cli("display version")
  version = re.findall(r'[Ss]oftware, Version (\d+.\d+.? \d*)', output)[0]
  return version
```

ii. Enter the change instructions and click **Save**.

iii. On the **History Versions** tab, click **Release**.

> **Note**
>
> Each **Save** operation generates an entry recorded in the **History Versions**. Such scripts are classified as test scripts by default. You can select a test script and click **Release** to change its version from test to release. Only the scripts of the release version can be executed online.

6. (Optional)In the left-side navigation pane, choose **Net Automation > Device Templates**. Find

the target template and then click the ✎ icon in the **Actions** column. In the dialog box that appears, modify the name, category, and description of the template.

7. (Optional)In the left-side navigation pane, choose **Net Automation > Device Templates**. Find the target device template and then click the ✎ icon in the **Actions** column to update the rules of the template.
8. (Optional)In the left-side navigation pane, choose **Net Automation > Device Templates**. Find the target device template and then click the 🗑 icon in the **Actions** column to delete the device template.

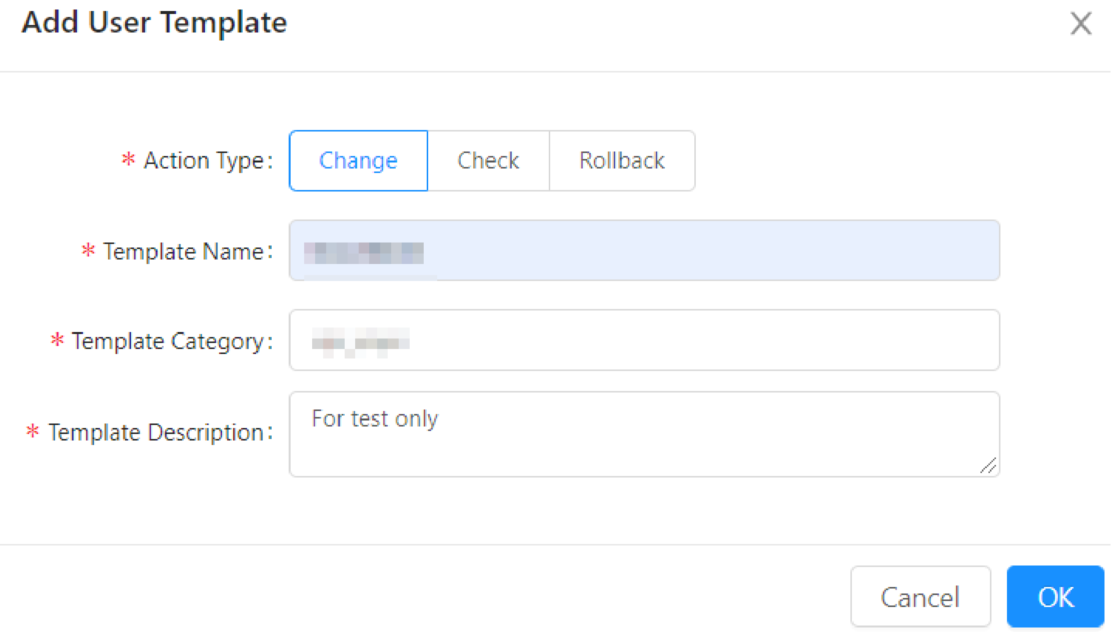
8.2.3.2.3. Create a user template

This topic describes how to create a user template. User templates are not related to devices. You can write user template code in Python, and use the built-in exec_script method to call other templates.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Net Automation > User Templates**.
3. Add a user template.
   i. Click **Add User Template**.

ii. In the **Add User Template** dialog box, configure the user template.



Add User Template

* Action Type: Change | Check | Rollback

* Template Name: [redacted]

* Template Category: [redacted]

* Template Description: For test only

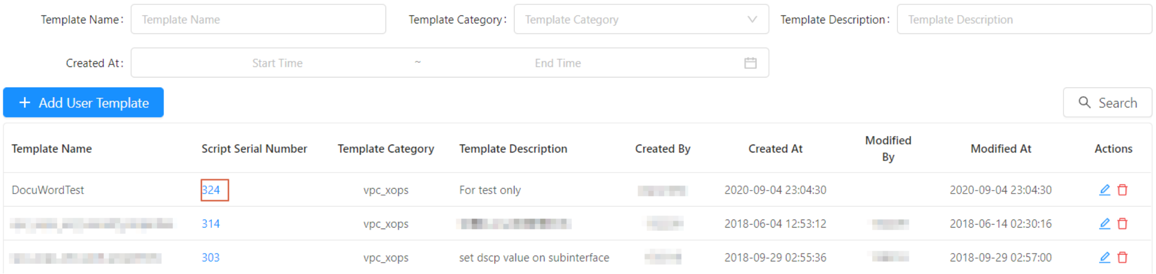
- **Action Type**: Select the action type for the user template. You can select one from **Change**, **Check**, and **Rollback**.
- **Template Name**: Enter a name for the user template.
- **Template Category**: Specify a category for the user template. User templates can be classified into different categories for merged queries.

  You can select an existing template category from the drop-down list.

  You can also enter a category name to create a new template category.
- **Template Description**: Enter a description for the user template.

iii. Click **OK**.

4. On the **User Templates** page, find the target user template and click the corresponding script serial number to edit the script.

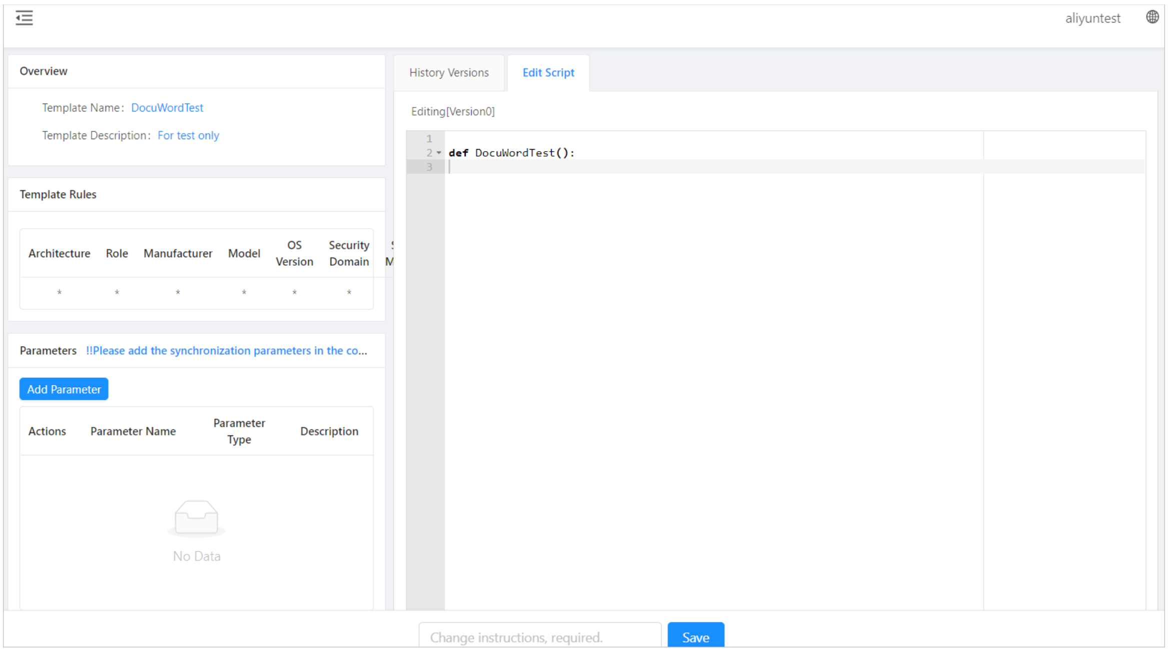


Template Name: Template Name　Template Category: Template Category　Template Description: Template Description

Created At: Start Time ~ End Time

Template Name	Script Serial Number	Template Category	Template Description	Created By	Created At	Modified By	Modified At	Actions
DocuWordTest	324	vpc_xops	For test only	[redacted]	2020-09-04 23:04:30		2020-09-04 23:04:30	✎ 🗑
[redacted]	314	vpc_xops	[redacted]	[redacted]	2018-06-04 12:53:12	[redacted]	2018-06-14 02:30:16	✎ 🗑
[redacted]	303	vpc_xops	set dscp value on subinterface	[redacted]	2018-09-29 02:55:36	[redacted]	2018-09-29 02:57:00	✎ 🗑

5. On the **Edit Script** tab, add parameters and write the script.



Template Name: DocuWordTest

Template Description: For test only

Template Rules

Architecture	Role	Manufacturer	Model	OS Version	Security Domain
*	*	*	*	*	*

Parameters !!Please add the synchronization parameters in the co...

Actions	Parameter Name	Parameter Type	Description

No Data

Editing[Version0]

```
def DocuWordTest():
```

Change instructions, required.

Call get_software_version to check whether the software version of the device meets the delivery requirement:

```
def check_device_version(device, version):
  """
  Check whether the OS version of the device meets the requirement
  : param device: the device name.
  : param version: the version number.
  : return: OK is returned if the version meets the requirement. Otherwise, an abort error is returned.
  """
  # Call get_software_version to retrieve the version number.
  # Call other templates by using the built-in exec_script method.
  # To call a device template, set the first parameter as the device template name and the second param
eter as the device name, which is followed by other parameters of the device template.
  # To call a user template, set the first parameter as the user template name, which is followed by othe
r parameters of the user template.
  dev_ver = exec_script("get_software_version", device)
  # Compare the retrieved version number of the device with the input parameter. If the version numbe
rs match, OK is returned. Otherwise, an abort error is returned.
  # abort is a built-in method, which is similar to raise Exception in Python.
  if version == dev_ver:
    return "OK"
  else:
    abort("version not match, input:%s <-> real:%s" % (version, dev_ver))
```

- The device_login decorator is unavailable because user templates are unrelated to devices.
- You can add parameters to a template function by clicking **Add Parameter** on the left side of the page. Parameters added otherwise will be discarded.
- In the template code, exec_script is a built-in method for nested calls to other templates.
- In the template code, abort is a built-in method that is used to throw an exception when a task fails. A normal return value indicates that the task has succeeded.

6. Enter the change instructions and click **Save**.

7. On the **History Versions** tab, click **Release**.

> ? Note
>
> Each **Save** operation generates an entry recorded in the **History Versions**. Such scripts are classified as test scripts by default. You can select a test script and click **Release** to change its version from test to release. Only the scripts of the release version can be executed online.

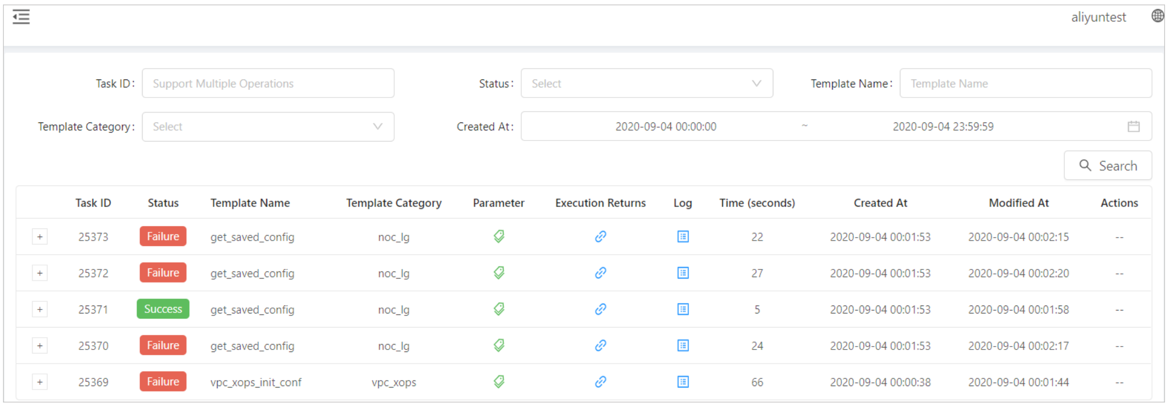
8. (Optional)In the left-navigation pane, choose **Net Automation** > **User Templates**. On the **User Templates** page, find the target user template and click the icon ✎ in the **Actions** column. In the dialog box that appears, modify the action type, and the name, category, and description of the user template.
9. (Optional)In the left-navigation pane, choose **Net Automation** > **User Templates**. On the **User Templates** page, find the target user template and click the 🗑 icon in the **Actions** column to delete the user template.

8.2.3.3. Manage change tasks

This topic describes how to manage change tasks on NET. Change tasks are triggered by platform applications or external API calls. After you specify the information such as the name of the task entry template and necessary parameters, the system automatically executes logic in the background based on the online template script.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Net Automation** > **Task Management**. The list of change tasks appears on the page.



Task ID: Support Multiple Operations
Status: Select
Template Name: Template Name
Template Category: Select
Created At: 2020-09-04 00:00:00 ~ 2020-09-04 23:59:59

	Task ID	Status	Template Name	Template Category	Parameter	Execution Returns	Log	Time (seconds)	Created At	Modified At	Actions
+	25373	Failure	get_saved_config	noc_lg	🏷	🔗	▤	22	2020-09-04 00:01:53	2020-09-04 00:02:15	--
+	25372	Failure	get_saved_config	noc_lg	🏷	🔗	▤	27	2020-09-04 00:01:53	2020-09-04 00:02:20	--
+	25371	Success	get_saved_config	noc_lg	🏷	🔗	▤	5	2020-09-04 00:01:53	2020-09-04 00:01:58	--
+	25370	Failure	get_saved_config	noc_lg	🏷	🔗	▤	24	2020-09-04 00:01:53	2020-09-04 00:02:17	--
+	25369	Failure	vpc_xops_init_conf	vpc_xops	🏷	🔗	▤	66	2020-09-04 00:00:38	2020-09-04 00:01:44	--

8.2.3.4. Trigger real-time tasks

This topic describes how to trigger real-time tasks by using device templates.

Procedure

1. Log on to the NET console.

2. In the left-side navigation pane, choose **Net Automation > Real-time Tasks**.
3. In the **Real-time Task Execution** section, select a device template and set the parameters for the real-time task.
4. Click **Execute**. After the execution, you can check the execution result in the **Task Execution Results** section.

8.2.3.5. Manage files

This topic describes how to upload the configuration files of devices by using the file management feature of the NET platform.

Procedure

1. Log on to the NET console.
2. In the left-side navigation page, choose **Net Automation > File Management**.
3. Click **Upload**. In the **Upload File** dialog box, specify the file type, hostname, serial number, and description, and then select the file to be uploaded.
4. Click **Submit**.

8.2.4. Network monitoring

8.2.4.1. Dashboards

8.2.4.1.1. Check the status of a device

This topic describes how to check the status of a device by using the status view feature.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Network Monitor > Monitor View > Status View**.
3. Select the target device and the event types.
4. Click **Search**.
5. Click the 👁 icon in the **Details** column to check the monitoring details.

8.2.4.1.2. Check the aggregate status

This topic describes how to check the aggregate status. The aggregate status displays the numerical aggregation of status data collected from monitored single devices.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Network Monitor > Monitor View > Aggregate Status**.

3. Select the alarm status, aggregate data, and aggregate type, and then enter the data items.
4. Click **Search** to check the aggregate status.

8.2.4.1.3. Check the data view

This topic describes how to view monitoring data by using the data view feature. You can use the data view feature to display the dashboards that visualize the data collected based on monitor settings.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Network Monitor > Monitor View > Data View**.
3. Enter one or more keywords in the search bar, and click **Search**.

8.2.4.2. Configuration management

8.2.4.2.1. Add a monitoring item

This topic describes how to configure monitoring by adding monitoring items. For each monitoring item, you can specify a collection type, such as PING or Simple Network Management Protocol (SNMP), define a collection interval, set data items, and add alarm rules.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Network Monitor > Configuration > Monitoring Items**.
3. On the **Monitoring Items** page, click **Add Monitoring Item**.
4. On the **Monitoring Item Management** page, configure the monitoring item.The following configuration parameters are included:
    - **Monitoring Item Name**: Specify a name for the monitoring item. The name must be globally unique. We recommend that you use a name that describes the feature of the monitoring item.
    - **Description**: Enter a comprehensive description of the feature of the monitoring item. A detailed description helps increase maintenance efficiency.
    - **Security Domain**: Security domains are not interconnected. Multiple Server Load Balancer (SLB) instances can be added in each security domain.
    - **Collection Type**: Select a collection type from the displayed options. PING and SNMP are the most common collection types.
        - PING: The device is pinged periodically based on the configuration to calculate the packet loss rate and latency. After you select PING as the collection type, you must set values for constant, interval, and packNum.
        - SNMP: Different types of data are collected based on the definitions of object identifiers (OIDs). After you select SNMP as the collection type, you must define the OIDs supported by the device, set a password, and specify the data types to be monitored.
    - **Effective**: Select whether to apply the monitoring item. If this parameter is set to NO, the monitoring agent does not collect data as the monitoring item specifies. We recommend that

you perform debugging first, and then set the monitoring item to be effective if no anomaly is detected.

- **Execution Interval**: Specify a time interval for periodic data collection. We recommend that you set the interval to one minute for PING or SNMP monitoring to avoid undetectable anomalies across long intervals.
- **Parsing Code**: The system formats and parses the data collected by the agent, and returns the data items in the specified format.
- **Data Item**: Set the data items to be collected for the monitoring item. This is an optional parameter.
- **Alarm Rules**: The system categorizes alarms into five status conditions: normal, warning, critical, error, and waiting.

  You can specify the rules for warning and critical alarms. The system changes the alarm status based on the specified rules.

5. Click **Debugging**.
6. Click **Submit**.

8.2.4.2.2. Add a notification group

This topic describes how to add a notification group to subscribe the intended recipients to receive notifications. You can use notification groups to reduce maintenance costs for subscriptions.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, click **Network Monitor > Configuration > Notification Group**.
3. Click **Add Notification Group**.
4. In the **Add** dialog box, specify the name, description, and contacts of the notification group.
5. Click **OK**.

8.2.4.2.3. Subscription management

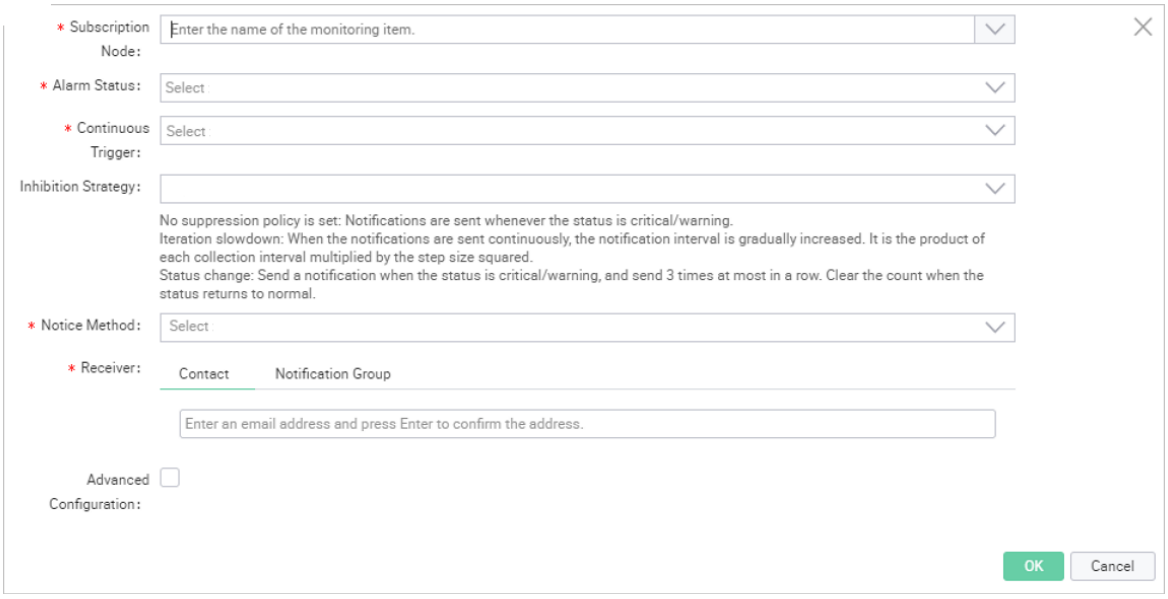
8.2.4.2.3.1. Subscribe to single-device notifications

This topic describes how to create a single-device notification subscription. Single-device alarms of different levels are generated based on configured alarm rules for the data collected by monitoring items, and are sent as emails, SMS messages, or DingTalk messages to specified recipients or notification groups.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Network Monitor > Configuration > Subscription**.
3. Click the **Subscribe Single Device Alarm** tab.
4. Click **Add Subscription**.
5. In the dialog box that appears, configure the subscription.The following configuration parameters are included:

   - **Subscription Node**: Set a monitoring item.
   - **Alarm Status**: Select the status that triggers the notification.
   - **Continuous Trigger**: You can set this parameter to 2 to prevent excessive false alarms. In this case, a notification is not triggered when the status changes from normal to warning or critical for the first time, and is only triggered if such a change occurs for the second time.
   - **Inhibition Strategy**: Select an inhibition strategy from the drop-down list.
     - No suppression policy is set: A notification is sent whenever the status becomes critical or warning.
     - Iteration slowdown: The notification intervals are prolonged with each successive notification, and a notification interval is the collection interval multiplied by the nth power of the step size.
     - Status change: Notifications are sent when the status becomes critical or warning, and can only be sent up to three consecutive times. When the status returns to normal, the count of notifications is reset back to zero.
   - **Notice Method**: Select a method for sending notifications.
   - **Receiver**: Enter recipient information or select a notification group.
   - **Advanced Configuration**: Configure fine-grained filtering based on the on-premises data center or role to which the device belongs.



No suppression policy is set: Notifications are sent whenever the status is critical/warning.
Iteration slowdown: When the notifications are sent continuously, the notification interval is gradually increased. It is the product of each collection interval multiplied by the step size squared.
Status change: Send a notification when the status is critical/warning, and send 3 times at most in a row. Clear the count when the status returns to normal.

6. Click **OK**.

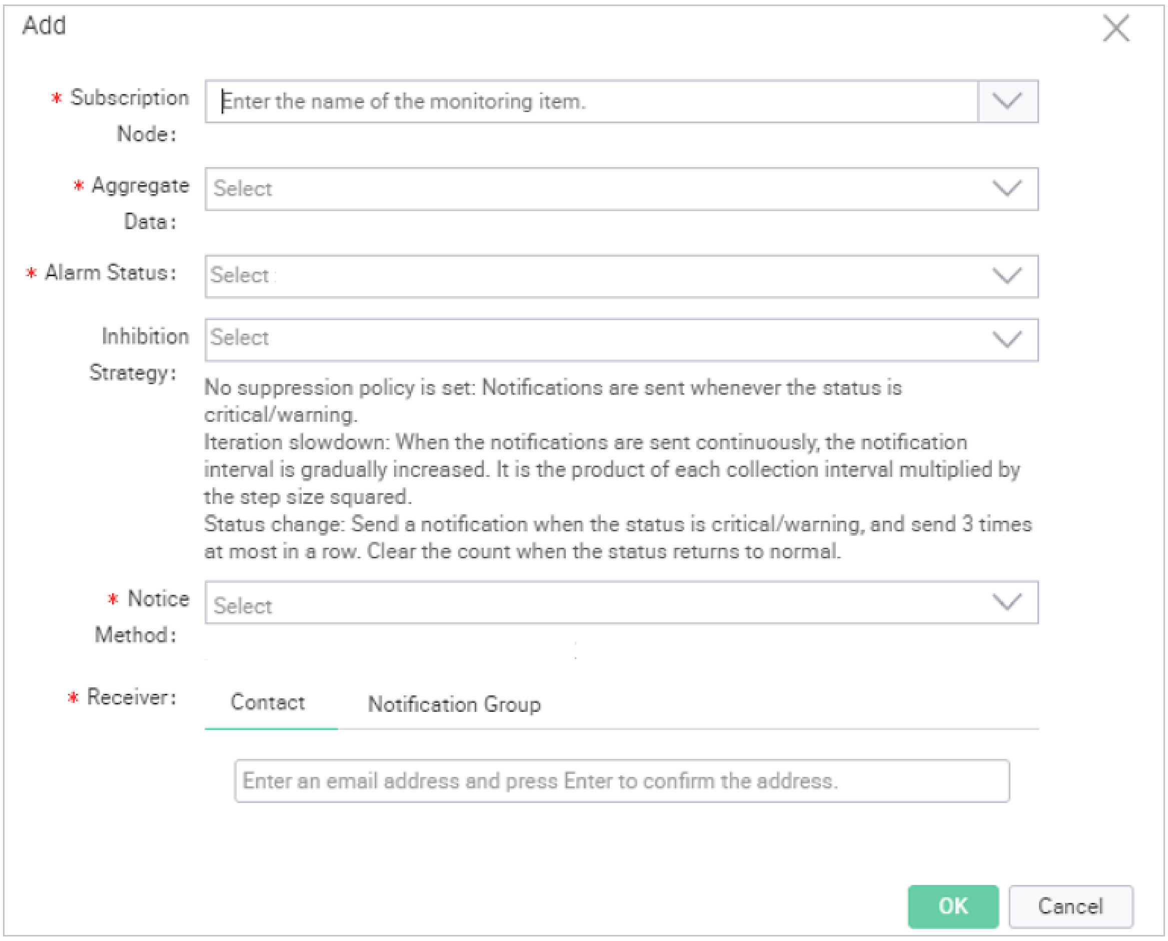
8.2.4.2.3.2. Subscribe to aggregate notifications

This topic describes how to create an aggregate notification subscription. Aggregate alarms of different levels are generated based on configured alarm rules for the data collected by monitoring items, and are sent as emails, SMS messages, or DingTalk messages to specified recipients or notification groups.

Procedure

1. Log on to the NET console.

2. In the left-side navigation pane, choose **Network Mnitor > Configuration > Suscription**.
3. Click the **Subscription Aggregate Alarm** tab and then click **Add Subscription**.
4. In the **Add** dialog box, configure the subscription.The following configuration parameters are included:
   - **Subscription Node**: Set a monitoring item.
   - **Aggregate Data**: Select aggregate data.
   - **Alarm Status**: Select the status that triggers the notification.
   - **Inhibition Strategy**: Select an inhibition strategy from the drop-down list.
     - No suppression policy is set: A notification is sent whenever the status becomes critical or warning.
     - Iteration slowdown: The notification intervals are prolonged with each successive notification, and a notification interval is the collection interval multiplied by the nth power of the step size.
     - Status change: Notifications are sent when the status becomes critical or warning, and can only be sent up to three consecutive times. When the status returns to normal, the count of notifications is reset back to zero.
   - **Notice Method**: Select a method for sending notifications.
   - **Receiver**: Enter recipient information or select a notification group.



No suppression policy is set: Notifications are sent whenever the status is critical/warning.
Iteration slowdown: When the notifications are sent continuously, the notification interval is gradually increased. It is the product of each collection interval multiplied by the step size squared.
Status change: Send a notification when the status is critical/warning, and send 3 times at most in a row. Clear the count when the status returns to normal.

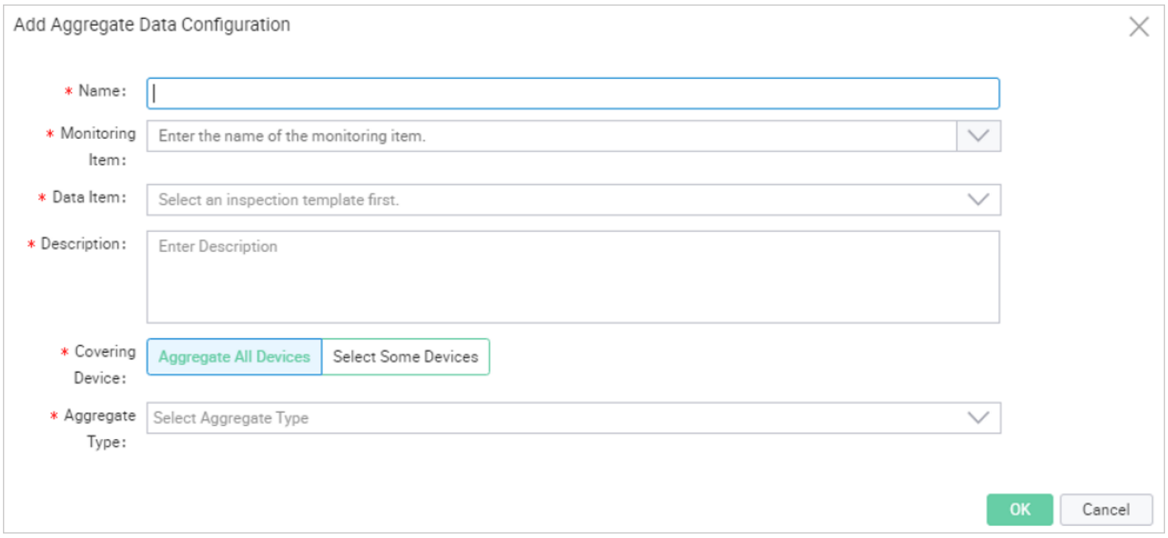
5. Click **OK**.

8.2.4.2.4. Add an aggregate data configuration

This topic describes how to add an aggregate data configuration. Aggregate data is the compilation of data sourced from one or more monitored devices, and is aggregated to calculate the maximum, minimum, average, or sum value of the data objects.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Network Monitor > Configuration > Aggregate Data Configuration**.
3. On the **Aggregate Data Configuration** tab, click **Add Aggregate Data Configuration**.
4. In the **Add Aggregate Data Configuration** dialog box, complete the configuration.The following configuration parameters are included:
    - **Name**: Enter a name for the aggregate data. The name must be globally unique.
    - **Monitoring Item**: Select the monitor item where the data to be aggregated is located.
    - **Data Item**: After the monitoring item is specified, select a data item from the drop-down list.
    - **Description**: Enter a description for the aggregate data.
    - **Covering Device**: Select the mode for device coverage.
        - Aggregate All Devices: Data collected from all the devices covered by the monitoring item are aggregated.
        - Select Some Devices: Only the data collected from one or more specified devices covered by the monitoring item are aggregated.
    - **Aggregate Type**: Select one or more aggregate functions. Available options include sum, avg, max, and min.



Add Aggregate Data Configuration

* Name:

* Monitoring Item: Enter the name of the monitoring item.

* Data Item: Select an inspection template first.

* Description: Enter Description

* Covering Device: Aggregate All Devices | Select Some Devices

* Aggregate Type: Select Aggregate Type

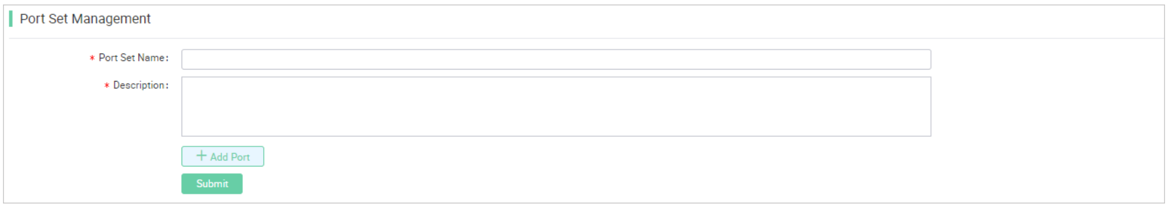
5. Click **OK**.

8.2.4.2.5. Add a port set

This topic describes how to add a port set to collect statistics on inbound and outbound traffic on specified device ports.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Network Monitor > Configuration > Port Set**.
3. On the **Port Set Management** tab, click **Add Port Set**.
4. On the **Port Set Management** page, configure the port set.The following configuration parameters are included:
    - **Port Set Name**: Enter a name for the port set. The name must be globally unique.
    - **Description**: Enter a comprehensive description of the feature of the port set. A detailed description helps increase maintenance efficiency.
    - **Add Port**: Select one or more devices and add ports used by the corresponding devices.



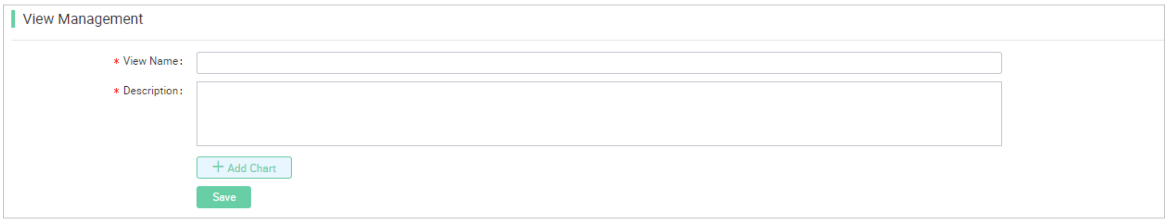
5. Click **Submit**.

8.2.4.2.6. Add a data view

This topic describes how to add and configure a data view as a monitoring dashboard to display aggregated data or port set statistics.

Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Network Monitor > Configuration > Data View**.
3. On the **Aggregate Data View** tab, click **Add View**.
4. On the **View Management** page, configure the data view.The following configuration parameters are included:
    - **View Name**: Enter a name for the data view. The name must be globally unique.
    - **Description**: Enter a comprehensive description of the feature of the data view. A detailed description helps increase maintenance efficiency.
    - **Add Chart**: Add one or more charts to the data view.
        - **Data Sources**: Select the source of data to be visualized for a chart. Available options include Aggregate Data and Port Set Traffic.
        - **Select Aggregate Data**: Select the aggregate data for the chart to display.
        - **Chart Type**: Choose a chart type for data visualization. Available options include Broken Line Chart and Area Chart.
        - **Chart Width**: Select a ratio from the drop-down list to determine how much width to be taken up by the chart on the web page.
        - **Sort Number**: Specify an order number for the chart. Charts are displayed in the ascending order in the dashboard.



5. Click **Save**.

8.2.5. Security Reinforcement

8.2.5.1. Log on to the srs-master.Server container

Security Reinforce Service (SRS) uses independent services to provide micro-segmentation for cloud services that are deployed in classic networks of Apsara Stack. SRS provides high availability, high throughput, and horizontal scaling.

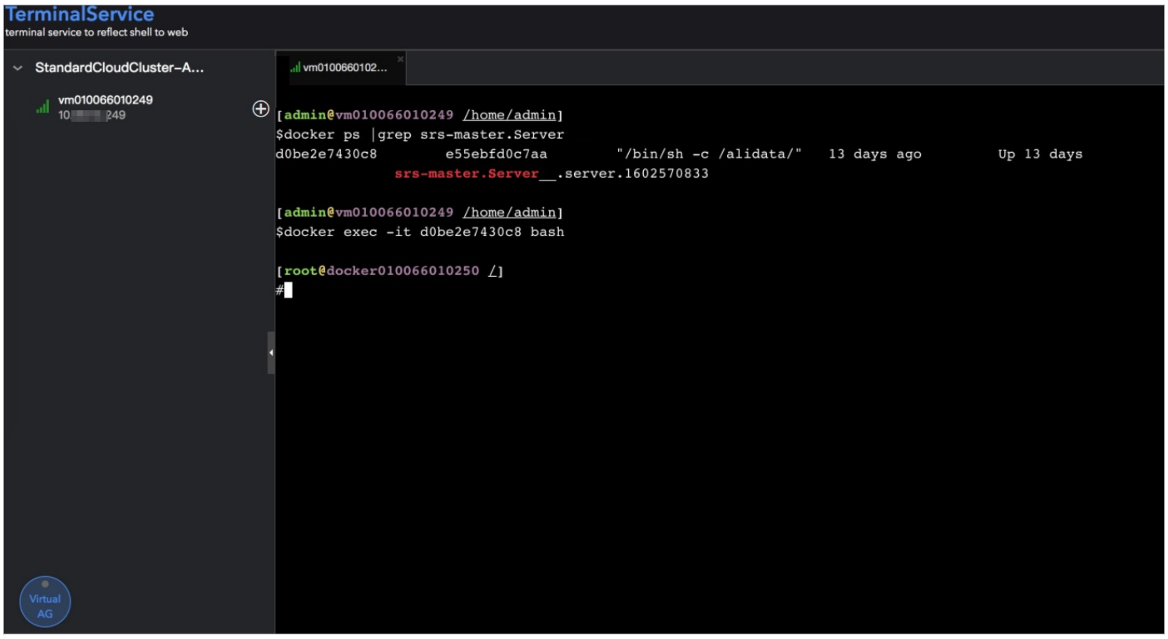
Procedure

1. Log on to the NET console.
2. In the left-side navigation pane, choose **Product Management** > **Products**.
3. On the **Products** page, click **Tianji** to log on to the Apsara Infrastructure Management Framework console.
4. In the left-side navigation pane, choose **Operations** > **Service Operations**.
5. On the **Services** page, click **srs-master** in the service list.
6. On the **Service srs-master** page, click the **Clusters** tab, find the cluster that you want to manage, and then click **Operations** in the Actions column.
7. On the **Cluster Details** page, click **Terminal** in the Actions column.
8. On the **TerminalService** page, click the ⊕ icon and enter the following commands into the command-line interface (CLI):

```
docker ps |grep srs-master.Server
docker exec -it d0be2e7430c8 bath
```

`docker ps` lists all running containers and `|grep srs-master.Server` locates the srs-master.Server container.

The result is shown in the following figure.



```
[admin@vm010066010249 /home/admin]
$docker ps |grep srs-master.Server
d0be2e7430c8        e55ebfd0c7aa        "/bin/sh -c /alidata/"   13 days ago         Up 13 days
              srs-master.Server__.server.1602570833

[admin@vm010066010249 /home/admin]
$docker exec -it d0be2e7430c8 bash

[root@docker010066010250 /]
#
```

8.2.5.2. Enable SRS

This topic describes how to enable Security Reinforce Service (SRS) in the Apsara Infrastructure Management Framework console.

Procedure

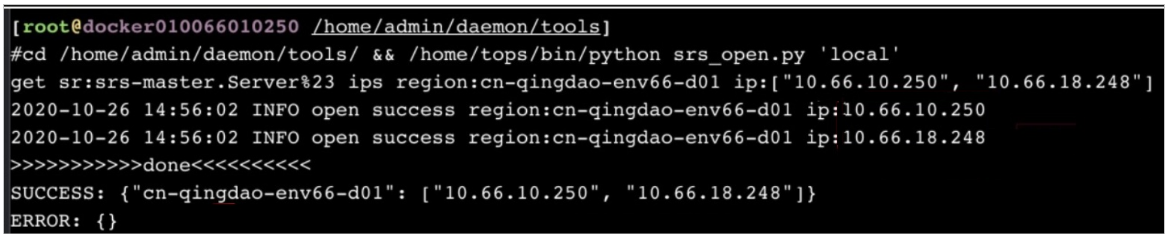
1. Log on to the srs-master.Server container.
2. Enter the following command into the command-line interface (CLI):

```
cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_open.py 'local'
```

Parameter descriptions:

- local: enables security isolation in the current region.
- all: enables security isolation in all regions.

The result is shown in the following figure.



```
[root@docker010066010250 /home/admin/daemon/tools]
#cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_open.py 'local'
get sr:srs-master.Server%23 ips region:cn-qingdao-env66-d01 ip:["10.66.10.250", "10.66.18.248"]
2020-10-26 14:56:02 INFO open success region:cn-qingdao-env66-d01 ip:10.66.10.250
2020-10-26 14:56:02 INFO open success region:cn-qingdao-env66-d01 ip:10.66.18.248
>>>>>>>>>>>done<<<<<<<<<<
SUCCESS: {"cn-qingdao-env66-d01": ["10.66.10.250", "10.66.18.248"]}
ERROR: {}
```

8.2.5.3. Disable SRS

This topic describes how to disable Security Reinforce Service (SRS) in the Apsara Infrastructure Management Framework console.

Procedure

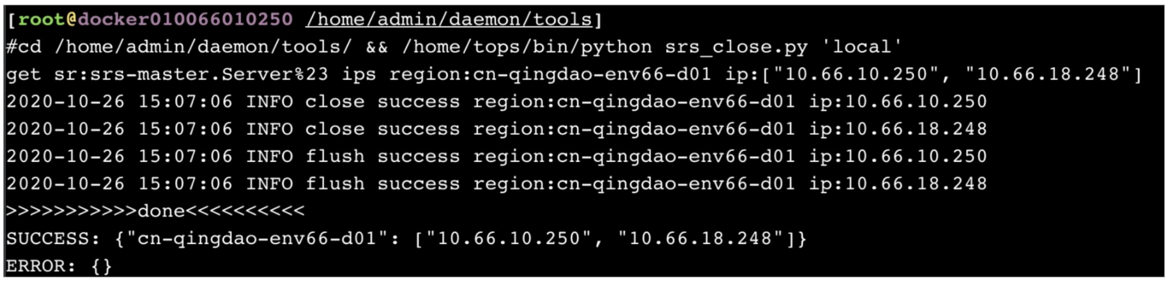
1. Log on to the srs-master.Server container.
2. Enter the following command into the command-line interface (CLI):

   ```
   cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_close.py 'local'
   ```

   Parameter descriptions:

   - local: disables security isolation in the current region.
   - all: disables security isolation in all regions.

   The result is shown in the following figure.

   ```
   [root@docker010066010250 /home/admin/daemon/tools]
   #cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_close.py 'local'
   get sr:srs-master.Server%23 ips region:cn-qingdao-env66-d01 ip:["10.66.10.250", "10.66.18.248"]
   2020-10-26 15:07:06 INFO close success region:cn-qingdao-env66-d01 ip:10.66.10.250
   2020-10-26 15:07:06 INFO close success region:cn-qingdao-env66-d01 ip:10.66.18.248
   2020-10-26 15:07:06 INFO flush success region:cn-qingdao-env66-d01 ip:10.66.10.250
   2020-10-26 15:07:06 INFO flush success region:cn-qingdao-env66-d01 ip:10.66.18.248
   >>>>>>>>>>>done<<<<<<<<<<
   SUCCESS: {"cn-qingdao-env66-d01": ["10.66.10.250", "10.66.18.248"]}
   ERROR: {}
   ```

8.2.5.4. Manage IP address whitelists

This topic describes how to manage IP address whitelists in the Apsara Infrastructure Management Framework console. This extends services for security isolation.

View IP address whitelists

To view IP address whitelists in the current region or in all regions, perform the following steps:

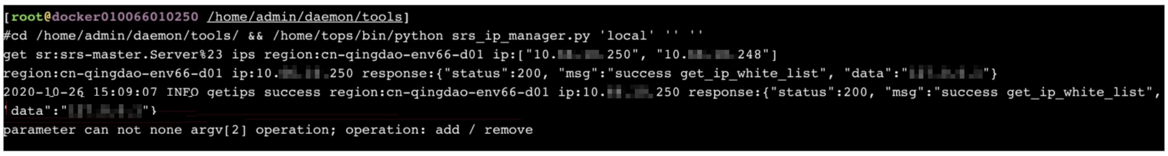
1. Log on to the srs-master.Server container.
2. Enter the following command into the command-line interface (CLI):

   ```
   cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_ip_manager.py 'local' '' ''
   ```

   Parameter descriptions:

   - local: views IP address whitelists in the current region.
   - all: views IP address whitelists in all regions.

   The result is shown in the following figure.

   ```
   [root@docker010066010250 /home/admin/daemon/tools]
   #cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_ip_manager.py 'local' '' ''
   get sr:srs-master.Server%23 ips region:cn-qingdao-env66-d01 ip:["10.[redacted].250", "10.[redacted].248"]
   region:cn-qingdao-env66-d01 ip:10.[redacted].250 response:{"status":200, "msg":"success get_ip_white_list", "data":"[redacted]"}
   2020-10-26 15:09:07 INFO getips success region:cn-qingdao-env66-d01 ip:10.[redacted].250 response:{"status":200, "msg":"success get_ip_white_list",
   'data":"[redacted]"}
   parameter can not none argv[2] operation; operation: add / remove
   ```

Add IP addresses to IP address whitelists

To add IP addresses to IP address whitelists in the current region or in all regions, perform the following steps:

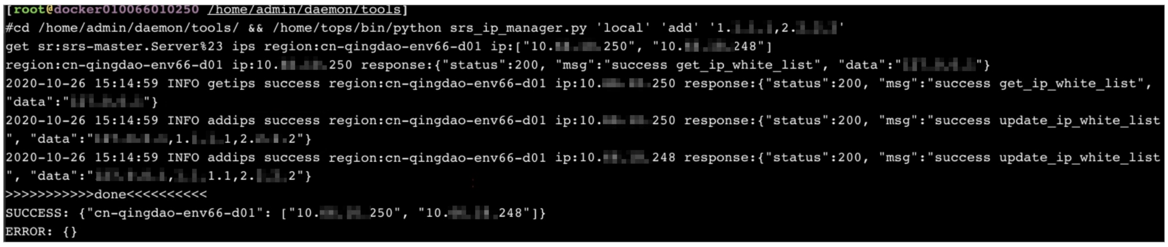
1. Enter the following command into the CLI:

   ```
   cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_ip_manager.py 'local' 'add' '1.x.x.1,2.x.x
   .2'
   ```

Parameter descriptions:

- local: adds IP addresses to IP address whitelists in the current region.
- all: adds IP addresses to IP address whitelists in all regions.
- add: adds IP addresses to IP address whitelists. This is a fixed parameter.
- x.x.x.x: the IP addresses that you want to add. Separate multiple IP addresses with commas (,).

The result is shown in the following figure.



```
[root@docker010066010250 /home/admin/daemon/tools]
#cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_ip_manager.py 'local' 'add' '1.[redacted],2.[redacted]'
get sr:srs-master.Server%23 ips region:cn-qingdao-env66-d01 ip:["10.[redacted]250", "10.[redacted]248"]
region:cn-qingdao-env66-d01 ip:10.[redacted]250 response:{"status":200, "msg":"success get_ip_white_list", "data":"[redacted]"}
2020-10-26 15:14:59 INFO getips success region:cn-qingdao-env66-d01 ip:10.[redacted]250 response:{"status":200, "msg":"success get_ip_white_list",
"data":"[redacted]"}
2020-10-26 15:14:59 INFO addips success region:cn-qingdao-env66-d01 ip:10.[redacted]250 response:{"status":200, "msg":"success update_ip_white_list
", "data":"[redacted],1.[redacted]1,2.[redacted]2"}
2020-10-26 15:14:59 INFO addips success region:cn-qingdao-env66-d01 ip:10.[redacted]248 response:{"status":200, "msg":"success update_ip_white_list
", "data":"[redacted],[redacted]1.1,2.[redacted]2"}
>>>>>>>>>>>done<<<<<<<<<<
SUCCESS: {"cn-qingdao-env66-d01": ["10.[redacted]250", "10.[redacted].248"]}
ERROR: {}
```

Remove IP addresses from IP address whitelists

To remove IP addresses from IP address whitelists in the current region or in all regions, perform the following steps:

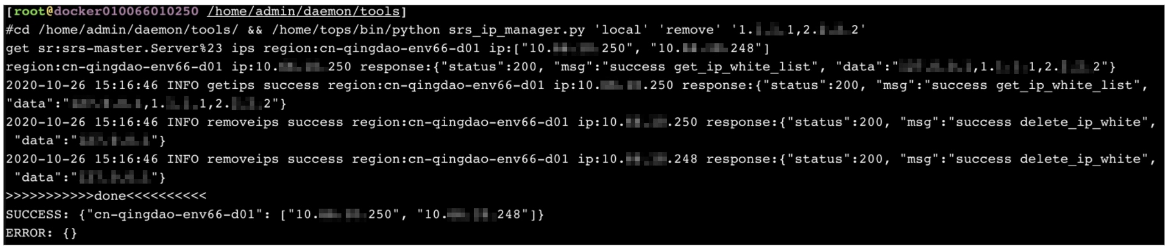
1. Enter the following command into the CLI:

```
cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_ip_manager.py 'local' 'remove' '1.x.x.1,
2.x.x.2'
```

Parameter descriptions:

- local: removes IP addresses from IP address whitelists in the current region.
- all: removes IP addresses from IP address whitelists in all regions.
- remove: removes IP addresses from IP address whitelists. This is a fixed parameter.
- x.x.x.x: the IP addresses that you want to remove. Separate multiple IP addresses with commas (,).

The result is shown in the following figure.



```
[root@docker010066010250 /home/admin/daemon/tools]
#cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_ip_manager.py 'local' 'remove' '1.[redacted]1,2.[redacted]2'
get sr:srs-master.Server%23 ips region:cn-qingdao-env66-d01 ip:["10.[redacted]250", "10.[redacted]248"]
region:cn-qingdao-env66-d01 ip:10.[redacted]250 response:{"status":200, "msg":"success get_ip_white_list", "data":"[redacted],1.[redacted]1,2.[redacted]2"}
2020-10-26 15:16:46 INFO getips success region:cn-qingdao-env66-d01 ip:10.[redacted].250 response:{"status":200, "msg":"success get_ip_white_list",
"data":"[redacted],1.[redacted]1,2.[redacted]2"}
2020-10-26 15:16:46 INFO removeips success region:cn-qingdao-env66-d01 ip:10.[redacted].250 response:{"status":200, "msg":"success delete_ip_white",
 "data":"[redacted]"}
2020-10-26 15:16:46 INFO removeips success region:cn-qingdao-env66-d01 ip:10.[redacted].248 response:{"status":200, "msg":"success delete_ip_white",
 "data":"[redacted]"}
>>>>>>>>>>>done<<<<<<<<<<
SUCCESS: {"cn-qingdao-env66-d01": ["10.[redacted]250", "10.[redacted]248"]}
ERROR: {}
```

8.2.5.5. Manage SRS disabled services

This topic describes how to manage Security Reinforce Service (SRS) disabled services in the Apsara Infrastructure Management Framework console.

View SRS disabled services

To view SRS disabled services in the current region or in all regions, perform the following operations:

1. Log on to the srs-master.Server container.

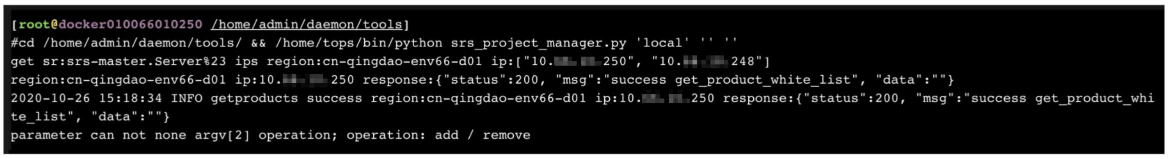
2. Enter the following command into the command-line interface (CLI):

```
cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_project_manager.py 'local' '' ''
```

Parameter descriptions:

- local: lists SRS disabled services in the current region.
- all: lists SRS disabled services in all regions.

The result is shown in the following figure.



```
[root@docker010066010250 /home/admin/daemon/tools]
#cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_project_manager.py 'local' '' ''
get sr:srs-master.Server%23 ips region:cn-qingdao-env66-d01 ip:["10.[redacted].250", "10.[redacted].248"]
region:cn-qingdao-env66-d01 ip:10.[redacted].250 response:{"status":200, "msg":"success get_product_white_list", "data":""}
2020-10-26 15:18:34 INFO getproducts success region:cn-qingdao-env66-d01 ip:10.[redacted].250 response:{"status":200, "msg":"success get_product_whi
te_list", "data":""}
parameter can not none argv[2] operation; operation: add / remove
```

> ? **Note** In the result shown in the preceding figure, the data parameter indicates SRS disabled services. If the value of the data parameter is empty, it means that all services in the specified region are isolated for security.

Add SRS disabled services

To add SRS disabled services to the current region or to all regions, perform the following operations:

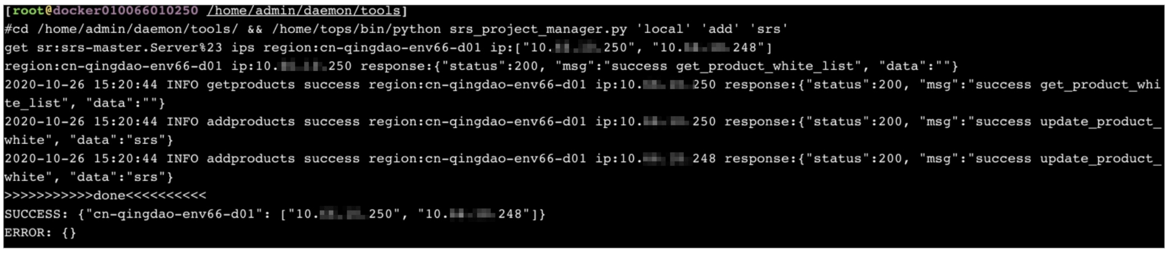
1. Enter the following command into the CLI:

```
cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_project_manager.py 'local' 'add' 'srs'
```

Parameter descriptions:

- local: adds SRS disabled services to the current region.
- all: adds SRS disabled services to all regions.
- add: adds SRS disabled services. This is a fixed parameter.
- srs: the SRS disabled services that you want to add. Separate multiple services with commas (,).

The result is shown in the following figure.



```
[root@docker010066010250 /home/admin/daemon/tools]
#cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_project_manager.py 'local' 'add' 'srs'
get sr:srs-master.Server%23 ips region:cn-qingdao-env66-d01 ip:["10.[redacted].250", "10.[redacted].248"]
region:cn-qingdao-env66-d01 ip:10.[redacted].250 response:{"status":200, "msg":"success get_product_white_list", "data":""}
2020-10-26 15:20:44 INFO getproducts success region:cn-qingdao-env66-d01 ip:10.[redacted].250 response:{"status":200, "msg":"success get_product_whi
te_list", "data":""}
2020-10-26 15:20:44 INFO addproducts success region:cn-qingdao-env66-d01 ip:10.[redacted].250 response:{"status":200, "msg":"success update_product_
white", "data":"srs"}
2020-10-26 15:20:44 INFO addproducts success region:cn-qingdao-env66-d01 ip:10.[redacted].248 response:{"status":200, "msg":"success update_product_
white", "data":"srs"}
>>>>>>>>>>>done<<<<<<<<<<
SUCCESS: {"cn-qingdao-env66-d01": ["10.[redacted].250", "10.[redacted].248"]}
ERROR: {}
```

Remove SRS disabled services

To remove SRS disabled services from the current region or from all regions, perform the following operations:

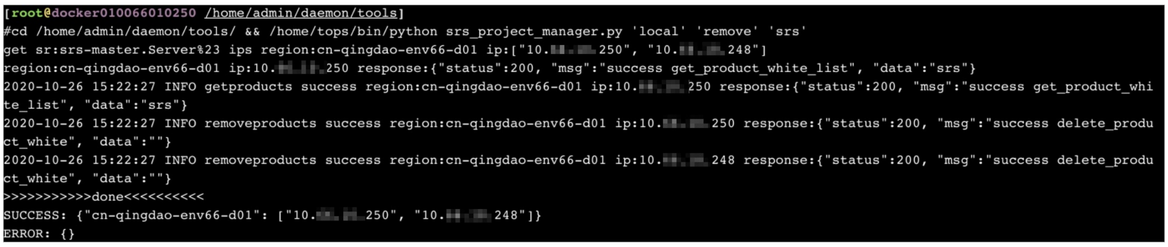
1. Enter the following command into the CLI:

```
cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_project_manager.py 'local' 'remove' 'sr
s'
```

Parameter descriptions:

- local: removes SRS disabled services from the current region.
- all: removes SRS disabled services from all regions.
- remove: removes SRS disabled services. This is a fixed parameter.
- srs: the SRS disabled services that you want to remove. Separate multiple services with commas (,).

The result is shown in the following figure.



```
[root@docker010066010250 /home/admin/daemon/tools]
#cd /home/admin/daemon/tools/ && /home/tops/bin/python srs_project_manager.py 'local' 'remove' 'srs'
get sr:srs-master.Server%23 ips region:cn-qingdao-env66-d01 ip:["10.[redacted]250", "10.[redacted]248"]
region:cn-qingdao-env66-d01 ip:10.[redacted]250 response:{"status":200, "msg":"success get_product_white_list", "data":"srs"}
2020-10-26 15:22:27 INFO getproducts success region:cn-qingdao-env66-d01 ip:10.[redacted]250 response:{"status":200, "msg":"success get_product_whi
te_list", "data":"srs"}
2020-10-26 15:22:27 INFO removeproducts success region:cn-qingdao-env66-d01 ip:10.[redacted]250 response:{"status":200, "msg":"success delete_produ
ct_white", "data":""}
2020-10-26 15:22:27 INFO removeproducts success region:cn-qingdao-env66-d01 ip:10.[redacted]248 response:{"status":200, "msg":"success delete_produ
ct_white", "data":""}
>>>>>>>>>>>done<<<<<<<<<<<
SUCCESS: {"cn-qingdao-env66-d01": ["10.[redacted]250", "10.[redacted]248"]}
ERROR: {}
```

8.2.6. Sample templates

This topic provides sample templates that are provisioned in production environments. Templates help you automate the implementation of network changes and configuration management with script logic and agile orchestration.

Sample templates

```
import datetime
import requests
import json
import time
import re
@login_device()
def atom_flow_isolate(restriction):
    """
    Isolate traffic before device OS upgrade
    Return: execution result and default routing peer
    """
    # Exit configuration mode and disable logging.
    exec_cli("return", strict=False)
    exec_cli("undo terminal monitor", strict=False)
    exec_cli("screen-length 0 temporary", strict=False)
    stack_check= exec_cli("display stack", strict=False)
    dis_version=exec_cli("display version", strict=False)
    check_isolate = exec_cli('display curr config bgp | in 2100', strict=False)
    if re.search('filter-policy 2100 export',check_isolate):
        logger.info("The filter-policy 2100 is existed in bgp config,Please check!")
        isolate_res.append([hostname+'(fail)',' filter-policy 2100 exists in BGP configuration.'])
        return default_peers, backup_ospf_stub,interfaces,isolate_res
    # Obtain the Border Gateway Protocol (BGP) number of the device.
    output = exec_cli("display cu configuration bgp | include bgp", strict=False)
    bgp_no = re.search(r"bgp (\d+)", output)
    if bgp_no:
        bgp_no = bgp_no.group(1)
        restriction['rollback_bgp_no']=bgp_no
    exec_cli("sys", strict=False)
    # Obtain the timestamp before isolation.
    time1=time.time()
    get_time()
    logger.info('begin time:%s'%time1)
    #1 Open Shortest Path First (OSPF) traffic isolation (LoadBalance Switch (LSW)).
    if cu_rol == 'LSW':
        output = exec_cli("display cu configuration ospf | include ospf", strict=False)
        ospf_no = re.search(r"ospf (\d+)", output)
        if ospf_no:
            ospf_no = ospf_no.group(1)
            backup_ospf_stub = exec_cli("disp cu conf ospf | in stub", strict=False)
            exec_cli("ospf %s" % ospf_no, strict=False)
            exec_cli("undo stub-router", strict=False)
            exec_cli("stub-router include-stub summary-lsa external-lsa", strict=False)
            exec_cli("commit", strict=False)
            logger.info('ospf_isolate')
            radar_chek=radar_result(15)
            if radar_chek:
                logger.info('%s ospf isolate successfull'%hostname)
            else:
                return default_peers, backup_ospf_stub,interfaces,isolate_res
    # Destack Access Switch (ASW) and Link Layer Discovery Protocol (LLDP) isolation.
    out1 = exec_cli("display stack", strict=False)
    if cu_rol == 'ASW' and (cu_arc == '5.0L' or '4.2' in cu_arc):
        # if 'ASW' in hostname:
        out2 = exec_cli('display lldp nei brief | ex "DSW|PSW|M"', strict=False)
        out3 = exec_cli('display interface brief | in up', strict=False,timeout = 120)
        int_down = []
        tmp_down = get_info(out2,0,2,3)
        for i in tmp_down:
            int_down.append(i[0])
        if 'Standby' in out1:
            isolate_res.append([hostname+'(fail)',' stack configuration exists for the ASW to be destacked, please c
heck'])
            return default_peers, backup_ospf_stub,interfaces,isolate_res
        else:
            exec_cli('sys', strict=False)
            exec_cli('undo lldp enable', strict=False)
            exec_cli('commit', strict=False)
            radar_chek_lldp=radar_result(30)
            if radar_chek_lldp:
                logger.info('%s lldp isolate successfull'%hostname)
            else:
                return default_peers, backup_ospf_stub,interfaces,isolate_res
            exec_cli('return', strict=False)
            exec_cli("reset interface counters", strict=False)
            exec_cli('sys', strict=False)
            radar_chek_lldp=radar_result(30)
            if radar_chek_lldp:
                logger.info('lldp isolate successfull')
            else:
                return default_peers, backup_ospf_stub,interfaces,isolate_res
    if ('4.1' in cu_arc or '3.' in cu_arc) and cu_rol == 'ASW':
        logger.info('stack device')
    else:
```

```
  else:
    #2 BGP traffic isolation (all).
    output = exec_cli("display ip interface brief | include Loop", strict=False)
    loop1 = re.search(r"LoopBack1\s+(\d+\.\d+\.\d+\.\d+)/\d+", output)
    loop1 = loop1.group(1)
    loop2 = re.search(r"LoopBack101\s+(\d+\.\d+\.\d+\.\d+)/\d+", output)
    loop2 = loop2.group(1) if loop2 else ""
    #2.1 Configure the access control list (ACL)
    exec_cli("acl number 2100", strict=False)
    exec_cli("rule permit source %s 0.0.0.0" % loop1, strict=False)
    if loop2:
      exec_cli("rule permit source %s 0.0.0.0" % loop2, strict=False)
    exec_cli("commit", strict=False)
    #2.2 Check the ACL
    output = exec_cli('dis acl 2100 | in " %s%s"' % (loop1, ('| '+loop2) if loop2 else ''), strict=False)
    if not output:
        isolate_res.append([hostname + '(fail)',' ACL 2100 configuration failed, please check'])
        return default_peers, backup_ospf_stub,interfaces,isolate_res
  #2.2 BGP configuration (PoD Switch (PSW), Distribution Switch (DSW), and LSW).
  if cu_rol in ['DSW','PSW','LSW','CSW']:
    exec_cli("bgp %s" % bgp_no, strict=False)
    exec_cli("ipv4-family unicast", strict=False)
    exec_cli("filter-policy 2100 export", strict=False)
    exec_cli("commit", strict=False)
    if cu_rol == 'DSW' and cu_arc ! = '4.0V' and cu_arc ! = '4.1Lv':
      sdn_check = exec_cli('display sdn openflow session', strict=False)
      adv_check = exec_cli('dis cu conf bgp | in advertise lowest-priority ', strict=False)
      restriction['rollback_sdn_check']=sdn_check
      restriction['rollback_adv_check']=adv_check
      if 'REGISTERED' not in sdn_check and 'advertise lowest-priority on-startup' in adv_check:
        exec_cli('undo advertise lowest-priority on-startup ', strict=False)
        exec_cli("commit", strict=False)
      logger.info('bgp_isolate')
  #2.3 ASW destacking and BGP isolation configuration.
  if cu_rol == 'ASW' and rate_check == True and 'Standby' not in out1 and not slot and (cu_arc == '5.0L' or '4.
2' in cu_arc or '5.1' in cu_arc):
    exec_cli("bgp %s" % bgp_no, strict=False)
    exec_cli("ipv4-family unicast", strict=False)
    exec_cli("filter-policy 2100 export", strict=False)
    exec_cli("commit", strict=False)
    logger.info('bgp_isolate')
 #2.3 MC BGP isolation.
  if cu_rol == 'MC':
    exec_cli("bgp %s" % bgp_no, strict=False)
    exec_cli("ipv4-family vpn-instance Alimaster", strict=False)
    exec_cli("filter-policy 2100 export", strict=False)
    exec_cli("ipv4-family vpn-instance Alimaster-public", strict=False)
    exec_cli("filter-policy 2100 export", strict=False)
    exec_cli("ipv4-family vpn-instance Alipay", strict=False)
    exec_cli("filter-policy 2100 export", strict=False)
    exec_cli("ipv4-family vpn-instance Alipay-public", strict=False)
    exec_cli("filter-policy 2100 export", strict=False)
    exec_cli("ipv4-family vpn-instance Aliyun", strict=False)
    exec_cli("filter-policy 2100 export", strict=False)
    exec_cli("ipv4-family vpn-instance Aliyun-public", strict=False)
    exec_cli("ipv4-family vpn-instance Aliyun-public", strict=False)
    exec_cli("filter-policy 2100 export", strict=False)
    exec_cli("commit", strict=False)
    logger.info('bgp_isolate')
  #3 Delete default route advertisements and close open ports.
  if cu_rol == 'LSW':
    output = exec_cli("disp cu conf bgp | in default-route-advertise", style='verbose', strict=False)
    logger.debug("default route: %s", output)
    default_peers = re.findall(r"peer (. *?) default-route-advertise", output)
    if default_peers:
      exec_cli("bgp %s" % bgp_no, strict=False)
      exec_cli("ipv4-family unicast", strict=False)
      for peer in default_peers:
        exec_cli("undo peer %s default-route-advertise" % peer)
      exec_cli("commit", strict=False)
    # Obtain the port list.
    output2 = exec_cli("display interface brief | include up | exclude NULL | exclude Loop | exclude M-G | exclu
de MEth", strict=False)
    rvs = re.findall(r"(. *?) \s+up\s+", output2)
    for rv in rvs:
      if '.' in rv:
        continue
      interfaces.append(rv.replace("(10GE)",""))
    # Shut down ports in batches.
    exec_cli("sys", strict=False)
    for interface in interfaces:
      exec_cli("interface %s" % interface)
      exec_cli("shutdown")
    exec_cli("commit", strict=False)
    radar_chek_lsw=radar_result(30)
    if radar_chek_lsw:
      logger.info('%s lsw isolate successfull'%hostname)
    else:
      return default_peers, backup_ospf_stub,interfaces,isolate_res
    # Check the isolation result.
    output3 = exec_cli("display interface brief | include up | exclude NULL0 | exclude Loop | exclude M-G | excl
ude MEth", strict=False)
    rvs = re.findall(r"(. *?) \s+up\s+", output3)
    for rv in rvs:
      if '.' in rv:
        continue
      isolate_res.append([hostname+'(fail)','Physical ports remain open after LSW port isolation, please che
ck')
      return default_peers, backup_ospf_stub,interfaces,isolate_res
# Stack ASW isolation.
  if cu_rol == 'ASW' and 'Standby' in stack_check and slot and action:
    slot1_check=True
    slot2_check=True
    slot1_int=exec_cli("display interface brief | in 1/0", strict=False,timeout=300)
    slot2_int=exec_cli("display interface brief | in 2/0", strict=False,timeout=300)
    if '*down ' in slot1_int and slot == '2' and not ingore_ADM:
      slot1_check=False
      isolate_res.append([hostname+'(fail)',unicode('Add/Drop Multiplexer (ADM) port is detected in slot 1 b
efore slot 2 isolation. Slot 2 is not isolated. Please check:\n%s','utf-8')%slot1_int])
      return default_peers, backup_ospf_stub,interfaces,isolate_res
```

```
        if '*down ' in slot2_int and slot == '1' and not ingore_ADM:
            slot2_check=False
            isolate_res.append([hostname+'(fail)',unicode('ADM port is detected in slot 2 before slot 1 isolation. Sl
ot 1 is not isolated. Please check:\n%s','utf-8')%slot2_int])
            return default_peers, backup_ospf_stub,interfaces,isolate_res
        if 'CE6851' in dis_version and slot == '1':
            exec_cli("sys", strict=False)
            exec_cli("interface M 0/0/0", strict=False)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
            exec_cli("interface range 40GE1/0/3 to 40GE1/0/6", strict=False,timeout=300)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
            exec_cli("interface range 10GE1/0/1 to 10GE1/0/48", strict=False,timeout=300)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
        elif 'CE6851' in dis_version and slot == '2':
            exec_cli("sys", strict=False)
            exec_cli("interface M 0/0/0", strict=False)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
            exec_cli("interface range 40GE2/0/3 to 40GE2/0/6", strict=False,timeout=300)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
            exec_cli("interface range 10GE2/0/1 to 10GE2/0/48", strict=False,timeout=300)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
        elif 'CE5850' in dis_version and slot == '1':
            exec_cli("sys", strict=False)
            exec_cli("interface  range 10GE 1/0/1 to 10GE 1/0/4", strict=False,timeout=300)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
            exec_cli("interface range GE 1/0/1 to GE 1/0/48", strict=False,timeout=300)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
        elif 'CE5850' in dis_version and slot == '2':
            exec_cli("sys", strict=False)
            exec_cli("interface  range 10GE 2/0/1 to 10GE 2/0/4", strict=False,timeout=300)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
            exec_cli("interface range GE 2/0/1 to GE 2/0/48", strict=False,timeout=300)
            exec_cli("shutdown", strict=False,timeout=300)
            exec_cli("commit", strict=False,timeout=300)
    # Destack ASW and shut down uplink and downlink ports.
    if cu_rol == 'ASW' and '5.1' in cu_arc and 'CE6865' in dis_version:
        exec_cli("interface range 25GE 1/0/1 to 25GE 1/0/48", strict=False,timeout=300)
        exec_cli("shutdown", strict=False,timeout=300)
        exec_cli("commit", strict=False,timeout=300)
        # exec_cli("interface range 100 1/0/1 to 100 1/0/8", strict=False,timeout=300)
        # exec_cli("shutdown", strict=False,timeout=300)
        exec_cli("commit", strict=False,timeout=300)
    check_2100 = exec_cli('display curr config bgp | in 2100', strict=False)
    if cu_rol == 'ASW' and '5.0L' in cu_arc and 'CE6860' in dis_version and '2100' in check_2100:
        exec_cli("interface range 25GE 1/0/1 to 25GE 1/0/48", strict=False,timeout=300)
        exec_cli("shutdown", strict=False,timeout=300)
        exec_cli("commit", strict=False)
        exec_cli("interface range 100 1/0/1 to 100 1/0/12", strict=False,timeout=300)
        exec_cli("shutdown", strict=False,timeout=300)
        exec_cli("commit", strict=False)
    if cu_rol == 'ASW' and '4.2L' in cu_arc and 'CE6851' in dis_version and '2100' in check_2100:
        exec_cli("interface range 10GE1/0/1 to 10GE1/0/48", strict=False,timeout=300)
        exec_cli("shutdown", strict=False,timeout=300)
        exec_cli("commit", strict=False)
        exec_cli("interface range 40GE1/0/1 to 40GE1/0/4", strict=False,timeout=300)
        exec_cli("shutdown", strict=False,timeout=300)
        exec_cli("commit", strict=False)
    if cu_rol == 'ASW' and '4.2M' in cu_arc and 'CE6851' in dis_version and '2100' in check_2100:
        exec_cli("interface range 10GE1/0/1 to 10GE1/0/48", strict=False,timeout=300)
        exec_cli("shutdown", strict=False,timeout=300)
        exec_cli("commit", strict=False)
        exec_cli("interface range 40GE1/0/3 to 40GE1/0/6", strict=False,timeout=300)
        exec_cli("shutdown", strict=False,timeout=300)
        exec_cli("commit", strict=False)
    exec_cli("commit", strict=False)
    return default_peers,backup_ospf_stub,interfaces,isolate_res
```

9.Operations of basic cloud products

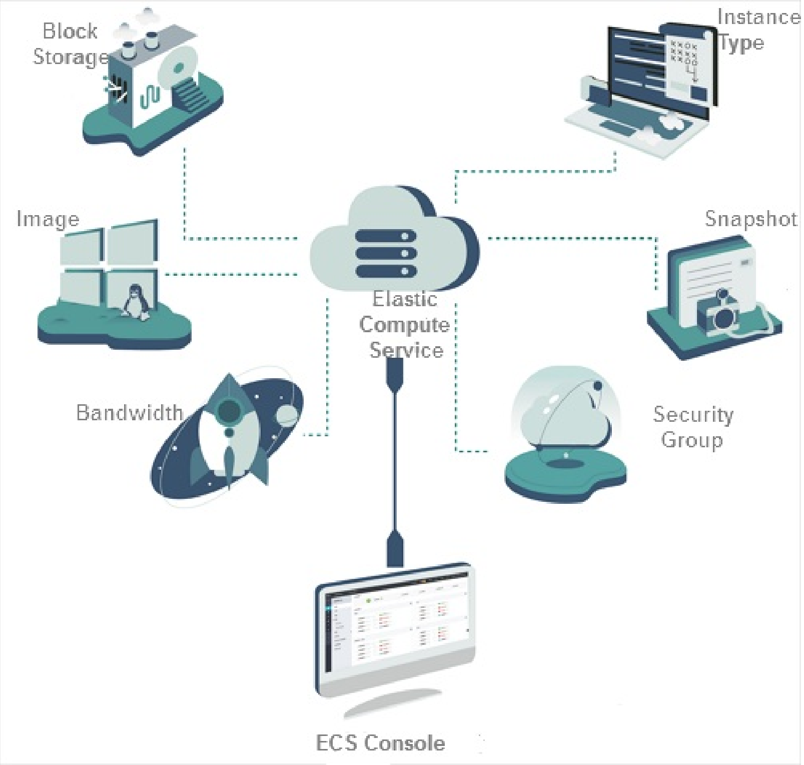
9.1. Elastic Compute Service (ECS)

9.1.1. ECS overview

Elastic Compute Service (ECS) is a user-friendly computation service featuring elastic processing capabilities that can be managed more efficiently than physical servers. You can create instances, resize disks, and release any number of ECS instances at any time based on your business needs.

An ECS instance is a virtual computing environment that includes basic components such as the CPU, memory, and storage. Users perform operations on ECS instances. Instances are the core concept of ECS, and are operated from the ECS console. Other resources such as block storage, images, and snapshots can be used only after they are integrated with ECS instances. For more information, see ECS instance.

ECS instance



9.1.2. Log on to the Apsara Uni-manager Operations Console

This topic describes how to log on to the Apsara Uni-manager Operations Console.

Prerequisites

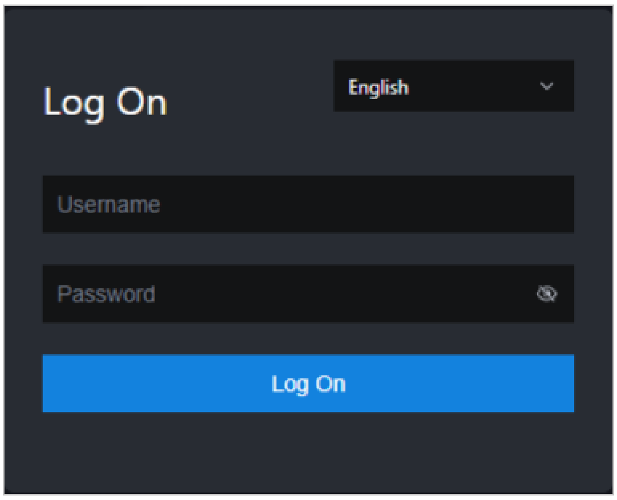
- The URL, username, and password that are required to log on to the Apsara Uni-manager Operations Console are obtained from the deployment personnel or administrators.

  The URL of the Apsara Uni-manager Operations Console is in the format of *region-id*.ops.console.*intranet-domain-id*.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL. Then, press the Enter key.

   > Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   > Note To obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console, contact the deployment personnel or administrators.

   If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username as prompted.

   To enhance security, make sure that the password meets the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password is 10 to 20 characters in length.

4. Click **Log On**.

9.1.3. ECS operations and maintenance

9.1.3.1. Overview

The ECS Operations and Maintenance Platform is a platform for support engineers to operate and monitor ECS instances, help users troubleshoot problems with ECS instances, and ensure that ECS instances are properly operated and utilized.

9.1.3.2. VM

9.1.3.2.1. Overview

On the ECS Operations and Maintenance Platform page, the existing ECS VM information and available O&M functions are displayed. You can search for, start, and migrate a VM as needed.

9.1.3.2.2. Query VMs

In the ECS Operations and Maintenance Platform, you can view the list of existing VMs and their information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **VMs** tab.
5. On the VMs tab, set the filter conditions and click **View**.
6. In the VM list, click a VM ID. You can view the information of the VM in the **VM Details** panel.

9.1.3.2.3. Start a VM

In the ECS Operations and Maintenance Platform, you can start a VM in the same manner as you start a real server.

Prerequisites

The VM to start is in the **Stopped** state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **VMs** tab.
5. On the VMs tab, set the filter conditions and click **View**.
6. In the VM list, select the VM to start. Click **Start** above the list.
7. In the Start VM dialog box, set Start.You can select **Normal** or **Repair**.

   > **Note** If you want to reset the network settings of the VM, set Start to **Repair**. Otherwise, set Start to **Normal**.

8. Set Operation Reason. Click **OK**.

9.1.3.2.4. Stop a VM

In the ECS Operations and Maintenance Platform, you can stop a VM in the same manner as you stop a real server.

Prerequisites

The VM to stop is in the **Running** state.

Context

This operation may interrupt the programs running on the VM. Perform this operation during off-peak hours to minimize the impact on services.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **VMs** tab.
5. On the VMs tab, set the filter conditions and click **View**.
6. In the VM list, select the VM to stop. Click **Stop** above the list.
7. In the Stop VM dialog box, set Shutdown Policy.You can select **Non-force Shutdown** or **Force Shutdown**.

   > **Note** When Force Shutdown is selected, the VM is stopped regardless of whether its processes have been stopped. We recommend that you do not select Force Shutdown unless Non-force Shutdown does not work.

8. Set Operation Reason. Click **OK**.

9.1.3.2.5. Restart a VM

In the ECS Operations and Maintenance Platform, you can restart a VM in the same manner as you restart a real server.

Prerequisites

The VM to restart is in the **Running** state.

Context

This operation may interrupt the programs running on the VM. Perform this operation during off-peak hours to minimize the impact on services.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.

2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **VMs** tab.
5. On the VMs tab, set the filter conditions and click **View**.
6. In the VM list, select the VM to restart. Click **Reboot** above the list.
7. In the Reboot VM dialog box, set Start and Shutdown Policy.
   - You can set Start to **Normal** or **Repair**.
   - You can set Shutdown Policy to **Non-force Shutdown** or **Force Shutdown**.
8. Set Operation Reason. Click **OK**.

9.1.3.2.6. Cold migration

In the ECS Operations and Maintenance Platform, you can perform cold migration on a VM to implement failover.

Prerequisites

Cold migration requires that the VM be taken offline. Make sure that the VM is in the **Stopped** state before you migrate it.

Context

If a VM or an NC fails, you must fail over the VM by stopping the VM and migrating it to a new NC. Failover can be performed only within the same zone. Cross-zone failover cannot be performed.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **VMs** tab.
5. On the VMs tab, set the filter conditions and click **View**.
6. In the VM list, select the VM to migrate. Click **Stop and Migrate** above the list.
7. In the Stop and Migrate VM dialog box, configure the parameters described in the following table.

Parameter	Description
Switchable NC	The destination NC to which to migrate the VM.
Switchover Policy	The switchover policy. Valid values: ○ **Force Migrate** ○ **Active Migrate**

Parameter	Description
Start	The startup mode. Valid values: ○ **Normal** ○ **Repair**
Recover	The recovery mode. Valid values: ○ **Start After Migration** ○ **Stop After Migration** ○ **Status Unchanged After Migration** **Status Unchanged After Migration** takes effect only on VMs that are in the Pending state.

8. Set Operation Reason. Click **OK**.

9.1.3.2.7. Hot migration

In the ECS Operations and Maintenance Platform, you can perform hot migration on VMs.

Context

- You can use hot migration to migrate a VM in the **Running** state from one NC to another without interrupting normal services. Hot migration can be used for load balancing or other purposes. If a failure occurs, hot migration cannot be performed and you must perform cold migration instead. For more information, see Cold migration.
- Security risks may arise if you perform hot migration. Exercise caution when you perform hot migration.
- Hot migration does not interrupt services running on the VM.
- Hot migration can be performed only within the same zone. Cross-zone hot migration cannot be performed.

Prerequisites

You can perform hot migration only on VMs in the **Running** state.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **VMs** tab.
5. On the VMs tab, set the filter conditions and click **View**.
6. In the VM list, select the VM to migrate. Choose **More > Online Migrate** above the list.
7. Set Throughput Limit.The value of Throughput Limit can range from 1 to 1000. Unit: MByte/s. Default value: 20.
8. Set Operation Reason. Click **Online Migrate**.The destination NC is automatically selected during

migration. You can view the ID of the destination NC in the migration result.

9.1.3.2.8. Reset a disk

In the ECS Operations and Maintenance Platform, you can reset disks to restore them to their initial status.

Prerequisites

- When you reset a disk, installed applications are cleared from the disk. Before you perform a reset operation, make sure that you have backed up your data.
- To reset a disk, make sure that the VM to which it is attached is in the **Stopped** state.

Context

After a disk is reset, it is restored to its initial status but is not reformatted. The image that is used to create the disk still exists after the disk is reset.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **VMs** tab.
5. On the VMs tab, set the filter conditions and click **View**.
6. In the VM list, select the VM to which the disk that you want to reset is attached. Choose **More > Reset Disk** above the list.
7. In the Reset Disk dialog box, select the disk that you want to reset and set Operation Reason. Click **OK**.

9.1.3.3. Disks

9.1.3.3.1. Overview

In an ECS instance, cloud disks can be considered as physical disks. You can mount, detach, and create snapshots for disks.

9.1.3.3.2. Query disks

In the ECS Operations and Maintenance Platform, you can view the list of existing disks and their information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.

4. Click the **Disks** tab.
5. On the Disks tab, set the filter conditions and click **View**.

9.1.3.3.3. View snapshots

In the ECS Operations and Maintenance Platform, you can view the list of snapshots created for a disk and their information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Disks** tab.
5. On the Disks tab, set the filter conditions and click **View**.
6. Find the disk whose snapshots you want to view and choose + **> View Snapshot**.

   The information of all snapshots on the disk is displayed.

9.1.3.3.4. Attach a disk

After a disk is created, you can attach the disk to a VM.

Context

Only disks in the **Available** state can be attached.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Disks** tab.
5. On the Disks tab, set the filter conditions and click **View**.
6. Find the disk to attach and choose + **> Mount**.
7. In the Mount Disk dialog box, set VM ID and Operation Reason. Click **OK**.

9.1.3.3.5. Detach a disk

In the ECS Operations and Maintenance Platform, only data disks can be detached. System disks and local disks cannot be detached.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.

3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Disks** tab.
5. On the Disks tab, set the filter conditions and click **View**.
6. Find the disk to detach and choose + > **Detach**.
7. In the Detach Disk dialog box, set Operation Reason. Click **OK**.

9.1.3.3.6. Create a snapshot

In the ECS Operations and Maintenance Platform, you can manually create snapshots for disks.

Context

Snapshots can be created only for system disks.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Disks** tab.
5. On the Disks tab, set the filter conditions and click **View**.
6. Find the disk for which you want to create a snapshot and choose + > **Take Snapshot**.
7. In the Disk Snapshot dialog box, set Snapshot Name, Snapshot Description, and Operation Reason. Click **OK**.

9.1.3.4. Snapshots

9.1.3.4.1. Overview

A snapshot stores the data stored on a disk for a certain point in time. Snapshots can be used to back up data or create a custom image.

When using disks, note the following points:

- When writing or saving data to a disk, we recommend that you use the data on one disk as the basic data for another disk.
- Although the disk provides secure data storage, you must still ensure that stored data is complete. However, data can be stored incorrectly due to an application error or malicious usage of vulnerabilities in the application. For these cases, a mechanism is required to ensure that data can be recovered to the desired state.

Alibaba Cloud allows you to create snapshots to retain copies of data on a disk for specific points in time.

9.1.3.4.2. Query snapshots

In the ECS Operations and Maintenance Platform, you can view the list of existing snapshots and their information.

Prerequisites

The AliUid of the disk for which the snapshot is taken is obtained. For more information, see Search for disks.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Snapshots** tab.
5. On the Snapshots tab, set the filter conditions and click **View**.AliUid is a required filter condition.

9.1.3.4.3. Delete a snapshot

In the ECS Operations and Maintenance Platform, you can delete snapshots that are no longer needed.

Prerequisites

The AliUid of the disk for which the snapshot is taken is obtained. For more information, see Search for disks.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Snapshots** tab.
5. On the Snapshots tab, set the filter conditions and click **View**.AliUid is a required filter condition.
6. Find the snapshot that you want to delete and choose + > **Delete**.
7. Set Operation Reason. Click **OK**.

9.1.3.4.4. Create an image

In the ECS Operations and Maintenance Platform, you can create a custom image from a snapshot. The image contains the operating system and environment variables of the snapshot.

Prerequisites

The AliUid of the disk for which the snapshot is taken is obtained. For more information, see Search for disks.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.

2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Snapshots** tab.
5. On the Snapshots tab, set the filter conditions and click **View**.AliUid is a required filter condition.
6. Find the snapshot from which you want to create an image and choose + > **Create Image**.
7. In the Create Image dialog box, set Image Name, Image Version, Image Description, and Operation Reason. Specify whether the system disk for which the snapshot was taken uses a public image or a custom image. Click **OK**.

9.1.3.5. Images

9.1.3.5.1. Overview

An ECS image is a template that contains software configurations such as the ECS instance operating system and the programs and servers for applications. You must specify an ECS image to create an instance. The operating system and software provided by the image will be installed on the instance that you create.

9.1.3.5.2. Query images

In the ECS Operations and Maintenance Platform, you can view the list of existing images and their information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Images** tab.
5. On the Images tab, set the filter conditions and click **View**.

> **Note** If you set Image Type to Custom Image, you must also set AliUid.

9.1.3.6. Security groups

9.1.3.6.1. Overview

A security group is a virtual firewall that provides Stateful Packet Inspection (SPI). Security groups provide virtual firewall-like functionality and are used for network access control for one or more ECS instances. They are important means of network security isolation and are used to divide security domains on the cloud.

Security group rules can permit the inbound and outbound traffic of the ECS instances associated with the security group. You can authorize or cancel security group rules at any time. Changes to security group rules are automatically applied to ECS instances that are members of the security group.

When you configure security group rules, ensure that the rules are concise and easy to manage. If you associate an instance with multiple security groups, hundreds of rules may apply to the instance, which may cause connection errors when you access the instance.

9.1.3.6.2. Query security groups

In the ECS Operations and Maintenance Platform, you can view the list of existing security groups and their information.

Context

After an ECS instance is added to a security group, you can add security group rules to allow or deny public or internal network traffic to and from the ECS instance. You can add or delete security group rules at any time. Changes to security group rules are automatically applied to ECS instances in the security group.

> Note
>
> - If two security group rules differ only in Authorization Policy, the deny rules takes precedence over allow rules.
> - No rule in a security group can allow outbound traffic from an instance while denying inbound traffic to the instance.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Security Groups** tab.
5. On the Security Groups tab, set the filter conditions and click **View**.

9.1.3.6.3. Add security group rules

You can add rules to security groups to control access to or from instances in the security groups.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Security Groups** tab.
5. On the Security Groups tab, set the filter conditions and click **View**.
6. Find the security group to which you want to add a security group rule and choose + > **Add Rule**.

7. In the Add Rule dialog box, configure parameters.The following table describes the parameters.

Parameter	Description
Protocol	○ TCP ○ UDP ○ ICMP ○ GRE ○ ALL: All protocols are supported.
Rule Priority (1-100)	A smaller value indicates a higher priority.
Network Type	○ Public: the Internet ○ Internal: the internal network
Authorization Policy	○ Accept: grants access. ○ Drop: discards the packet on access. ○ Reject: denies the packet on access.
Port Number Range	Valid values: 1 to 65535. Example: 1/200, 80/80, or -1/-1.
Access Direction	○ Ingress: allows inbound traffic. ○ Egress: allows outbound traffic.
IP Address Range	Enter an IP address or a CIDR block. Only IPv4 addresses are supported. Example: 10.0.0.0, 0.0.0.0/0, or 192.168.0.0/24.
Security Group ID	Enter the ID of the security group which you want to allow or deny access to the current security group.
Operation Reason	Optional. Enter a reason for the operation.

8. Click **OK**.

9.1.3.7. Custom instance types

9.1.3.7.1. Add custom instance types

When existing instance types cannot meet your business requirements, you can add custom instance types in the ECS Operations and Maintenance Platform and create instances of the custom instance types.

Context

Custom instance types are of the ecs.anyshare instance family. You can set the instance type name, number of vCPUs, and memory size. Parameters such as base bandwidth, network packet forwarding rate, and NIC queues are generated by the system. For more information, see Instance types in *ECS Product Introduction*.

> ⓘ **Note** All custom instance types are shared instance types.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Custom Instance Type** tab.
5. Click **Add**.
6. In the **Add Instance Type** panel, set the Instance Type, vCPUs, and Mem (GiB) parameters.
7. Click **OK**.

Result

The new custom instance type is displayed in the custom instance type list. After you add a custom instance type, you can create ECS instances of the instance type by selecting ecs.anyshare as the instance family. For more information, see Create an instance in *ECS User Guide*.

9.1.3.7.2. Query custom instance types

In the ECS Operations and Maintenance Platform, you can view the custom instance types that you have added and their information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Custom Instance Type** tab.
5. View the information about the custom instance types. If the custom instance type list does not automatically refresh, click **Search**.

9.1.3.7.3. Modify custom instance types

If you want to retain a custom instance type but the specifications of this instance type do not meet your requirements, you can modify the number of vCPUs and memory size of the instance type.

Prerequisites

A custom instance type is added.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Custom Instance Type** tab.
5. Find the custom instance type that you want to modify and click **Modify** in the **Actions** column.
6. In the **Modify Instance Type** panel, set the vCPUs and Mem (GiB) parameters.
7. Click **OK**.

9.1.3.7.4. Delete custom instance types

In the ECS Operations and Maintenance Platform, you can delete custom instance types that are no longer needed. After you delete a custom instance type, you cannot select it when you create a new instance. However, existing instances of this custom instance type can continue to be used.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, select an environment version and a region.
3. In the top navigation bar, click **O&M**. Then, the in the left-side navigation pane, choose **Product Management > ECS Operations and Maintenance Platform**.
4. Click the **Custom Instance Type** tab.
5. Find the custom instance type that you want to delete and click **Delete** in the **Actions** column.
6. In the **Deleted** message, click **OK**.

Result

The custom instance type is removed from the custom instance type list.

9.1.4. Apsara Distributed File System Management

9.1.4.1. View ECS disk size rankings

The ECS Disk Size Ranking module allows you to view the amount of space occupied by all disks within the elastic block storage attached to an ECS cluster in Apsara Distributed File System.

Context

When an ECS cluster occupies a large amount of space in Apsara Distributed File System, the on-site O&M personnel must check the space occupied by each disk in the elastic block storage attached to the ECS clusters. Then, they must contact the business side to migrate data and release disks. The ECS disk size ranking feature helps O&M personnel easily identify which disks occupy a large space in Apsara Distributed File System so that they can perform targeted cleaning and quickly lower the space usage.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.

2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > ECS Disk Size Ranking**.
4. Select the ECS cluster that you want to query from the **Cluster** drop-down list and click **Search**. All disks attached to the elastic block storage of the selected ECS cluster are listed from large to small based on the actual size of the space they occupy in Apsara Distributed File System. You can view the cluster name, cluster ID, and zone of the selected cluster, as well as the storage type, size, and identifier of each disk.
5. (Optional) you can click **Reset** to clear the preceding search conditions.

9.1.4.2. EBS dashboard

The EBS Dashboard module allows you to view the overview information and cluster usage trend charts of EBS clusters.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > EBS Dashboard**. On the page that appears, cluster overview information and cluster usage trend charts of all EBS clusters are displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. View the following information:
    - The **Overview** section shows data overview information of the selected cluster, including the storage space, server information, and health information.

      In the **Health** section, when the value of **Abnormal Cloud Disks**, **Abnormal Masters**, **Abnormal Block GcWorker**, or **Abnormal Block Servers** is greater than 0, it is displayed in red.
    - The **Trend Chart of Cluster Usage** section shows the storage usage curve of the cluster for the last 30 days.

9.1.4.3. Block master operations

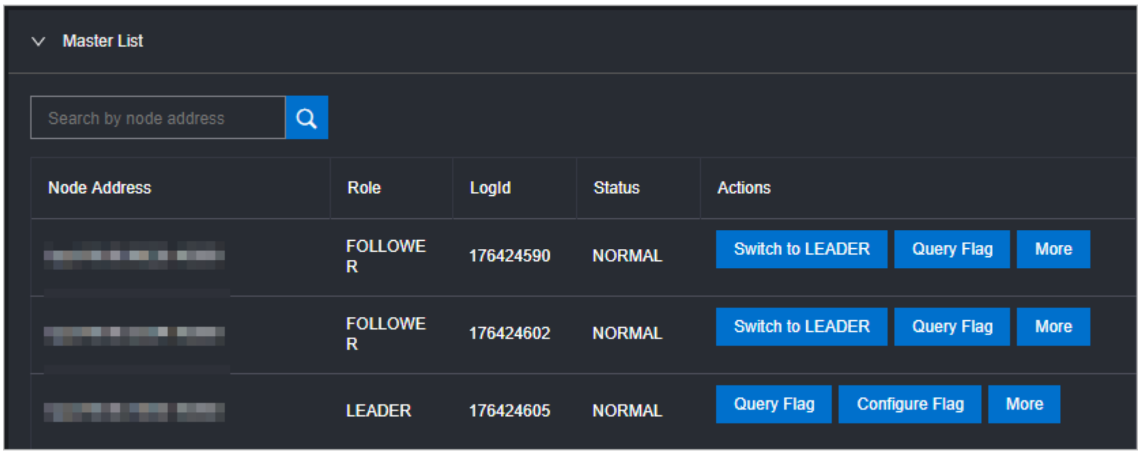
The Block Master Operations module shows the block master node information of EBS clusters, including the IP addresses and roles of nodes. The module also allows you to switch the role of a node to LEADER as well as query and configure flags.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Block Master Operations**. On the page that appears, the master node list and cluster information of the first cluster in the **Cluster Name** drop-down list are displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. In the **Master List** section, perform the following steps:

- View the master node list

  You can view the master node information of the selected cluster, including the IP address, role, log ID, and status.

Node Address	Role	LogId	Status	Actions
[redacted]	FOLLOWER	176424590	NORMAL	Switch to LEADER Query Flag More
[redacted]	FOLLOWER	176424602	NORMAL	Switch to LEADER Query Flag More
[redacted]	LEADER	176424605	NORMAL	Query Flag Configure Flag More

- Switch to LEADER

  A LEADER role for a master node has the same functions as a FOLLOWER role, including controlling and scheduling resources, as well as controlling deployment and service configurations.

  If a node in the master node list assumes a FOLLOWER role, you must switch its role to LEADER. Click **Switch to LEADER** in the **Actions** column. In the message that appears, click **OK**.

- Query a flag

  In the master node list, click **Query Flag** in the **Actions** column corresponding to a node. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the block master node are displayed.

  Perform the following steps to query the flag_key value:

  a. In the left-side navigation pane of the Apsara Infrastructure Management Framework console, choose **Operations > Cluster Operations**.

  b. Enter EBS in the **Cluster** search box.

  c. Find the EBS cluster and click the cluster name.

  d. Click the **Configure** tab.

  e. Find the *pangu_blockmaster_flag.json* file in */services/EbsBlockMaster/user/pangu_blockmaster*.

     The flag_key values of all block master nodes are stored in the *pangu_blockmaster_flag.json* file.

- Configure a flag

  If you want to modify the deployment and service configurations of a block master node, you can configure a flag and assign it to the node.

  In the master list, find a node that assumes the LEADER role and click **Configure Flag** in the **Actions** column. In the dialog box that appears, configure the parameters and click **OK**.

  The following table describes the parameters.

Parameter	Description
flag_key	This value is obtained from the service template of the EBS cluster that is stored in the *pangu_blockmaster_flag.json* file.
flag_value	This value is customized.
flag_type	Select a flag type. Valid values: ■ **int** ■ **bool** ■ **string** ■ **double**

- Check the maser node status

  In the master node lits, choose **More > Check Master Status** in the **Actions** column corresponding to a node.

- Query the version information

  In the master node list, choose **More > Query Version Information** in the **Actions** column corresponding to a node.

6. In the **Cluster Overview** section, you can query the disk size, number of segments, total storage size, and storage usage of the cluster.

9.1.4.4. Block server operations

The Block Server Operations module shows the block server node information of EBS clusters, including the IP address, status, and real-time server load. The module also allows you to query and modify flags, configure server node status, as well as add nodes to and delete nodes from blacklists.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Block Master Operations**. On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. In the **Server List** section, perform the following operations:
   - View the server node list

     You can view server node information of the cluster, including the IP addresses, status, number of segments, and real-time load (read IOPS, write IOPS, read bandwidth, write bandwidth, read latency, and write latency).

   - Query a flag

In the server list, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the block server node are displayed.

Perform the following steps to query the flag_key value:

a. In the left-side navigation pane of the Apsara Infrastructure Management Framework console, choose **Operations > Cluster Operations**.

b. Enter EBS in the **Cluster** search box.

c. Find the EBS cluster and click the cluster name.

d. Click the **Configure** tab.

e. Find the *pangu_blockserver_flag.json* file in */services/EbsBlockServer/user/pangu_blockserver*.

   The flag_key values of all block server nodes are stored in the *pangu_blockserver_flag.json* file.

- Configure a flag

  In the server list, find a node and click **Configure Flag** in the **Actions** column. In the dialog box that appears, set flag_key and flag_value, select flag_type, and then click **OK**.

  The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the *pangu_blockserver_flag.json* file.
flag_value	The customized falg value.
flag_type	The flag type. Valid values: ■ **int** ■ **bool** ■ **string** ■ **double**

- Configure server node status

  In the server list, find a node and choose **More > Set Server Status** in the **Actions** column. In the dialog box that appears, specify server node status and click **OK**.

  The following table describes the server node status.

Status	Description
NORMAL	Indicates that the node is running normally.
DISCONNECTED	Indicates that the node is disconnected.
OFFLOADING	Indicates that the node is being disabled.

Status	Description
OFFLOADED	The node is disabled.
UPGRADE	The node is upgraded.
RECOVERY	The node is restored.

- Query the version information

  In the server list, find a node and choose **More > Query Version Information** in the **Actions** column. In the dialog box that appears, view the version information of the block server node.

6. In the **Block Server Blacklist** section, perform the following operations:

   - Add a block server node to the blacklist

     In the upper-right corner of the **Block Server Blacklist** section, click **Add**. In the dialog box that appears, select the IP address of the block server node that you want to add to the blacklist and click **OK**.

     The block server node that was added to the blacklist is disabled and no longer provides services.

   - View the block server blacklist

     You can view all block server nodes that are added to the blacklist in the **Block Server Blacklist** section.

   - Remove a block server node from the blacklist

     In the **Block Server Blacklist** section, find the block server node that you want to remove from the blacklist and click **Delete** in the **Actions** column. In the message that appears, click **OK**.

     The block server node that is removed from the blacklist can continue to provide services.

9.1.4.5. SnapShotServer

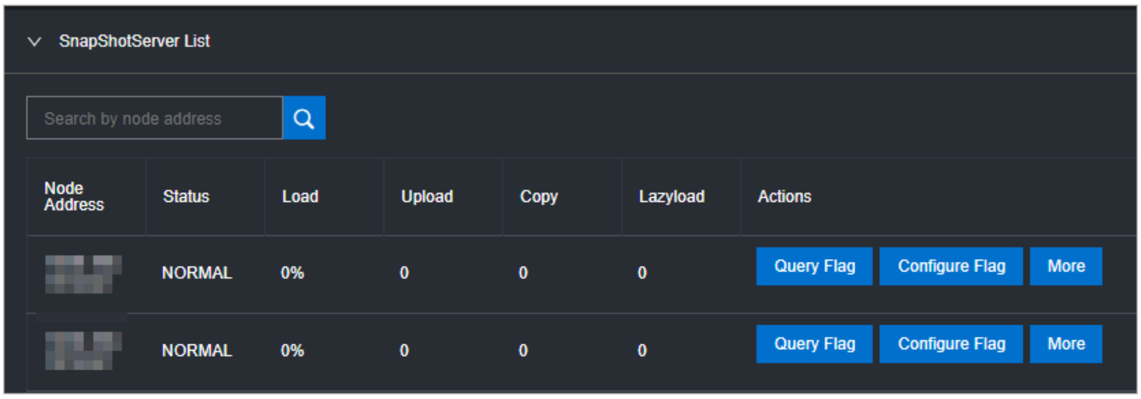
The SnapShotServer module shows the snapshot server node information of EBS clusters, including the IP address, status, and other performance parameters. The module also allows you to query and modify flags and configure snapshot server node status.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > SnapShotServer**. On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. Perform the following operations:

   - View the snapshot server node list

     You can view snapshot server node information of the cluster, including the IP address, status, loading rate, and the number of uploads, replicas, and delayed loadings.



SnapShotServer List

Search by node address

Node Address	Status	Load	Upload	Copy	Lazyload	Actions
[redacted]	NORMAL	0%	0	0	0	Query Flag Configure Flag More
[redacted]	NORMAL	0%	0	0	0	Query Flag Configure Flag More

- Query a flag

  In the snapshot server node list, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the snapshot server node are displayed.

  Perform the following steps to query the flag_key value:

  a. In the left-side navigation pane of the Apsara Infrastructure Management Framework console, choose **Operations > Cluster Operations**.

  b. Enter EBS in the **Cluster** search box.

  c. Find the EBS cluster and click the cluster name.

  d. Click the **Configure** tab.

  e. Find the *pangu_snapshotserver_flag.json* file in */services/EbsSnapshotServer/user/pangu_snapshotserver*.

     The flag_key values of all snapshot server nodes are stored in the *pangu_snapshotserver_flag.json* file.

- Configure a flag

  In the snapshot server node list, find a node and click **Configure Flag** in the **Actions** column. In the dialog box that appears, set flag_key, flag_value, and flag_type, and then click **OK**.

  The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the *pangu_snapshotserver_flag.json* file.
flag_value	The customized flag value.
flag_type	The flag type. Valid values: ▪ int ▪ bool ▪ string ▪ double

- Configure the snapshot server node status

  In the snapshot server node list, find a node and choose **More > Set snapshotserver Status** in the **Actions** column. In the dialog box that appears, select the snapshot server node status and click **OK**.

  The following table describes the snapshot server node status.

Status	Description
NORMAL	Indicates that the node is running normally.
DISCONNECTED	Indicates that the node is disconnected.
OFFLOADING	Indicates that the node is being disabled.
OFFLOADED	Indicates that the node is disabled.

- Query the version information

  In the snapshot server node list, find a node and choose **More > Version Information** in the **Actions** column. In the dialog box that appears, view the version information of the node.

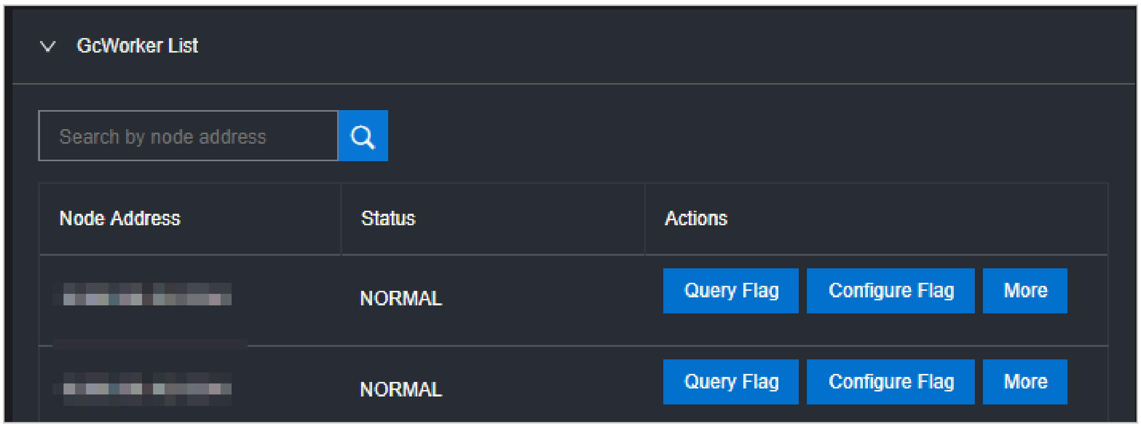
9.1.4.6. Block gcworker operations

The Block Gcworker Operations module allows you to view the IP addresses and status of block gcworker nodes in EBS clusters. You can also query and modify flags, configure the gcworker node status, and query version information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Block Gcworker Operations**. On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. Perform the following operations:
   - View the gcworker node list

     You can view the IP addresses and status of the block gcworker nodes in the selected cluster.



Node Address	Status	Actions
[redacted]	NORMAL	Query Flag Configure Flag More
[redacted]	NORMAL	Query Flag Configure Flag More

- Query a flag

  In the gcworker node list, find a node and click **Query Flag** in the **Actions** column. In the dialog box that appears, set flag_key and click **Submit**. The deployment and service configurations of the block gcworker node are displayed.

  Perform the following steps to query the flag_key value:

  a. In the left-side navigation pane of the Apsara Infrastructure Management Framework console, choose **Operations > Cluster Operations**.

  b. Enter EBS in the **Cluster** search box.

  c. Find the EBS cluster and click the cluster name.

  d. Click the **Configure** tab.

  e. Find the *pangu_blockgcworker_flag.json* file in */services/EbsBlockGCWorker/user/pangu_blockgcworker*.

     The flag_key values of all block server nodes are stored in the *pangu_blockgcworker_flag.json* file.

- Configure a flag

  In the gcworker node list, find a node and click **Configure Flag** in the **Actions** column. In the dialog box that appears, set flag_key, flag_value, and flag_type and click **OK**.

  The following table describes the parameters.

Parameter	Description
flag_key	The flag key. The value of this parameter is obtained from the service template of the EBS cluster that is stored in the *pangu_blockgcworker_flag.json* file.
flag_value	The customized flag value.
flag_type	The flag type. Valid values: ▪ int ▪ bool ▪ string ▪ double

- Configure the gcworker node status

  In gcworker node list, find a node and choose **More > Configure gcworker Status** in the **Actions** column. In the dialog box that appears, specify the gcworket node status and click **OK**.

  The following table describes the gcworker node status.

Status	Description
NORMAL	Indicates that the node is running normally.
DISCONNECTED	Indicates that the node is disconnected.
OFFLOADING	Indicates that the node is being disabled.
OFFLOADED	Indicates that the node is disabled.

- Query the version information

  In the gcworker node list, find a node and choose **More > Query Version Information** in the **Actions** column. In the dialog box that appears, view the version information of the block gcworker node.

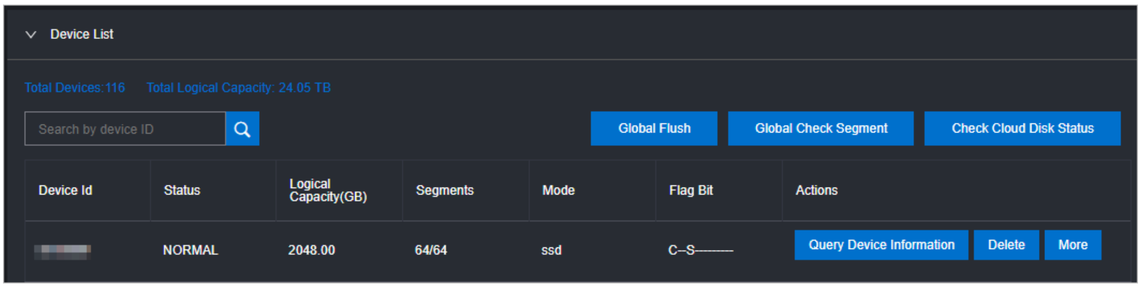
9.1.4.7. Device operations

The Device Operations module allows you to view disk information in EBS clusters, such as the disk ID, status, capacity, and category. You can also perform flush operations, modify disk configurations, query segment information, and enable, disable, delete, or restore devices.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Device Operations**. On the page that appears, the information of the first cluster in the **Cluster Name** drop-down list is displayed.
4. Select a cluster from the **Cluster Name** drop-down list.
5. Perform the following operations:
   - View the device list

     You can view the total number of devices, the total logical space of devices, and information about each device in the cluster, including the device ID, status, logical capacity, number of segments, mode, and flags.

     Total Devices:116 Total Logical Capacity: 24.05 TB

Device Id	Status	Logical Capacity(GB)	Segments	Mode	Flag Bit	Actions
[redacted]	NORMAL	2048.00	64/64	ssd	C--S--------	Query Device Information Delete More

   - Global check segments

In the upper-right corner of the **Device List** section, click **Global Check Segment**. You can view all the segments in the selected cluster and their indexes and status.

- Check disk status

  In the upper-right corner of the **Device List** section, click **Check Cloud Disk Status**. You can view the number of invalid disks in the selected cluster.

- Query device information

  In the device list, click **Query Device Information** in the **Actions** column corresponding to a device. In the dialog box that appears, view the disk information such as the disk ID, status, and capacity.

- Delete a device

  In the device list, click **Delete** in the **Actions** column corresponding to a disk.

  After you delete the disk, its status becomes **DELETING**, and the disk is unavailable. You are not allowed to perform operations on the deleted disk, such as enabling the device or modifying the configurations.

- Restore a device

  In the device list, find a deleted device that is in the **DELETING** state and click **Restore** in the **Actions** column. In the dialog box that appears, click **OK** to restore the deleted device to its normal state.

  After you restore the disk, it becomes available. You can perform operations on the disk, such as enabling the disk and modifying the configurations.

- Enable a device

  In the device list, find a device and choose **More > Enable** in the **Actions** column. In the dialog box that appears, configure the required parameters and click **Submit**.

  > ⓘ **Note** You can perform read and write operations on a disk only after the disk is enabled.

  The following table describes the parameters for enabling a device.

Parameter	Description
client_ip	Optional. Specifies the client on which the disk is enabled. The client IP address is the IP address of the block server. If the client IP address is not specified, the IP address of the local server is used.
token	Specifies a string as a token to be used to disable the device.
mode	Specifies the disk mode. Valid values: ■ **ro**: read-only ■ **rw**: read/write Default value: **rw**.

- Disable a device

  Notice After a disk is disabled, data can no longer be read from or written to the disk. Proceed with caution.

  In the device list, find a device and choose **More** > **Disable** in the **Actions** column corresponding to the device. In the dialog box that appears, configure the parameters and click **Submit**.

  The following table describes the parameters for disabling a device.

Parameter	Description
client_ip	Specifies the client IP address of the disk to be disabled. If the client IP address is not specified, the IP address of the local server is used.
token	Specifies the token for disabling the device, which is configured when the device is enabled. You can query the token by running the **dev -query** command on any server located in the EBS cluster.
open_ver	Specifies the current openversion of the device if the client IP address is not specified. If a client IP address is specified, you do not need to specify openversion. You can query openversion by running the **dev -query** command on any server in the EBS cluster.

- Flush

  In the device list, find a device and choose **More** > **Flush** in the **Actions** column corresponding to the device. In the dialog box that appears, configure the parameters and click **Submit**.

  The following table describes the parameters.

Parameter	Description
segment	Specifies the segments to be flushed. If you do not specify segments, all segments are flushed.
ifnsw	Valid values: ■ **0**: specifies to flush the index file. ■ **1**: specifies not to flush the index file.
dfnsw	Valid values: ■ **0**: specifies to flush the data files. ■ **1**: specifies not to flush the data files.

Parameter	Description

- Global flush

  You can perform the flush operation to clear disks or the transaction logs of segments.

  On the right of the **Device List** section, click **Global Flush**. In the dialog box that appears, select ifnsw and dfnsw, and click **OK**. Then, the transaction logs of all the disks or segments in the current cluster are flushed.

- Query configuration status

  In the device list, find a device and choose **More > Query Configuration Status** in the **Actions** column corresponding to the device. In the dialog box that appears, enter config_ver and click **OK**. You can determine whether the disk is configurable based on the check result.

  config_ver is the config_version parameter of the queried device information.

- Modify device configurations

  You can modify the configurations of a disk, such as specifying whether to enable data compression, compression algorithms, and storage modes.

  In the device list, find a device and choose **More > Modify Device Configurations** in the **Actions** column corresponding to the device. In the dialog box that appears, modify the parameters and click **OK**.

  The following table describes the parameters.

Parameter	Description
compress	Specifies whether to enable data compression. Valid values: ■ **enable** ■ **disable**
algorithm	Specifies a data compression algorithm. Valid values: ■ **0**: indicates that no data compression algorithms are used. ■ **1**: indicates that the snappy data compression algorithm is used. ■ **2**: indicates that the LZ4 data compression algorithm is used.
ec	Specifies whether to enable the EC storage mode. Default value: disable. Valid values: ■ **enable** ■ **disable**

Parameter	Description
data_chunks	Specifies the number of data chunks. Default value: 8.
parity_chunks	Specifies the number of parity chunks. Default value: 3.
packet_bits	Specifies the size of single data block in EC mode. Default value: 15.
copy	Specifies the number of data replicas. Default value: 3.
storage_mode	Specifies the storage mode of the disk.
cache	Specifies whether to enable the cache mode. Default value: 0. Valid values: ■ **0**: disabled ■ **1**: enabled
storage_app_name	Specifies the data storage name.
simsuppress	Specifies whether to enable the delay simulation feature. Default value: disable. Valid values: ■ **enable** ■ **disable**
baselatency	Specifies the basic latency. Default value: 300.
consumespeed	Specifies the processing speed. Default value: 256 bit/μs.
lat80th	Specifies the quantile jitter control of the latency as 80%.
lat90th	Specifies the quantile jitter control of the latency as 90%.
lat99th	Specifies the quantile jitter control of the latency as 99%.

- Query segment information

  In the device list, find a device and choose **More > Segment Information** in the **Actions** column corresponding to the device. In the dialog box that appears, view the information about the segments, such as the index and status.

- Check a segment

  In the device list, find a device and choose **More > Check Segment** in the **Actions** column corresponding to the device. In the dialog box that appears, select the segment to be checked and click **Submit**.

9.1.4.8. Enable or disable Rebalance

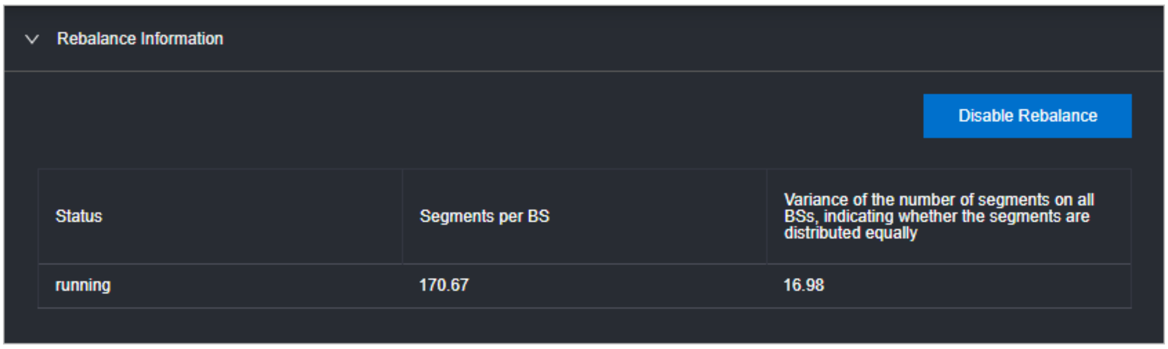
When segments are unevenly distributed among block servers, you can enable the Rebalance feature to redistribute the segments. After you redistribute the segments, you can disable Rebalance.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Rebalance**.
4. Click **Enable Rebalance** or **Disable Rebalance**.

   After you click **Enable Rebalance**, the status of Rebalance changes to **running**.

   After you click **Disable Rebalance**, the status of Rebalance changes to **stopped**.

   Rebalance Information

Status	Segments per BS	Variance of the number of segments on all BSs, indicating whether the segments are distributed equally
running	170.67	16.98

9.1.4.9. IO hang fault analysis

The IO HANG module allows you to view the affected virtual machine (VM) list, VM cluster statistics, and device cluster statistics.

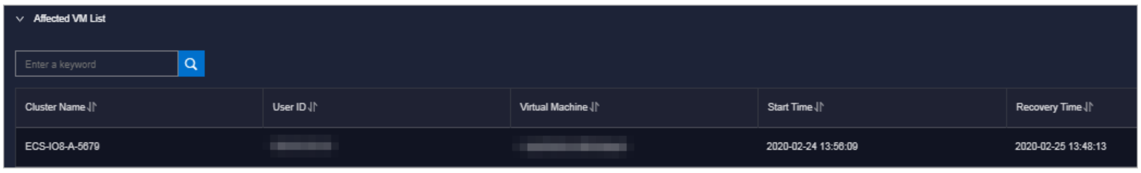
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > IO HANG**. By default, the system shows the affected VM list, VM cluster statistics, and device cluster statistics for the last 24 hours.
4. Select a time range (**One Hour**, **Three Hours**, **Six Hours**, **One Day**, or a customized time range) and click **Search**. View the following information:

   - **Affected VM List**

     The **Affected VM List** section shows the IO hang start time and recovery time of all the VMs, as well as the cluster name and user ID of the cluster to which these VMs belong.

     To view the information of a cluster, a user, or a VM, enter the cluster name, user ID, or VM name in the search box to perform a fuzzy search.

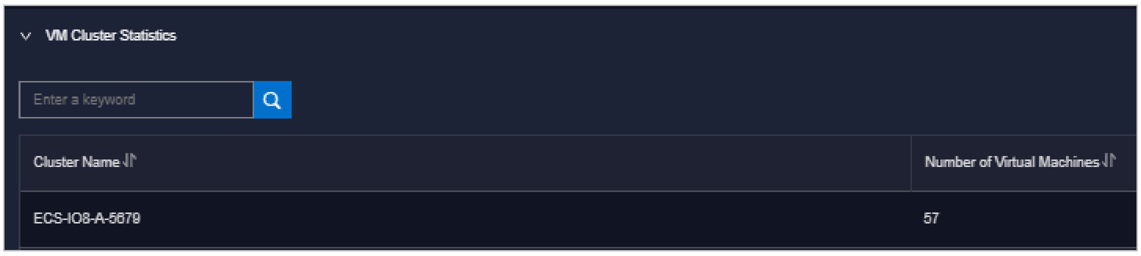
     Affected VM List

Cluster Name	User ID	Virtual Machine	Start Time	Recovery Time
ECS-IO8-A-5679	[redacted]	[redacted]	2020-02-24 13:56:09	2020-02-25 13:48:13

   - **VM Cluster Statistics**

     The **VM Cluster Statistics** section shows the number of affected VMs in a cluster.

To view the VM statistics of a cluster, enter the cluster name in the search box to perform a fuzzy search.



VM Cluster Statistics

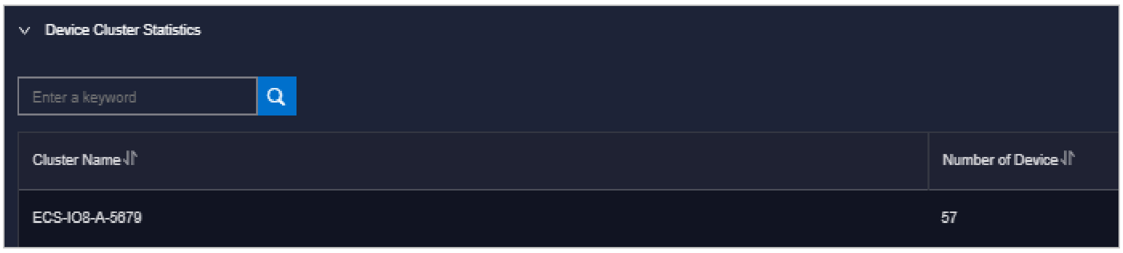
Enter a keyword

Cluster Name	Number of Virtual Machines
ECS-IO8-A-5679	57

- **Device Cluster Statistics**

  The **Device Cluster Statistics** section shows the number of affected devices in a cluster.

  To view the device statistics of a cluster, enter the cluster name in the search box to perform a fuzzy search.



Device Cluster Statistics

Enter a keyword

Cluster Name	Number of Device
ECS-IO8-A-5679	57

9.1.4.10. Slow IO analysis

The Slow IO Analysis page allows you to view the slow IO list, top ten NCs, cluster statistics, top five cluster statistics, and reasons.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > SLOW IO**. By default, the system shows the slow IO list, top ten NCs, cluster statistics, top five cluster statistics, and reasons in the last 24 hours.
4. Select the time range (**One Hour**, **Three Hours**, **Six Hours**, **One Day**, or customize the time range) and click **Search**. View the following information:
    - **Slow IO List**

      The **Slow IO List** section shows the slow IO-related cluster name, NC IP address, virtual machine, device ID, storage type, start time, recovery time, number of slow IOs, and causes.

      To view the information of a cluster, an NC, or a block device, you can enter the cluster name, NC IP address, or device ID in the search box to perform a fuzzy search.

      You can also sort data by Cluster Name, NC IP, Virtual Machine, Device ID, Storage Type, Start Time, Recovery Time, Number of Slow IO, or Reason.

    - **Top10 NC**

      The system shows the information of the top ten NCs on a graph and table.

      Notes:

- The **Graphical Analysis** section shows the proportion for the number of slow IO in each cluster of the top ten NCs by using a pie chart.
- The **Top10 NC** section shows the NC IP address, cluster name, number of slow IOs, percentage, and primary cause of slow IOs on the top ten NCs.

  To view the information of a cluster or NC, enter the NC IP address or cluster name in the search box to perform a fuzzy search.

  You can also sort data by NC IP, Cluster Name, Slow IO, and Major Reason.

- **Cluster Statistics**

  The **Cluster Statistics** section shows the cluster name, number of devices, number of slow IOs, percentage, and primary cause of slow IOs on clusters.

  To view the information of a cluster, enter the cluster name in the search box to perform a fuzzy search.

  You can also sort data by Cluster Name, Number of Device, Number of Slow IO, and Major Reason.

- **Top Five Cluster Statistics**

  The system shows the statistics of top five clusters by using a graph and a table.

  Notes:

  - The **Graphical Analysis** section shows the proportion for the number of slow IOs on each of the top five clusters on a pie chart.
  - The **Top Five Cluster Statistics** section shows the cluster name, number of devices, number of slow IOs, percentage, and primary cause of slow IOs on the top five clusters on a table.

    To view the information of a cluster, enter the cluster name in the search box to perform a fuzzy search.

    You can also sort data by Top Five Cluster, Number of Device, Number of Slow IO, and Major Problem.

- **Reason**

  The system shows the primary cause on a graph and table.

  Notes:

  - The **Graphical Analysis** section shows the proportion of reasons by using a pie chart.
  - The **Reason** section shows the number of slow IO from the dimension of reasons.

    To query the information of a reason, enter the reason information in the search box to perform a fuzzy search.

    You can also sort data by Reason and Number of Slow IO.

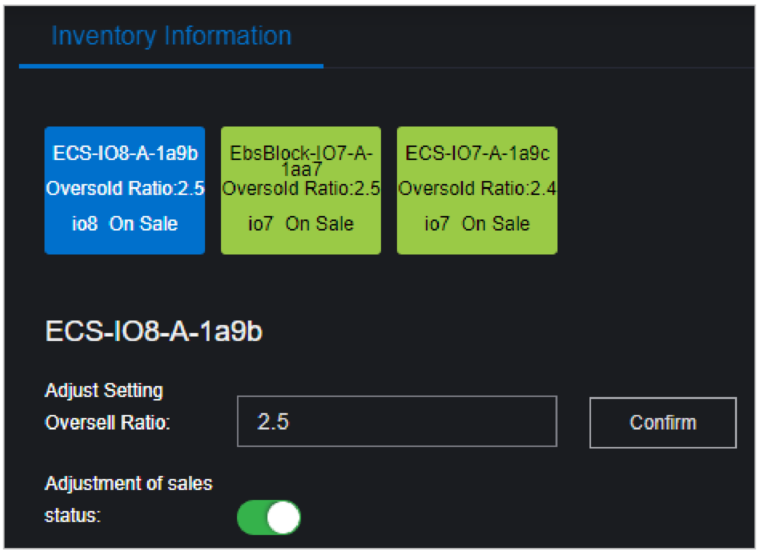
9.1.4.11. Product settings

The Product Settings module allows you to view the sales status of a cluster, configure the oversold ratio of a cluster, and specify whether a cluster is available for sale.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.

2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Apsara Distributed File System Management > Product Settings**. By default, the system shows the data of each cluster within the current environment, including the cluster name, oversold ratio, and sales status.



Inventory Information

ECS-IO8-A-1a9b
Oversold Ratio:2.5
io8 On Sale

EbsBlock-IO7-A-1aa7
Oversold Ratio:2.5
io7 On Sale

ECS-IO7-A-1a9c
Oversold Ratio:2.4
io7 On Sale

ECS-IO8-A-1a9b

Adjust Setting Oversell Ratio: 2.5

Confirm

Adjustment of sales status:

4. Perform the following operations:
   - Select a cluster, enter a number in the **Adjust Setting Oversell Ratio** field, and then click **Confirm** to set the oversold ratio of the cluster.
   - Select a cluster and turn on or off **Adjustment of sales status** to enable or disable the cluster for sale.

9.1.5. VM hot migration

9.1.5.1. Overview

Hot migration is the process of migrating a running VM from one host to another. During migration, the VM runs normally and its services are not aware that any migration task is occurring. However, these services can detect a very short interruption between 100 and 1,000 ms.

Scenarios

During system operations and maintenance, hot migration is typically used for the following scenarios:

- **Active O&M**: The host is faulty and must be repaired, but the fault does not affect the operation of the system. You can use hot migration to migrate the VM to another host and repair the faulty host in offline mode.
- **Server load balancing**: When a host is experiencing a high load, you can migrate some of its VMs to other idle hosts to reduce resource consumption on the source host.
- Other scenarios where a VM must be migrated without affecting its business operations.

9.1.5.2. Limits on hot migration

Before performing hot migration, you must understand the limits.

The hot migration feature of Apsara Stack is subject to the following limits:

- Only the go2hyapi command can be used to implement hot migration in the KVM virtualization environment. ECS Operations and Maintenance Platform does not support hot migration.
- Only standard ECS instances support hot migration. ECS provides a list of migratable images. Alibaba Cloud does not take any responsibility for errors that occur when migrating a VM that is not included in the list of migratable images.
- If a VM is used as an RS to provide SLB or as a client to access SLB, the previous session will be closed after hot migration. New sessions created after migration are not affected.
- Migration can only be performed between hosts of the same type. Furthermore, each host must be running the same versions of software.
- Hot migration is not supported in DPDK avs scenarios.
- VMs using local storage solutions do not support hot migration. This is because after a VM is migrated to another host, it can no longer access the previous local storage space.
- VMs that use GPU, FPGA, or other (passthrough or SR-IOV) devices do not support hot migration.

> **Note** VMs created in Apsara Stack versions earlier than V3.3 do not support hot migration. Hot migration becomes available after you restart the VMs.

9.1.5.3. Complete hot migration on AG

In the Apsara Uni-manager Operations Console, you can run commands to start and cancel hot migration operations.

Trigger hot migration

After hot migration is triggered for a VM, you can run the `go2which` command or use the ECS Operations and Maintenance System to check that the VM enters the migrating state. When hot migration is complete, the VM changes to the running state.

To trigger hot migration, run the following `go2which` command:

```
go2hyapi live_migrate_vm == Functions usage: == |- live_migrate_vm <vm_name> [nc_id] [rate] [no_check_image] [no_check_load] [downtime]== Usage: == houyi_api.sh <function_name> [--help|-h] [name=value]
```

Parameters

Parameter	Description	Impact	Value
vm_name	The name of the VM to migrate.	N/A	N/A
nc_id	Specifies the destination NC to which to migrate the VM.	If the NC does not support the specifications of the VM, the VM may fail to be migrated.	N/A
rate	The amount of bandwidth to allocate for the migration task.	The migration uses the bandwidth resources of the physical machines.	• 10 GB network: 80 MB • 1 GB network: 40 MB

Parameter	Description	Impact	Value
downtime	The maximum allowable downtime caused by migration. The default value is 300 ms.	The service downtime caused by migration is affected.	200 ms to 2,000 ms
no_check_image	Forcibly migrates images that are not supported.	The SLA may be violated if this parameter is set to false.	false
no_check_load	Forcibly migrates images even when the load threshold requirements are not met.	Downtime cannot be controlled if this parameter is set to false.	false

Cancel hot migration

To cancel hot migration, run the following command:

```
go2hyapi cancel_live_migrate_vm  == Usage: ==  houyi_api.sh <function_name> [--help|-h] [name=value] ==
Functions usage: ==  |- cancel_live_migrate_vm <region_id> <vm_name>
```

Parameters

Parameter	Description	Impact	Value
vm_name	The name of the VM to migrate.	N/A	N/A
region_id	The ID of the region where the VM is currently located.	N/A	N/A

9.1.5.4. Modify the position of the NC where the VM is located

When an exception occurs during hot migration and the migration cannot be rolled back through ECS Operations and Maintenance Platform, you can modify the VM state to trigger rollback.

Trigger rollback

If an exception occurs during hot migration, run the following command to trigger rollback:

```
go2hyapi call_api manually_change_migration_status  == Functions usage: ==  |- call_api manually_change_
migration_status <vm_name> <region_id> <where>
```

Parameter description

Parameter	Function	Impact	Value
vm_name	The name of the VM to be migrated.	N/A	N/A
region_id	The ID of the region where the target VM is located.	N/A	N/A
where	The ID of the NC where the VM is located.	N/A	N/A

9.1.5.5. FAQ

This topic lists common problems that you may encounter during hot migration and how to resolve them.

- **Which parameters are required to call the Server Controller API to perform a hot migration?**
    - Vm_name: VM name
    - nc_id
- **What preparations should I make before performing a hot migration operation?**
    - Confirm that the VM is in the running state.
    - Confirm the destination of the VM migration.
- **Can hot migration be canceled? How can I cancel hot migration?**

  Yes. If the API request is successful and the migration has not completed, run the `go2hyapi cancel_live_migrate_vm vm_name=[vm_name] region_id=[region_id]` command to cancel the hot migration. If the VM has completed its migration to the destination NC, it is too late to cancel the hot migration.

  You can get the value of region_id by running the `go2which [vm_name]` command to view region_info.
- **The VM is still in the migrating state after the hot migration has completed, and the cancel_live_migrate_vm command is not working. What should I do?**

  You can run the `virsh query-migrate [domid]` command on the source NC of the VM to check whether the VM is still being migrated. If the VM is still being migrated, a piece of JSON information will be returned. If the VM has finished migration, run the following command on the AG to modify the state of the VM:

  ```
  go2hyapi manually_change_migration_status vm_name=[vm_name] where=[nc_id for the VM] region_id=[region_id]
  ```

  domid is the name of the VM instance. You can run the `virsh list|grep vm_name` command to view it.
- **How can I confirm whether the VM is migrated successfully?**

  On the destination NC of the VM, run the `sudo virsh list|grep [vm_name]` command. If the VM instance exists and is not in the running state, the migration is successful.
- **When an exception occurs during hot migration, which logs should I refer to?**

  - View the Libvirt bottom layer migration log on the NC.

    Run the `/var/log/libvirt/libvirt.log` command to view information about the migration process, such as vport offline, detach, delete, and relay route.

  - Run the following command to view the API management log of Server Controller on the AG:

    ```
    /var/log/houyi/pync/houyipync.log
    ```

  - View the Qemu log.
  - Run the following command to view the regionmaster log on the VM:

    ```
    regionmaster/logs/regionmaster/error.log
    ```

- **A VM fails to start after hot migration. Is the VM still in the pending state?**

  If **error vport update nc conf by vpc master fails dest_nc_id:xxx** is returned, it indicates that a VPC fault has occurred and the underlying task is interrupted.

- **During hot migration, the API returns the following error message: distributed lock fail. What are the possible causes of this issue?**

  The API has been called too many times within a short period of time. Wait several minutes and then try again.

- **What are some common scenarios where migration fails? How can I resolve these issues?**Hot migration issues

Scenario	Cause	Solution
The load is too high and the VM migration does not pass the pressure inspection.	Long service interruption.	You can run no_check_load=true to skip this inspection.
The VM fails to pass image inspection.	It is not an Alibaba Cloud-specified image.	You can run no_check_image=true to skip this inspection. Be aware of the risks involved.

9.1.6. Hot migration of disks

9.1.6.1. Overview

Hot migration seeks to facilitate operations and maintenance of online clusters and improve service operation. Hot migration provides online migration capabilities for virtual disks. This function can also quickly copy data to new locations, enhancing the flexibility of services.

9.1.6.2. Limits

Before performing hot migration on a disk, you need to understand the limits.

Limits

- Only disks of the river type support hot migration.
- The source and destination clusters for hot migration must belong to the same OSS domain.

- Disk sharing is not supported.
- Hot migration is not supported on disks whose capacity is greater than 2 TB.
- Format and capacity changes are not supported.
- Hot migration is only supported within the same zone.
- Due to how hot migration is implemented internally, the names of the source and destination clusters must be less than 15 bytes in length.

> Note
>
> - The data of the original source disk will remain on the disk after hot migration has completed. You can use the pu tool to delete the remaining data. Job recycling is unavailable.
> - During migration, an I/O latency of less than 1 second is considered normal.
> - Migration cannot be rolled back.
> - Migration will consume network bandwidth, so you must take measures to limit concurrent traffic during migration.

Migration operation

For more information about the APIs related to disk hot migration, see "**Disk hot migration**" in *ECS Developer Guide* .

9.1.6.3. O&M after hot migration

The original source disk data remains on the source disk after hot migration and data backup operations are completed. To release disk space, delete the data from the source disk. After the data is deleted from the source disk, the space will be released at a later time.

Procedure

1. On the compute cluster AG, run the `go2houyiregiondbrnd -e 'select task_id from device_migrate_log where status="complete"'` command to obtain *task: allTaskIds*.
2. On the compute cluster AG, run the `go2riverdbrnd -e 'select task_id,src_pangu_path,dst_pangu_path from migration_log where task_id in ($allTaskIds) and status=2 and src_recycled=0 and DATE(gmt_finish) < DATE_ADD(CURDATE(), INTERVAL -1 DAY)'` command.
3. Perform the following operations for each set of <task_id,src_pangu_path,dst_pangu_path>:
   1. Run the `/apsara/deploy/bsutil rlm --dir=$dst_pangu_path|grep 'not-loaded'|wc -l` command on the host that runs the bstools role in the storage cluster. If the command output is not 0, proceed to the next step.
   2. Run the `/apsara/deploy/bsutil delete-image --dir=$src_pangu_path` command on the host that runs the bstools role in the storage cluster.
   3. Run the `/apsara/river/river_admin migrate recycle $task_id` command on the host that runs the river role in the storage cluster.

9.1.7. Upgrade solution

9.1.7.1. Overview

For both hot and cold migration of GPU and FPGA clusters, you must understand the limitations that apply to cluster upgrades.

9.1.7.2. Limits on GPU clusters

Before upgrading a GPU cluster, you must understand the limits.

The upgrade of GPU clusters in Apsara Stack are subject to the following limits:

- GPU clusters are only supported in Apsara Stack 3.3 or later versions.
- To upgrade a GPU cluster, you must restart the NC server.
- VMs that use GPU, FPGA, or other passthrough or SR-IOV devices do not support hot migration.
- The GN5I, GN5E, and GN4 type GPU clusters do not have the specifications of local disk instances and only support offline cold migration.
- When you perform a forced cold migration on GN5 and GA1 type GPU clusters that have specifications of local disk instances, the local disk will be reformatted, resulting in data loss. These disks must be backed up before they can be migrated.

9.1.7.3. Limits on FPGA clusters

Before upgrading an FPGA cluster, you must understand the limits.

The upgrade of FPGA clusters in Apsara Stack are subject to the following limits:

- FPGA clusters are only supported in Apsara Stack 3.5 or later versions.
- VMs in an FPGA cluster must be shut down before the cluster can be upgraded.
- The FPGA service relies on Redis to a great extent. If the Redis service is interrupted during the hot upgrade of Apsara Stack, the FPGA service will be interrupted. The FPGA service will recover after the Redis service is restored. However, if a Redis instance fails to be created, you must restart the FPGA service after the Redis service is restored.

9.1.8. Handle routine alarms

9.1.8.1. Overview

This topic describes the definition of each key metric and how to handle alerts.

The metrics monitored in ECS can be categorized into three types:

- Basic metrics: These metrics are used to monitor the CPU, memory, and correlated service processes of hosts.
- Connectivity metrics: These metrics are used to monitor the connectivity between different components and the connectivity between different networks.
- Service metrics: These metrics are used for service monitoring, such as the state of various types of API requests.

Description of metric types

Metric type	Function	Solution
Basic metric/service availability metric	Monitors the basic performance of the host and the availability of the services on the host. This kind of metrics includes CPU, memory, and handle count.	When CPU utilization is too high: identify which process consumes a large amount of CPU resources. If it is a key process, evaluate whether it can be restarted.
		When the memory usage is too high (for key services): dump the memory data, request the back-end R&D team to analyze the data, and restart the application.
Connectivity metric	Checks the connectivity between each module and its related modules.	• First, check the health status of the corresponding modules. For example, check whether the host works normally and whether services, ports, and domain names are normal. • If two modules that are connected to each other are healthy, check the network connectivity between them.
Service metric	Monitors aspects of key request calls such as the latency, total number, failures of API requests, and database SQL exceptions.	• In case of an API request failure, you must view the corresponding logs to identify the cause of the failure. • In case of a database SQL exception, check whether the exception was caused by a database exception (system breakdown or high connection count) or a problem with the application. If it is an application problem, forward the error information to the back-end R&D team for troubleshooting.

9.1.8.2. API proxy

This topic describes the metrics of API proxy.

Metric description

Metric	Alert item	Description
check_apiproxy_dns	Database HA switchover occurs or not	Checks whether Server Controller database switchover occurs. If so, nginx will be reloaded automatically.
check_apiproxy_conn_new	check_apiproxy_conn_new	Checks the connectivity to the Server Controller database.
		Checks the connectivity to the API Server: • Checks whether the API Server is down. • Checks the network connectivity.

Metric	Alert item	Description
check_apiproxy_proc_new	check_apiproxy_proc_new	Checks the memory usage and CPU utilization for nginx and memcache processes.

9.1.8.3. API Server

The topic describes the metrics of the API Server.

Metric description

Metric	Alert Item	Solution
check_API Server_proc_new	The process does not exist or is abnormal.	Checks the state of the Java process: whether the process exists, and the CPU utilization and memory usage
check_API Server_conn_new	Checks the connectivity between the API Server and Server Controller database.	Checks whether the corresponding component is down. If the corresponding component is down, fix the issue by taking necessary O&M measures. If the database is down, contact DBA to fix the issue. Checks whether the VIP is connected to the corresponding component. If not, contact the network engineer to fix it.
	Checks the connectivity between the API Server and TAIR.	
	Checks the connectivity between the API Server and RegionMaster.	
	Checks the connectivity between the API Server and the RMS.	
check_API Server_perf	Monitors metrics for API requests, such as the latency, total number of API requests, and number of failed API requests.	It is primarily used to identify faults.
check_API Server_errorlog	Checks database exceptions and instance creation failures.	• If an exception occurs to the database, contact DBA to check whether the database is normal. • If the creation of an instance fails, locate the cause of the failure.

9.1.8.4. RegionMaster

This topic describes the metrics of RegionMaster.

Metric description

Metric	Alert item	Description
check_regionmaster_proc	The process does not exist or is abnormal.	Checks the state of the Java process: whether the process exists, and the CPU utilization and memory usage.
check_regionmaster_work	rms_connectivity	Checks the connectivity to RMS.
	regiondb_connectivity	Checks the connectivity to the houyiregiondb database.
	houyi_connectivity	Checks the connectivity to the Server Controller database.
	tair_connectivity	Checks the connectivity to TAIR.
check_zookeeper_work	status	Checks the operating state of the Zookeeper process on the Server Controller.
check_regionmaster_errorlog	errorlog_for_db	Checks whether the SQL statements are properly executed.
	check_regionmaster_errorlog	
check_workflow_master	Checks the operating state of the master in the workflow process.	-
check_workflow_worker	Checks the operating state of the worker in the workflow process.	-

9.1.8.5. RMS

This topic describes the metrics of RMS.

Metric description

Metric	Alert item	Description
check_rms_proc	Checks the process status, CPU utilization, and memory usage of RMS.	-
check_rabbitmq_proc	Checks the process status, CPU utilization, and memory usage of the rabbitmq cluster.	-
check_rabbitmq_status	Checks the number of queues, exchanges, and bindings in the rabbitmq cluster.	Follow the maintenance guide for the rabbitmq cluster.

Metric	Alert item	Description
check_rabbitmq_queues	Checks whether messages are accumulated.	If messages are accumulated, it will also check for the cause.
	Check whether there are consumers.	If there are no consumers, check whether Regionmaster and APIserver are operating normally. If they are operating normally, check whether there is a problem with the rabbitmq cluster.

9.1.8.6. PYNC

This topic describes the metrics that are monitored for PYNC.

Metric description

Metric	Alert item	Description
check_vm_start_failed	Checks the causes of a VM startup fault.	You do not need to handle it immediately. It is typically caused by custom images.
check_pync	Checks the CPU utilization and memory usage of PYNC.	-
	PYNC has too many open file handles.	-
	PYNC process count.	PYNC must have four processes.
	It has been long since pyncVmMonitor.LOG was last updated at ${pync_monitor_log_last_updated}.	Checks for reasons why a log has not updated for a long period of time, such as: • Whether a PYNC process has encountered a problem. • Whether the NC is running a key process called Uninterruptible Sleep.

9.1.8.7. Zookeeper

This topic describes the metrics of Zookeeper.

Metric description

Metric	Alert item	Description
check_zookeeper_proc	proc	The process does not exist.
		The memory usage or CPU utilization is too high.

9.1.8.8. AG

This topic describes the metrics of AGs.

Metric description

Metric	Alert item	Description
disk_usage	apsara_90	*/apsara* disk usage.
	homeadmin_90	Usage of */home/admin*.
check_system_ag	mem_85	Memory usage.
	cpu_98	CPU utilization.
	df_98	Disk usage of the root directory.
check_ag_disk_usage	check_ag_disk_usage	Disk usage.
check_nc_down_new	check_recover_failed	Checks the causes of a VM migration fault. Possible causes include: • No resources are available in the cluster. • A VM does not belong to any cluster.
	check_repeat_recovered	Continuous VM migration.
	check_continuous_nc_down	Checks continuous NC downtime.
	check_nc_down_with_vm	The state of the NC in the database is nc_down, but there are still VMs operating normally on the NC. Checks the NC for hardware faults: • If a hardware fault occurs, you must perform operations and maintenance to resolve the fault. • If no hardware fault is detected, restore the NC and change its state to locked.
check_ag_fhtd_new	Checks whether the FHT downtime migration tool, mostly used by local disks, is operating normally.	If the tool does not exist, download the FHT downtime migration tool.

9.1.8.9. Server groups

This topic describes the metrics that are monitored for server groups.

Metric description

Metric	Alert item	Description
check_pync	pync_mem	Monitors the memory usage of PYNC.
	pync_cpu	Monitors the CPU utilization of PYNC.
	pync_nofile	Monitors the number of PYNC handles.
	pync_nproc	Monitors the number of PYNC processes.
	pync_monitor_log_not_updated	Monitors the status of PYNC scheduled tasks.

9.1.9. Inspection

9.1.9.1. Overview

ECS inspection includes cluster basic health inspection and cluster resources inspection.

9.1.9.2. Cluster basic health inspection

9.1.9.2.1. Overview

Cluster basic health inspection includes monitoring inspection, inspection of basic software package versions, and basic public resources inspection.

9.1.9.2.2. Monitoring inspection

This topic describes basic monitoring inspections and connectivity monitoring inspections.

9.1.9.2.3. Inspection of basic software package versions

This topic describes the version inspections of Server Controller components, Apsara system, virtualization packages, and basic service packages.

9.1.9.2.4. Basic public resources inspection

This topic describes ISO inspections and basic image inspections.

ISO inspection

ECS Operations and Maintenance System provides two basic ISO files for each region:

- linux-virt-release-xxxx.iso
- windows-virt-release-xxxx.iso

You can run the following command to search the database for relevant information:

```
$ houyiregiondb
mysql>select name,os_type,version,path,oss_info from iso_resource where os_type! =''\G
```

Parameters in the command are as follows:

- *name*: the name of the ISO file, such as xxxx.iso.
- *os_type*: the operating system (OS) type of an image.
- *path*: the path on the Apsara Distributed File System cloud disk where the ISO file is stored. You can run the `/apsara/deploy/pu meta $path` command to check whether the ISO exists in the files of Apsara Distributed File System.
- *oss_info*: the path on the local OSS disk where the ISO file is stored. To search for this path, you must provide relevant information to OSS support engineers for inspection.

Basic image inspection

- Run the following command to check the state of a basic image in the database:

  ```
  houyiregiondb
  mysql>select image_no,status,visibility,platform,
  region_no from image;
  ```

- Check whether the basic image is usable. You can call the create_instance API to use relevant images to create a VM and manually check whether the VM can operate normally.

9.1.9.3. Cluster resource inspection

9.1.9.3.1. Overview

Cluster resource inspection includes cluster inventory inspection and VM inspection.

9.1.9.3.2. Cluster inventory inspection

This topic describes the inspections of cluster inventory resources. Cluster inventory resources are specified by the number of VMs that can be created by using the remaining resources in the cluster. You can use the database to obtain the cluster inventory resources.

Suppose you need to inspect the inventory resources of a cluster based on 16-core 64 GB VMs. Run the following command to obtain the inventory resources of the cluster:

```
$ houyiregiondb
mysql> select sum( least ( floor(available_cpu/16),floor(available_memory/64/1024))) from nc_resource,nc w
here nc.cluster_id=$id and nc.biz_status='free' and nc.id=nc_resource.id;
```

If the current cluster contains a relatively large VM, ensure that the cluster has enough free resources to handle the VM, as well as an available host with sufficient resources for backup. This host will be the migration destination of the large VM in case the current host goes down. Otherwise, the large VM cannot be migrated when its host goes down, and you will have to either use hot migration to transfer resources or release redundant VMs in the cluster.

NC state inspection

NC state inspection mainly checks whether the state of a host is normal in the database and Apsara Infrastructure Management Framework.

- A host can be in one of the following states in Apsara Infrastructure Management Framework:
  - Good: indicates that the host is in a normal working state.

- Error: indicates that the host has an active monitoring alert.
- Probation: indicates that the host is in the probationary period and may fail.
- OS _error: indicates that the host has failed and is being cloned.
- Hw_error: indicates that the hardware of a host has failed and is being repaired.
- OS _probation: indicates the host is recovering from a fault or hardware failure and is in a probationary period. If the host recovers within the probationary period, the state will change to probation. If the host fails to recover within the probationary period (an error is reported), the state will change to OS _error.

> **Note** The Good state is considered to be the stable state, and all other states are considered to be unstable states.

- Cluster definitions for Apsara Infrastructure Management Framework:
  - Default cluster: the cluster where NCs are placed when they go offline.
  - Non-default cluster: the cluster for online NCs.

  An NC that is operating normally is placed in a non-default cluster, and is in the Good state.

The mappings of host states between the ECS database and Apsara Infrastructure Management Framework are described in Mappings of host states between the ECS database and Apsara Infrastructure Management Framework.

Mappings of host states between the ECS database and Apsara Infrastructure Management Framework

Host states in ECS database	Cluster	Host state	Scenario
mlock	Non-default cluster	Unstable	A host that goes online is immediately and proactively locked.
locked	Non-default cluster	Unstable	An NC needs to be unlocked.
free	Non-default cluster	Stable	A host operates normally.
nc_down	Non-default cluster	Unstable	A host operates normally or is in downtime.
offline	Default cluster	Unstable	A host goes offline from business attributes.

9.1.9.3.3. VM inspection

This topic describes pending VM inspections, VM state inspections, and VM resource inspections.

Pending VM inspection

This type of inspection focuses on VMs that have been in the pending state for a long period of time. When a VM has been in the pending state for a long period of time, it is considered a redundant resource. Contact the user to handle it.

VM state inspection

This type of inspection focuses on the VM state consistency. For example, a VM is displayed as stopped in the database, but is displayed as running in NC. During the inspection, the VM states recorded in the database and on the host are checked. If the VM states are inconsistent, corresponding operations are performed.

- Run the following command to obtain the VM state in a database:

  ```
  houyiregiondb –Ne “select status from vm where name=’$name’”
  ```

- Run the following command to obtain the VM state on a host:

  ```
  sudo virsh list | grep $name
  ```

VM resource inspection

After the configuration of a VM is changed, the system checks whether the configuration of the VM recorded in the database is consistent with that used on the host.

- Run the following command to obtain the VM configuration in a database:

  ```
  houyiregiondb –Ne “select vcpu, memory from vm where name=’$name’”
  ```

- Run the following command to obtain the VM configuration on a host:

  ```
  sudo virsh list | grep $name
  ```

  Obtain information about CPU and memory by viewing the corresponding fields.

9.2. Container Service for Kubernetes

9.2.1. Components and features

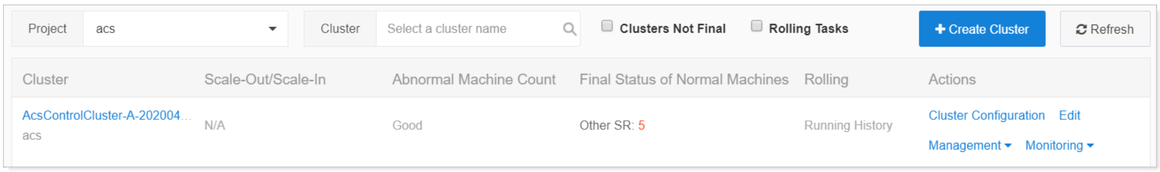
9.2.1.1. Console

The Container Service console provides a graphical user interface (GUI) that serves as a portal for all operations on Container Service. The console uses the deployment mode that applies to standard Java applications on Apsara Stack. The Container Service console consists of a Tengine server and a Jetty container.

Log on to the console

1. Log on to the Apsara Uni-manager Operations Console. In the top navigation bar, click **O&M**. In the left-side navigation pane, choose **Product Management > Products**. In the **Apsara Stack O&M** section, click **Apsara Infrastructure Management Framework**.
2. You are redirected to the **Infrastructure Operation Platform** console. In the left-side navigation pane, click **Reports**.
3. On the **Reports** page, click **Go**.

4. You are redirected to the Apsara Infrastructure Management Framework console. In the top navigation bar, choose **Operations > Cluster Operations**. On the Cluster Operations page, find the Container Service cluster that you want to manage.



Cluster	Scale-Out/Scale-In	Abnormal Machine Count	Final Status of Normal Machines	Rolling	Actions
AcsControlCluster-A-202004... acs	N/A	Good	Other SR: 5	Running History	Cluster Configuration Edit Management ▾ Monitoring ▾

5. Click **Cluster Configuration** in the **Actions** column. On the Cluster Configuration page, find the CosConsoleAliyunCom server role in the **Server Role** section and check the machine of the server role.
6. In the left-side navigation pane, enter the hostname in the Machine search box. Move the pointer over the More icon next to the hostname and select Terminal from the shortcut menu. This allows you to log on to the host by using a terminal session. On the command line, enter `docker ps` to query the ID of the cos-console-aliyun-com container.
7. Run the `sudo docker exec -it container_id bin/bash` command to log on to the container.
8. Go to the specified directory to find Tengine and Jetty.

O&M commands

- Restart Tengine: `/etc/rc.d/init.d/tengine restart`
- Restart Jetty: `/etc/init.d/jetty restart`

Directories

- Root directory of web applications: `/alidata/www/`
- WAR directory of applications: */alidata/www/wwwroot/cos-console-aliyun-com*

Application log files

- The root directory that stores log files: */alidata/www/logs*
- The path to Jetty: */alidata/www/logs/*jetty
- The path to application log files: */alidata/www/logs/java/cos-console-aliyun-com/applog*

9.2.1.2. Troopers

This topic describes the features of Troopers and how to use them.

The Troopers daemon is used to create clusters and machines. You can also use Troopers to manage clusters and machines in Container Service.

Troopers is programmed in Go. Each container runs only the Troopers daemon and does not use any other daemons.

To use Troopers, perform the following steps:

1. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**. In the left-side navigation pane, choose **Product Management > Products**. In the **Apsara Stack O&M** section, click **Apsara Infrastructure Management Framework**.
2. You are redirected to the **Infrastructure Operation Platform** console. In the left-side navigation pane, click **Reports**.

3. On the **Reports** page, click **Go**.
4. You are redirected to the Apsara Infrastructure Management Framework console. In the top navigation bar, choose **Operations > Cluster Operations**. On the Cluster Operations page, find the Container Service cluster that you want to manage. Click **Cluster Configuration** in the Actions column. On the Cluster Configuration page, find the Troopers server role in the Server Role section and check the machine of the server role.
5. In the left-side navigation pane, enter the hostname in the Machine search box. Move the pointer over the More icon next to the hostname and choose Terminal from the shortcut menu. This allows you to log on to the machine by using a terminal session. On the command line, enter `docker ps` to query the ID of the Troopers container.
6. Run the `sudo docker exec -it container_id bin/bash` command to log on to the container.

The following list describes the structures of specific directories of the container:

- */usr/aliyun/acs/troopers*: the root directory of the application.
  - troopers: the main program of Troopers.
  - troopers.json: the configuration file of Troopers.
  - troopers.ym: the configurations of certificate encryption.
  - start.sh: the entry script used to start Troopers. If the Troopers daemon already exists, do not run the *start.sh* script.
- */opt/aliyun/install/check_health.sh*: the script that is used to run health checks.
- */usr/aliyun/acs/certs/control*: the directory that stores a certificate. Troopers uses the certificate to access the Region Controller (RC). You can use OpenSSL to validate the certificate.

Troopers log files are exported to the stdout stream. No log files are stored in the container. To view log data, run the `docker logs` command outside the container.

9.2.1.3. Mirana

This topic describes the deployment modes and features of Mirana.

Server role

1. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**. In the left-side navigation pane, choose **Product Management > Products**. In the **Apsara Stack O&M** section, click **Apsara Infrastructure Management Framework**.
2. You are redirected to the **Infrastructure Operation Platform** console. In the left-side navigation pane, click **Reports**.
3. On the **Reports** page, click **Go**.
4. You are redirected to the Apsara Infrastructure Management Framework console. In the top navigation bar, choose **Operations > Cluster Operations**. On the Cluster Operations page, find the Container Service cluster that you want to manage. Click **Cluster Configuration** in the Actions column. On the Cluster Configuration page, find the Mirana server role in the Server Role section and check the machine of the server role.

Query log data

In the left-side navigation pane, enter the hostname in the Machine search box. Move the pointer over the More icon next to the hostname and choose Terminal from the shortcut menu. This allows you to log on to the machine by using a terminal session. On the command line, enter `docker ps` to query the ID of the Mirana container. Run the `docker logs contianer_id` command to query the log data.

The Mirana container is stateless. You can trv to restart the container if the service is unavailable. On the command line, enter `docker restart ${container_id}` to restart the container.

Deployment modes

- A Mirana container is deployed in each cluster. The deployment mode of the Mirana container is similar to that of the Commander container.
- Mirana containers are deployed on control machines and use HTTPS to provide services. Mirana requires the Kubernetes API certificate that is provided by Troopers.

Features

- Provides the Kompose tool to convert the Compose file into a YMAL deployment file.
- Allows you to use the Helm client to manage orchestration templates.
- Allows you to call API operations to perform blue-green releases.
- Serves as the proxy for Kubernetes-native API operations.

9.2.2. System restart

9.2.2.1. Restart a control node

A container control node runs a Docker container where Services such as CosConsoleAliyunCom, Troopers, and etcd are deployed. The following procedure demonstrates how to restart a control node:

Procedure

1. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**. In the left-side navigation pane, choose **Product Management > Products**. In the **Apsara Stack O&M** section, click **Apsara Infrastructure Management Framework**.
2. You are redirected to the **Infrastructure Operation Platform** console. In the left-side navigation pane, click **Reports**.
3. On the **Reports** page, click **Go**.
4. You are redirected to the Apsara Infrastructure Management Framework console. In the top navigation bar, choose **Operations > Cluster Operations**. On the Cluster Operations page, find the Container Service cluster that you want to manage. Click **Cluster Configuration** in the Actions column. On the Cluster Configuration page, find the server role of the control node in the Server Role section and find the machine where the control node is deployed.
5. On the command line, enter `docker ps|grep [app]` to query the container ID.

   `[app]` specifies the name of the application that is deployed in the container. You can query the container ID by using the application name.
6. On the command line, enter `docker restart container_id` to restart the container.

9.3. Auto Scaling (ESS)

9.3.1. Log on to the Apsara Uni-manager Operations Console

This topic describes how to log on to the Apsara Uni-manager Operations Console.

Prerequisites

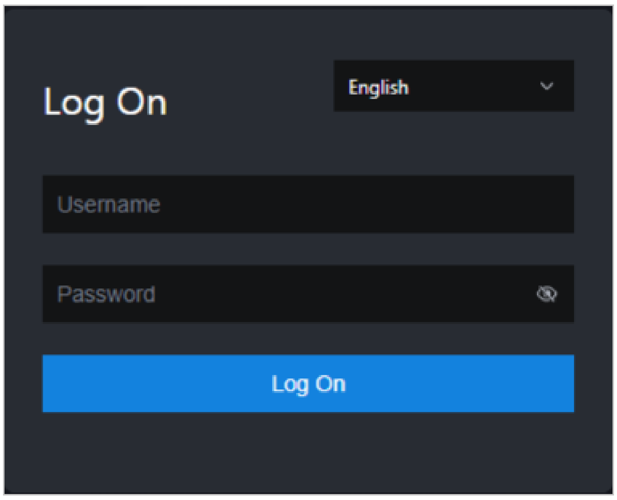
- The URL, username, and password that are required to log on to the Apsara Uni-manager Operations Console are obtained from the deployment personnel or administrators.

  The URL of the Apsara Uni-manager Operations Console is in the format of *region-id*.ops.console.*intranet-domain-id*.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL. Then, press the Enter key.

   Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   Note To obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console, contact the deployment personnel or administrators.

   If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username as prompted.

   To enhance security, make sure that the password meets the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number

signs (#), dollar signs ($), and percent signs (%).

- The password is 10 to 20 characters in length.

4. Click **Log On**.

9.3.2. Product resources and services

9.3.2.1. Application deployment

All applications at the Auto Scaling business logic layer are stateless. You must restart the applications by running the docker restart command.

- ess-init

  ess-init first initializes the database service and then pushes all API configuration files of Auto Scaling to the pop configuration center to initialize OpenAPI.

- Trigger (dependent on ess-init)
  - Trigger executes tasks such as performing checks on the health, minimum number, and maximum number of instances as well as deleting scaling groups.
  - Trigger triggers scheduled tasks and event-triggered tasks.

- coordinator

  Coordinator is the open API layer that provides public-facing services. It maintains persistent requests and issues tasks.

- worker
  - Worker executes all scaling tasks, such as creating ECS instances, adding instances to SLB backend server groups and RDS whitelists, and synchronizing Cloud Monitor group information.
  - It retries failed tasks and provides the rollback mechanism.

- service-test

  service-test is used for regression tests on the overall application running status. It contains more than 60 regression test cases to test the integrity of features.

9.3.2.2. Troubleshooting

This topic describes how to handle issues related to the business logic layer.

Procedure

1. Go to the Alibaba Cloud Support Platform to submit a ticket.
2. Check the status of services that depend on the business logic layer in the Apsara Infrastructure Management Framework console.

   If a service cannot be executed, the Auto Scaling business logic layer is affected. The following table describes the services and their impacts.

   Services and their impacts

Service name	Key impact

Service name	Key impact
middleWare.dubbo	Deployment is affected, and the service is unavailable.
middleWare.tair	Deployment is affected, and the service is unavailable.
middleWare.metaq (message midddleware)	Deployment is affected.
middleWare.zookeeper	Deployment is affected, and the service is unavailable.
middleWare.jmenvDiamondVips	Deployment is affected, and the Diamond configuration item cannot be obtained.
ram.ramService (RAM)	The RAM user is unavailable.
webapp.pop (API Gateway)	The OpenAPI service is unavailable.
ecs.yaochi (ECS Business Foundation System)	All ECS creation requests become invalid.
slb.yaochi (SLB Business Foundation System)	All SLB association requests become invalid.
rds.yaochi (RDS Business Foundation System)	All ApsaraDB RDS association requests become invalid.
tianjimon (Monitoring System)	Some services are unavailable.

9.3.3. Inspection

9.3.3.1. Overview

Auto Scaling inspection monitors the basic health conditions of clusters.

The inspected basic health conditions include the following aspects:

- Monitoring inspection
- Basic software package version inspection

9.3.3.2. Monitoring inspection

The monitoring inspection includes the basic monitoring and connectivity monitoring inspection.

9.3.3.3. Basic software package version inspection

The basic software package version inspection includes the version inspection for trigger, coordinator, worker, and base services.

9.4. Resource Orchestration Service (ROS)

9.4.1. ROS component O&M

9.4.1.1. API Server

The API Server is used to receive ROS requests, send requests to RabbitMQ clusters, and send the responses returned by the Engine Server to callers. The API Server is used to connect the frontend and backend services.

- Components

  The Engine Server and API Server share three servers, all of which are attached to a special Server Load Balancer (SLB) instance.

- O&M methods
  - The storage path of the API Server information is /home/admin/ros-server/bin/.
  - Basic operations of the API Server: `#/usr/local/ros-python/bin/python/home/admin/ros-service/bin/ros-api{stop|status|--daemon}`
    - `stop` : stops the API Server.
    - `status` : queries the status of the API Server.
    - `--daemon` : starts the API Server in daemon mode.
- Health criteria
  - Intrinsic availability: The CPU usage and system memory are within the normal range. The API Server is running normally.
  - Associated component availability: ROS is available.

9.4.1.2. Engine Server

The Engine Server is used to process stack requests. It shares the three servers with the API Server.

- O&M methods
  - The storage path of the API Server information is /home/admin/ros-server/bin/.
  - Basic operation of the Engine Server: `/usr/local/ros-python/bin/python /home/admin/ros-service/bin/ros-engine {stop|status|--daemon}`
    - `stop` : stops the Engine Server.
    - `status` : queries the status of the Engine Server.
    - `--daemon` : starts the Engine Server in daemon mode.
- Health criteria
  - Intrinsic availability: The CPU usage and system memory are within the normal range. The Engine Server is running normally.
  - Associated component availability: ROS is available.

9.4.1.3. RabbitMQ clusters

RabbitMQ clusters are used to receive requests from the API Sever and responses from the Engine Server.

- Components

RabbitMQ clusters are composed of nodes.

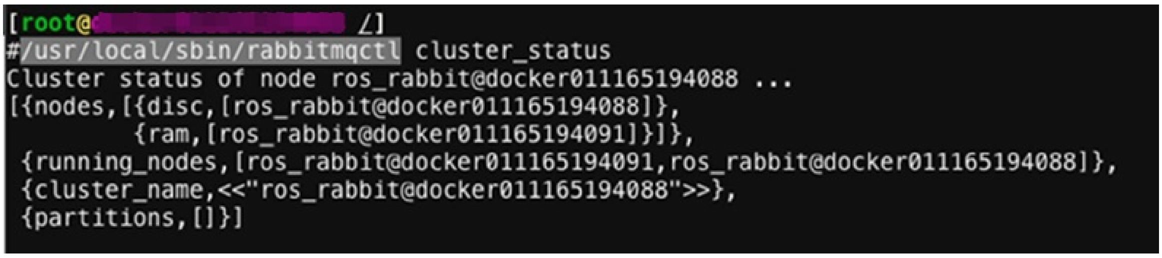
RabbitMQ clusters are used for messaging. Nodes in the clusters use disks for non-persistent storage. Messages are written into the queues that correspond to the nodes. Nodes in a cluster can communicate with each other. Typically, to ensure data accuracy, the minimum number of working nodes is set to [Total number of nodes/2] rounded up. If data of nodes are inconsistent, the secondary nodes synchronize queue messages from the primary nodes.

- O&M methods

  The storage path of the RabbitMQ information is /opt/rabbitmq-server/.

  Common RabbitMQ commands are as follows:

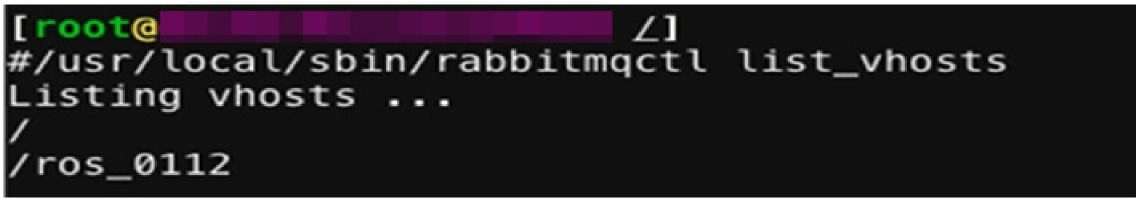
  - You can run the following command to query the cluster status: `sudo /usr/local/sbin/rabbitmq-server/sbin/rabbitmqctl cluster_status`

    ```
    [root@[redacted] ~]
    #/usr/local/sbin/rabbitmqctl cluster_status
    Cluster status of node ros_rabbit@docker011165194088 ...
    [{nodes,[{disc,[ros_rabbit@docker011165194088]},
             {ram,[ros_rabbit@docker011165194091]}]},
     {running_nodes,[ros_rabbit@docker011165194091,ros_rabbit@docker011165194088]},
     {cluster_name,<<"ros_rabbit@docker011165194088">>},
     {partitions,[]}]
    ```

    - `Nodes` : indicates the nodes in the cluster.
    - `Disc` : indicates that the cluster uses disks for storage.
    - `Mem` : indicates that the cluster uses memory for non-persistent storage.
    - `Running_nodes` : indicates the information of the running nodes in the cluster.
    - `Partition` : indicates the partitions of the cluster. If the value field is brackets [], the cluster has no partitions. If this parameter is not empty, the cluster nodes are divided into several partitions.

  - You can run the following command to query the virtual hosts in a cluster: `sudo /usr/local/sbin/rabbitmqctl list_vhosts`

    ```
    [root@[redacted] ~]
    #/usr/local/sbin/rabbitmqctl list_vhosts
    Listing vhosts ...
    /
    /ros_0112
    ```

    Typically, there are two virtual hosts. One is displayed as a forward slash (/), and the other is named based on the region where it resides.

  - Health criteria

    - Intrinsic availability: The CPU usage and system memory are within the normal range. RabbitMQ is running normally, which indicates that clusters have no partitions, queues are properly processed, and messages are properly consumed.
    - Associated component availability: ROS is available.

9.4.1.4. Notify Server

The Notify Server is the proxy server for ECS instances that reside in a VPC. It sends the execution status and information of operations on ECS instances to ROS.

- Components

  The Notify Server consists of three servers, all of which are attached to a special SLB instance.

- O&M methods

  For example, the virtual IP address of the SLB instance is 10.152.XX.XX. You can run curl `http://10.152.XX.XX:80/health-check` to check whether the Notify Server is running.

- Health criteria
  - Intrinsic availability: The CPU usage and system memory are within the normal range.
  - Associated component availability: ROS is available.

9.4.2. Failed to create a scaling group stack

Problem description

When Resource Orchestration Service (ROS) is used to create a scaling group stack, the following error message appears, which indicates that the stack fails to be created.

```
Resource CREATE failed: ResponseException: resources.ScalingGroup: Ess should be authorized in ram to operate user resource. Code: UserNotAuthorize Ess RequestId: F1B3E2B9-B537-49AC-B2DB-D58AD697667A
```

Possible cause

In the template, the maximum number of ECS instances in the scaling group may be equal to the minimum number of ECS instances. MaxSize specifies the maximum number of ECS instances in a scaling group, whereas MinSize specifies the minimum number of ECS instances in a scaling group.

```
{
 "ROSTemplateFormatVersion": "2015-09-01",
 "Resources": {
  "ScalingGroup": {
   "Type": "ALIYUN::ESS::ScalingGroup",
   "Properties": {
    "MaxSize": 1,
    "MinSize": 1,
    "VSwitchId":"vsw-zj8hvzg2qhz4wfrnb****"
   }
  }
 },
 "Outputs": {
  "ScalingGroup": {
     "Value": {"Fn::GetAtt": ["ScalingGroup", "ScalingGroupId"]}
  }
 }
}
```

Solution

Modify the MaxSize value in the template. The MaxSize value must be larger than the MinSize value. For example, you can set the MaxSize value to 10.

Procedure

1. Log on to the ROS console.
2. In the upper-right corner of the page, click **Create Stack**.
3. In the **Select Template** step, set **Organization**, **Resource Set**, and **regionId**.
4. In the **Prepare Template** section, enter template content in the JSON format. Click **Next**.

```
{
 "ROSTemplateFormatVersion": "2015-09-01",
 "Resources": {
  "ScalingGroup": {
   "Type": "ALIYUN::ESS::ScalingGroup",
   "Properties": {
    "MaxSize": 10,
    "MinSize": 1,
    "VSwitchId":"vsw-zj8hvzg2qhz4wfrnb****"
   }
  }
 },
 "Outputs": {
  "ScalingGroup": {
     "Value": {"Fn::GetAtt": ["ScalingGroup", "ScalingGroupId"]}
  }
 }
}
```

5. In the **Configure Template Parameters** step, configure the stack name and parameters, and click **Next**.
6. In the **Configure Stack** step, set Rollback on Failure and Timeout Period, and click **Next**.
7. In the **Confirm** step, check the template and stack configurations, and click **Create Stack**.After the stack is created, the status of the stack is **Created**.
8. If the problem persists after you perform the preceding operations, submit an Apsara Stack ticket.

9.4.3. Failed to create an ECS resource stack

Problem description

When Resource Orchestration Service (ROS) is used to create an ECS resource stack, the `StackValidationFailed` error message appears, which indicates that the stack fails to be created.

Possible cause

The specified password of the ECS instance is invalid.

Solution

Set a new password that complies with the ECS password rules.

Procedure

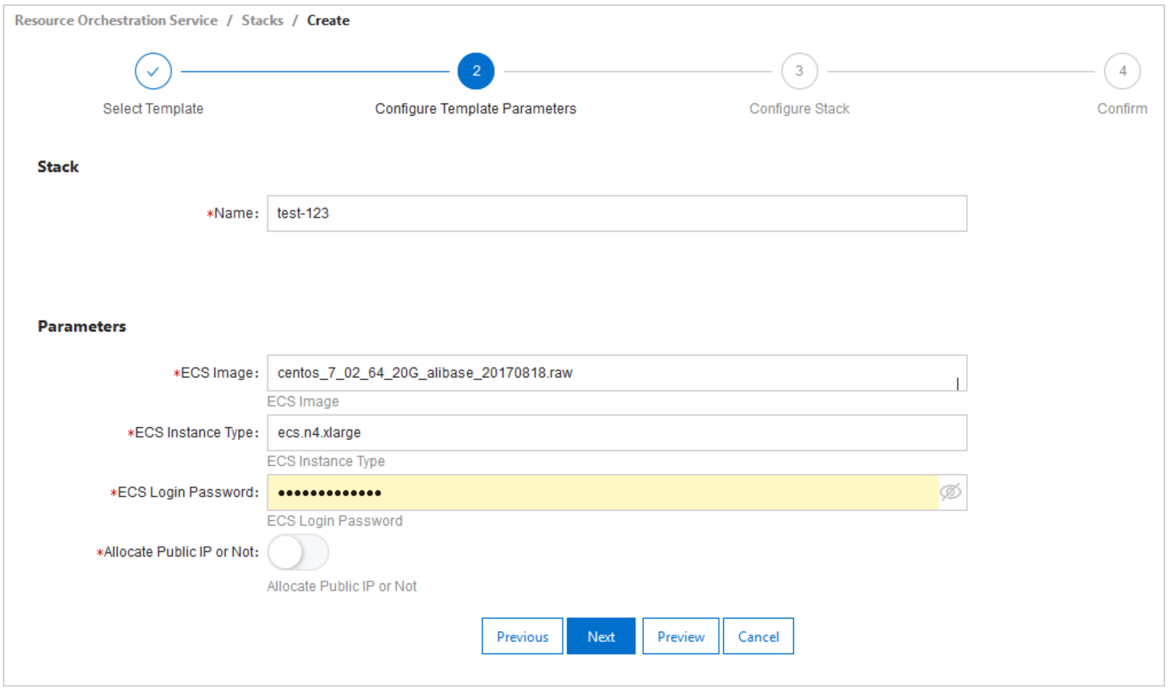
1. Log on to the ROS console.
2. In the upper-right corner of the page, click **Create Stack**.

3. In the **Select Template** step, set **Organization**, **Resource Set**, and **regionId**.
4. In the **Prepare Template** section, enter template content in the JSON format. Click **Next**.

```
{
  "ROSTemplateFormatVersion": "2015-09-01",
  "Description": "Create VPC ECS instance",
  "Parameters": {
    "ImageId": {
      "Type": "String",
      "Description": "ECS Image",
      "Label": "ECS Image",
      "Default": "centos_7_02_64_20G_alibase_20170818.raw"
    },
    "InstanceType": {
      "Type": "String",
      "Description": "ECS Instance Type",
      "Label": "ECS Instance Type",
      "Default": "ecs.n4.xlarge"
    },
    "LoginPassword": {
      "NoEcho": true,
      "Type": "String",
      "Description": "ECS Login Password",
      "AllowedPattern": "(? =^\\S{8,30}$)(? =[^_]*$)(? =[^']*$)(?! ^[\\d\\W_]*$)(?! ^[\\da-z]*$)(?! ^[\\dA-Z]*
$)(?! ^[\\W_a-z]*$)(?! ^[\\W_A-Z]*$)(?! ^[a-zA-Z]*$)\\S*$",
      "Label": "ECS Login Password",
      "MinLength": 8,
      "MaxLength": 30
    },
    "PublicIP": {
      "Type": "Boolean",
      "Description": "Allocate Public IP or Not",
      "Label": "Allocate Public IP or Not",
      "Default": false
    }
  },
  "Resources": {
    "vswitch": {
      "Type": "ALIYUN::ECS::VSwitch",
      "Properties": {
        "VpcId": {
          "Ref": "vpc"
        },
        "ZoneId": {
          "Fn::Select": [
            "0",
            {
              "Fn::GetAZs": {
                "Ref": "ALIYUN::Region"
              }
            }
          ]
        },
        "CidrBlock": "192.168.0.0/16"
      }
    },
    "ecs": {
      "Type": "ALIYUN::ECS::Instance",
      "Properties": {
        "IoOptimized": "optimized",
        "PrivateIpAddress": "192.168.0.1",
        "VpcId": {
          "Ref": "vpc"
        },
        "SecurityGroupId": {
          "Ref": "sg"
        },
        "VSwitchId": {
          "Ref": "vswitch"
        },
        "ImageId": {
          "Ref": "ImageId"
        },
        "AllocatePublicIP": {
          "Ref": "PublicIP"
        },
        "InstanceType": {
          "Ref": "InstanceType"
        },
        "SystemDiskCategory": "cloud_ssd",
        "Password": {
          "Ref": "LoginPassword"
        }
      }
    },
    "sg": {
      "Type": "ALIYUN::ECS::SecurityGroup",
      "Properties": {
        "VpcId": {
          "Ref": "vpc"
        },
        "SecurityGroupName": "mysg",
        "SecurityGroupIngress": [
          {
            "PortRange": "-1/-1",
            "Priority": 1,
            "SourceCidrIp": "0.0.0.0/0",
            "IpProtocol": "all",
            "NicType": "intranet"
          }
        ],
        "SecurityGroupEgress": [
          {
            "PortRange": "-1/-1",
            "Priority": 1,
            "IpProtocol": "all",
            "DestCidrIp": "0.0.0.0/0",
            "NicType": "intranet"
          }
        ]
      }
    },
    "vpc": {
      "Type": "ALIYUN::ECS::VPC",
      "Properties": {
        "CidrBlock": "192.168.0.0/16",
        "VpcName": "myvpc"
      }
    }
  },
  "Outputs": {
    "ecs_instance_id": {
      "Value": {
        "Fn::GetAtt": [
          "ecs",
          "InstanceId"
        ]
      }
    }
  }
}
```

5. In the **Configure Template Parameters** step, configure a new password based on the ECS password rules, and click **Next**.ECS password rules:
   - The password must be 8 to 30 characters in length
   - and must contain at least three of the following character types: uppercase letters, lowercase letters, digits, and special characters. Special characters include

     ```
     :()/.' ~! @#$%^&*-+=|{}[]:;'<>,.? )
     ```

   Resource Orchestration Service / Stacks / Create

   Stack

   *Name: test-123

   Parameters

   *ECS Image: centos_7_02_64_20G_alibase_20170818.raw
   ECS Image

   *ECS Instance Type: ecs.n4.xlarge
   ECS Instance Type

   *ECS Login Password: ••••••••••••••
   ECS Login Password

   *Allocate Public IP or Not: ○
   Allocate Public IP or Not

6. In the **Configure Stack** step, set Rollback on Failure and Timeout Period, and click **Next**.

7. In the **Confirm** step, check the template and stack configurations and stack and click **Create Stack**.After the stack is created, the status of the stack is **Created**.
8. If the problem persists after you perform the preceding operations, submit an Apsara Stack ticket.

9.5. Object Storage Service (OSS)

9.5.1. Log on to the Apsara Uni-manager Operations Console

This topic describes how to log on to the Apsara Uni-manager Operations Console.

Prerequisites

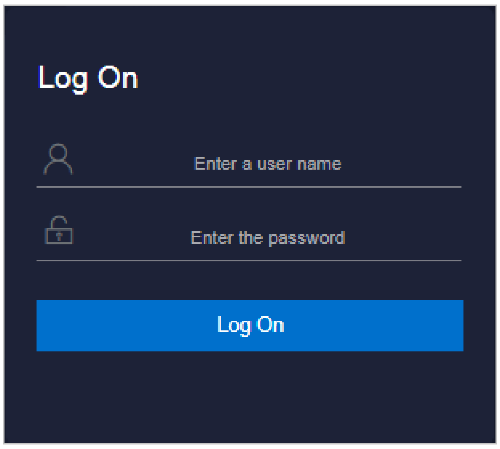
- The URL of the ASO console, and the username and password used for logging on to the console are obtained from the deployment personnel or an administrator.

  The URL of the ASO console is in the following format: *region-id*.aso.*intranet-domain-id*.com.

- A browser is available. We recommend that you use the Google Chrome browser.

Procedure

1. Open your browser.
2. In the address bar, enter the URL *region-id*.aso.*intranet-domain-id*.com and press the Enter key.

   > **Note** You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   > **Note** Obtain the username and password for logging on to the ASO console from the deployment personnel or an administrator.

   When you log on to the ASO console for the first time, you must change the password of your username as prompted.

   To enhance security, a password must meet the following requirements:

- It must contain uppercase and lowercase letters.
- It must contain digits.
- It must contain special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- It must be 10 to 20 characters in length.

4. Click **Log On** to go to the **ASO** console.

9.5.2. OSS operations and maintenance

9.5.2.1. User data

9.5.2.1.1. Basic bucket information

This topic describes how to query the basic information about a bucket, such as the cluster deployment location, configurations, current capacity, and the number of objects stored in the bucket.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > OSS Users**.
4. On the page that appears, select **Bucket Name** from the drop-down list, and then enter the name of the bucket that you want to query.
5. Click **View** to view the basic information about the bucket.You can also click the **Data Monitoring** tab to view the SLA, traffic, and QPS of the bucket.

9.5.2.1.2. User data overview

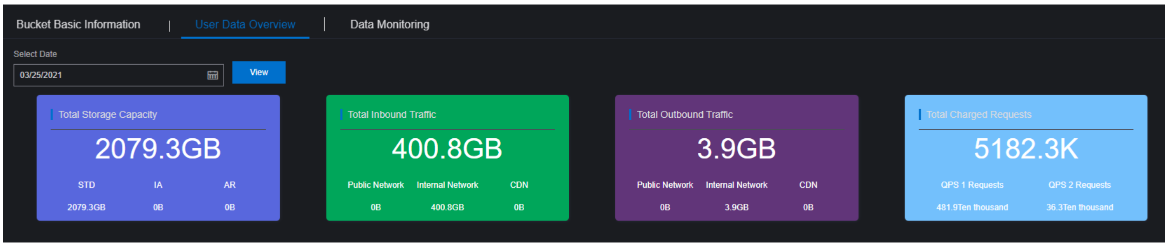
OSS allows you to view the statistical data of a user, such as the resource usage and the attributes of resources. You can measure the total resource usage of all buckets owned by a user on a specified day.

Context

The overview of user data is displayed only when you search the data by using UIDs or Alibaba Cloud accounts. You can view the following user data: total storage capacity, total inbound and outbound traffics (including traffics transferred over public networks, internal networks, and CDN), and total charged requests.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > OSS Users**.
4. On the page that appears, select **Alibaba Cloud Account** or **UID** from the drop-down list, and then enter the Alibaba Cloud account or UID whose data you want to view.
5. Click **View**. Then, click the **User Data Overview** tab.You can select a date and then click **View** to view the user data on a specified day.



Select Date: 03/25/2021

Total Storage Capacity: 2079.3GB
STD: 2079.3GB | IA: 0B | AR: 0B

Total Inbound Traffic: 400.8GB
Public Network: 0B | Internal Network: 400.8GB | CDN: 0B

Total Outbound Traffic: 3.9GB
Public Network: 0B | Internal Network: 3.9GB | CDN: 0B

Total Charged Requests: 5182.3K
QPS 1 Requests: 481.9Ten thousand | QPS 2 Requests: 36.3Ten thousand

9.5.2.1.3. Data monitoring

This topic describes how to monitor the data of OSS in the Apsara Uni-manager Operations Console.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > OSS Users**.
4. On the page that appears, select **Alibaba Cloud Account** or **UID** from the drop-down list, and then enter the Alibaba Cloud account or UID whose data you want to monitor. Then, click **View**.
5. Click the **Data Monitoring** tab and configure the parameters described in the following table.

Parameter	Description
Bucket Name	Select the bucket you want to monitor from the drop-down list.
Specify Time Range	Select the time range that you want to monitor.
Monitoring Items	Select one or more of the following items that you want to monitor. ○ **SLA**: The service level agreement provided by OSS. The SLA of OSS can be calculated based on the following formula: `Number of non-5XX requests per 10 seconds or an hour/Number of valid requests x 100%` . ○ **HTTP Status**: The number of the returned 5XX, 403, 404, 499, 4XX_other, 2XX, and 3XX status codes and the percentage of the requests to which these codes are returned. ○ **Latency**: The latencies of API requests and the maximum value of the latencies. ○ **Storage Capacity**: The storage capacity of the bucket. ○ **Image Processing Capacity**: The number of images processed by using OSS. ○ **Traffic**: The traffic generated by the bucket. ○ **QPS**: The number of API requests sent to the bucket.

6. Click **View**.

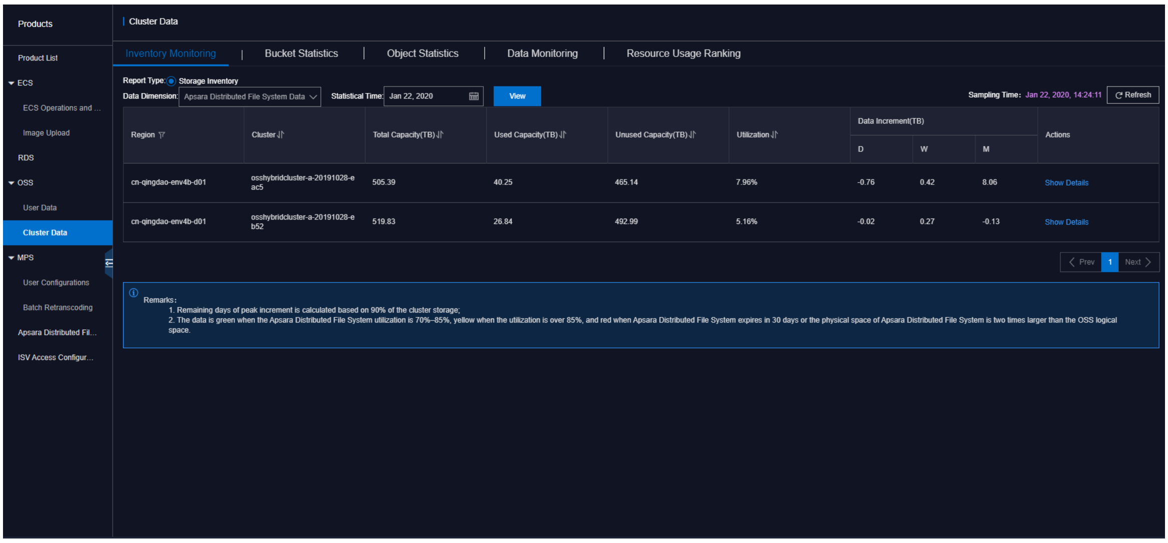
9.5.2.2. Cluster data

9.5.2.2.1. Inventory monitoring

You can monitor the following metrics: total capacity, unused capacity, used capacity, and storage utilization.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > OSS Clusters**.
4. Click the **Inventory Monitoring** tab. You can select the data that you want to monitor from the Data Dimension drop-down list.



Report Type: ● Storage Inventory
Data Dimension: Apsara Distributed File System Data
Statistical Time: Jan 22, 2020
Sampling Time: Jan 22, 2020, 14:24:11

Region	Cluster	Total Capacity(TB)	Used Capacity(TB)	Unused Capacity(TB)	Utilization	Data Increment(TB)			Actions
						D	W	M	
cn-qingdao-env4b-d01	osshybridcluster-a-20191028-eac5	505.39	40.25	465.14	7.96%	-0.76	0.42	8.06	Show Details
cn-qingdao-env4b-d01	osshybridcluster-a-20191028-eb52	519.83	26.84	492.99	5.16%	-0.02	0.27	-0.13	Show Details

Remarks:
1. Remaining days of peak increment is calculated based on 90% of the cluster storage;
2. The data is green when the Apsara Distributed File System utilization is 70%–85%, yellow when the utilization is over 85%, and red when Apsara Distributed File System expires in 30 days or the physical space of Apsara Distributed File System is two times larger than the OSS logical space.

You can select to view the following data:

- Apsara Distributed File System Data: includes the total capacity, used capacity, unused capacity, utilization, and data increment of the cluster.
- Metric Data: includes the statistical capacity that shares and does not share ECS quota.
- KV Data: includes the logic KV data, KV data in the recycle bin, and data increment (by day, week, or month).

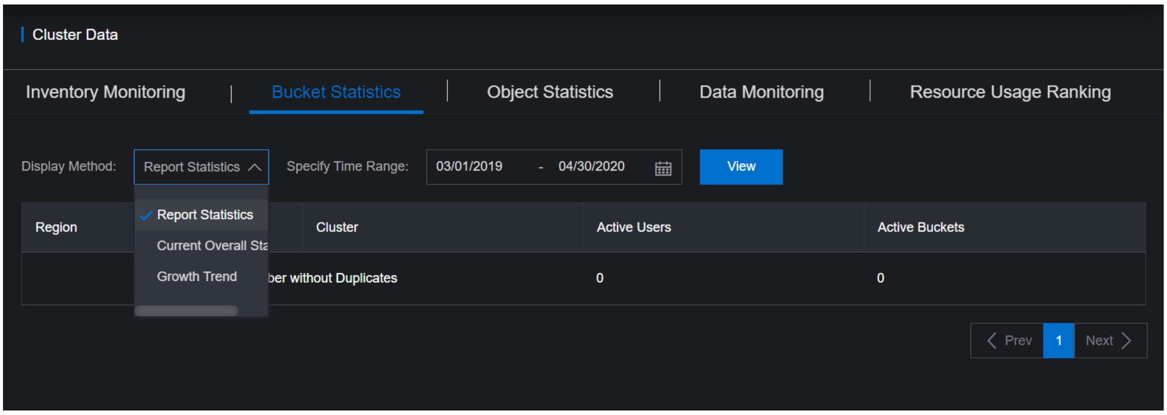
9.5.2.2.2. Bucket statistics

This topic describes how to measure the number of buckets created in each cluster.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > OSS Clusters**.

4. Click the **Bucket Statistics** tab. You can select **Report Statistics**, **Current Overall Statistics**, or **Growth Trend** from the Display Method drop-down list to view the statistics in different methods.



Display Method: Report Statistics

Specify Time Range: 03/01/2019 - 04/30/2020

Region	Cluster	Active Users	Active Buckets
	ber without Duplicates	0	0

- If you select **Report Statistics**, specify a time range.
- If you select **Current Overall Statistics**, by default, the statistics that you query is generated based on the data in the last hour.
- If you select **Growth Trend**, you can select the following values from the Recent drop-down list to view the statistics within a specific range: *7 Days*, *30 Days*, *3 Months*, *6 Months*, and *1 Year*.

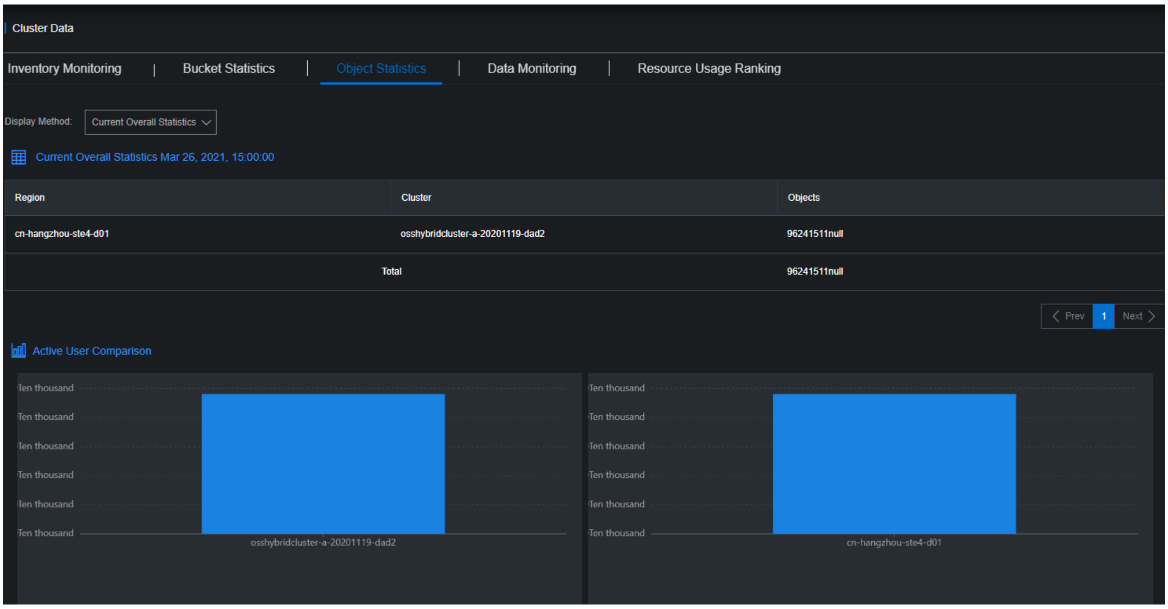
5. Click **View**.

9.5.2.2.3. Object statistics

This topic describes how to measure the number of objects stored in each cluster and the trend of the number.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > OSS Clusters**.
4. Click the **Object Statistics** tab. You can select **Current Overall Statistics** or **Growth Trend** from the Display Method drop-down list to view the statistics in different methods.



Display Method: Current Overall Statistics

Current Overall Statistics Mar 26, 2021, 15:00:00

Region	Cluster	Objects
cn-hangzhou-ste4-d01	osshybridcluster-a-20201119-dad2	96241511null
Total		96241511null

- If you select **Current Overall Statistics**, by default, the statistics that you query is generated based on the data in the last hour.
- If you select **Growth Trend**, you can select the following values from the Recent drop-down list to view the statistics within a specific range: *7 Days*, *30 Days*, *3 Months*, *6 Months*, and *1 Year*.

5. Click **View**.

9.5.2.2.4. Data monitoring

This topic describes how to view the metrics used to monitor data.

Context

Metrics used to monitor cluster data are the same as those used to monitor user data except that the monitored data are collected by cluster.

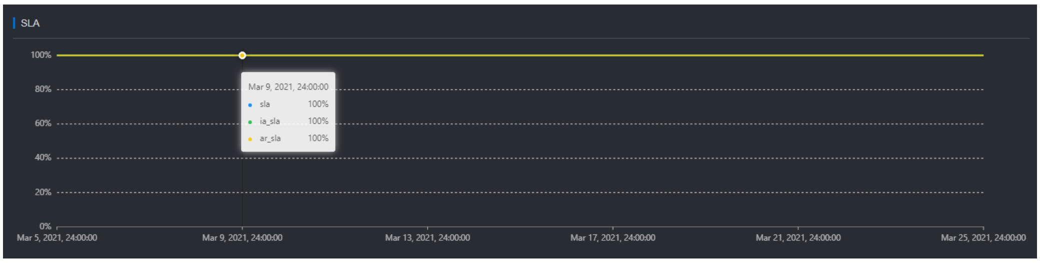
Procedure

1. Log on to the Apsara Stack Operations console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management** > **OSS Clusters**.
4. Click the **Data Monitoring** tab, select the metrics from the **Monitoring Items** drop-down list and set a time range in the **Specify Time Range** field. Then, click **View**.

> **Note** You can select to view the following monitoring metrics:
>
> - SLA: The service level agreement provided by OSS. The SLA of OSS can be calculated based on the following formula: Number of non-5XX requests per 10 seconds or an hour/Number of valid requests x 100%.
> - Traffic: The traffic generated by the bucket, including the inbound and outbound traffics transferred over public networks, internal networks, and CDN and the inbound and outbound traffic for synchronization.
> - QPS: The number of the following charged requests sent to the bucket: CopyObject, GetObject, PutObject, UploadPart, PostObject, AppendObject, HeadObject, and GetObjectInfo.
> - Latency: The latencies of API requests such as PutObject, GetObject, and UploadPart and the maximum value of the latencies.
> - HTTP Status: The number of the returned 5XX, 403, 404, 499, 4XX_other, 2XX, and 3XX status codes and the percentage of the requests to which these codes are returned.
> - Storage Capacity: The storage capacity of the bucket, including the capacity and increment of the Standard, IA, and Archive storage.

5. Move the pointer over the trend chart to display data at a specific point in time.

Data monitoring 1



You can view the following monitoring metrics in the chart:

- SLA: The service level agreement provided by OSS. The SLA of OSS can be calculated based on the following formula: Number of non-5XX requests per 10 seconds or an hour/Number of valid requests x 100%.
- HTTP Status: The number of the returned 5XX, 403, 404, 499, 4XX_other, 2XX, and 3XX status codes and the percentage of the requests to which these codes are returned.
- Latency: The latencies of API requests such as PutObject, GetObject, and UploadPart and the maximum value of the latencies.
- Storage Capacity: The storage capacity of the bucket, including the capacity and increment of the Standard, IA, and Archive storage.
- Image Processing Capacity: The number of images processed by using OSS.

  > **Note** By default, this metric is not displayed. You can select this metric from the **Monitoring Items** drop-down list.

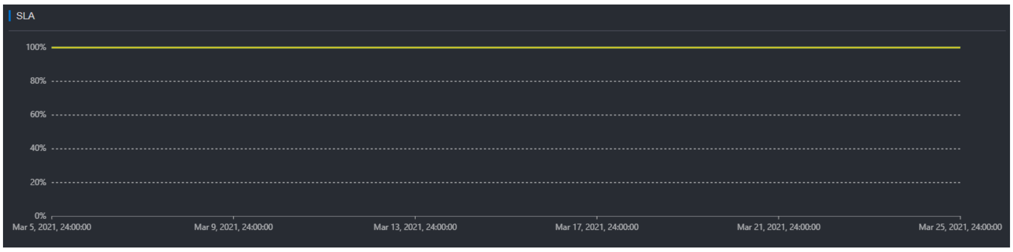
- Traffic: The traffic generated by the bucket, including the inbound and outbound traffics transferred over public networks, internal networks, and CDN and the inbound and outbound traffic for synchronization.

- QPS: The number of the following charged requests sent to the bucket: CopyObject, GetObject, PutObject, UploadPart, PostObject, AppendObject, HeadObject, and GetObjectInfo.

The following examples show the common operations that you can perform on the data monitoring trend chart:

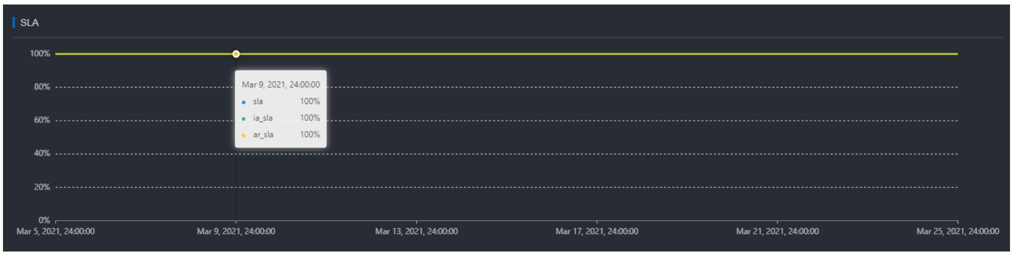
- If you want to query the monitored data by user, you can click the bucket name in the trend chart to show or hide the curve.

Data monitoring 2



- Move the pointer over the trend chart to display data at a specific point in time.

Data monitoring 3



9.5.2.2.5. Resource usage rankings

This topic describes how to measure the usage of resources by cluster. This way, administrators can monitor users that consume more resources.

Context

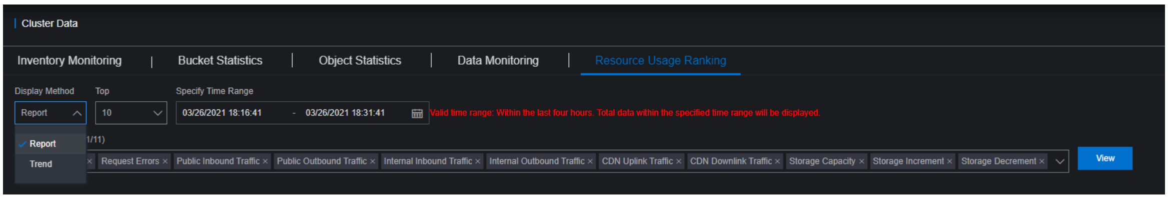
Data resources can be ranked based on the following metrics:

- Total Requests
- Request Errors
- Public Inbound Traffic and Public Outbound Traffic
- Internal Inbound Traffic and Internal Outbound Traffic
- CDN Uplink Traffic and CDN Downlink Traffic
- Storage Capacity, Storage Increment, and Storage Decrement

Procedure

1. Log on to the Apsara Stack Operations console.
2. In the top navigation bar, click **O&M**.
3. In the left-side navigation pane, choose **Product Management > OSS Clusters**.
4. Click the **Resource Usage Ranking** tab and then select **Report** or **Trend** from the Display Method drop-down list. Select a number from the **Top** drop-down list. Select the metrics from the

Monitoring Items drop-down list and set a time range in the **Specify Time Range** field to view resource usage.



Cluster Data

Inventory Monitoring | Bucket Statistics | Object Statistics | Data Monitoring | Resource Usage Ranking

Display Method: Report (✓ Report, Trend)

Top: 10

Specify Time Range: 03/26/2021 18:16:41 - 03/26/2021 18:31:41

Valid time range: Within the last four hours. Total data within the specified time range will be displayed.

(1/11)

Request Errors × Public Inbound Traffic × Public Outbound Traffic × Internal Inbound Traffic × Internal Outbound Traffic × CDN Uplink Traffic × CDN Downlink Traffic × Storage Capacity × Storage Increment × Storage Decrement ×

- If you select the **Report** method, you can view the resource usage of the top **10**, **30**, or **50** buckets in reports.
- If you select the **Trend** method, you can view the resource usage of the top **10** buckets in trend charts.

5. Click **View**.

9.5.3. Tools and commands

9.5.3.1. Typical commands supported by tsar

You can use tsar to perform operations and maintenance on OSS. This topic describes typical commands supported by tsar.

tsar allows you to run the following commands:

- View help details of tsar

  Command: **tsar -help**

- View the NGINX operation data of each minute from the past two days

  Command: **tsar -n 2 -i 1 -nginx**

  In this command, *-n 2* indicates the data generated in the past two days. *-i 1* indicates one result record generated each minute.

- View the tsar load status and operation data of each minute from the past two days

  Command: **tsar --load -n 2 -i 1**

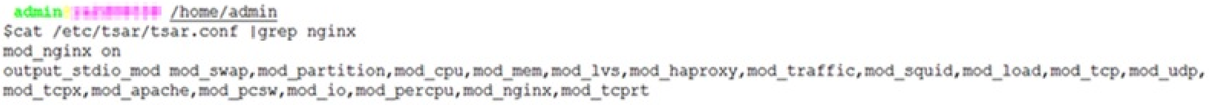
9.5.3.2. Configure tsar for statistic collection

You can configure tsar to collect data generated when NGINX runs.

Run the following command to configure tsar for statistic collection:

```
cat /etc/tsar/tsar.conf |grep nginx
```

Ensure themod_nginx item is in the *on* state. The following figure shows that the status of mod_nginx is *on*.



```
 admin [redacted] /home/admin
$cat /etc/tsar/tsar.conf |grep nginx
mod_nginx on
output_stdio_mod mod_swap,mod_partition,mod_cpu,mod_mem,mod_lvs,mod_haproxy,mod_traffic,mod_squid,mod_load,mod_tcp,mod_udp,
mod_tcpx,mod_apache,mod_pcsw,mod_io,mod_percpu,mod_nginx,mod_tcprt
```

9.6. Tablestore

9.6.1. Tablestore Operations and Maintenance System

9.6.1.1. Overview

This document describes the features, domain name, and modules of Tablestore Operations and Maintenance System.

Tablestore Operations and Maintenance System helps find problems during operations and maintenance (O&M) and notifies you of the current running status of the services. Appropriate use of Tablestore Operations and Maintenance System can significantly improve O&M efficiency.

The domain name of Tablestore Operations and Maintenance System is in the following format: chiji.ots.${global:intranet-domain}.

Tablestore Operations and Maintenance System consists of the following modules: user data, cluster management, inspection center, monitoring center, system management, and platform audit. These modules provide comprehensive O&M functions to meet different requirements.

9.6.1.2. User data

9.6.1.2.1. Instance management

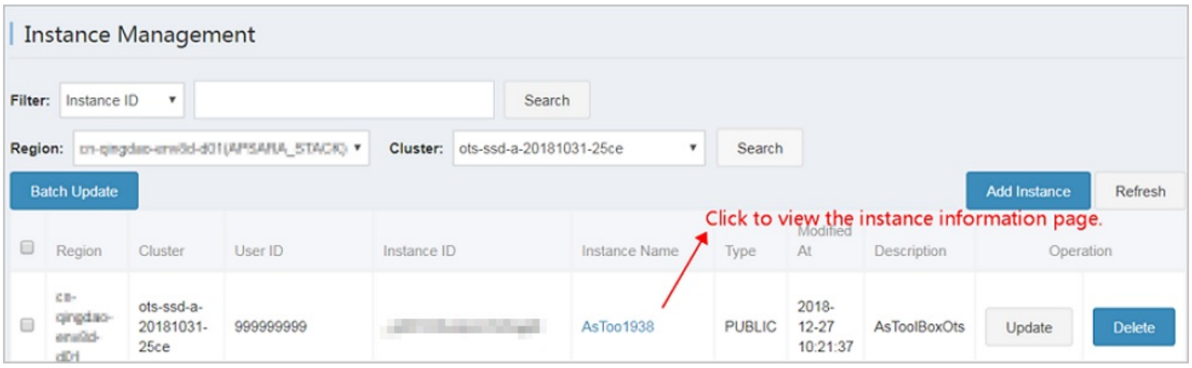
You can query an instance list by specifying the region, and cluster name. You can also query an instance by specifying the filter conditions and view details of the instance and tables.

Instance management provides the following features:

- Query an instance list by specifying the region, and cluster name.

  You can specify a region, and a cluster to view the instances, and the basic information of each instance in the specified cluster.

  - Query the list of instances in a cluster.
  - View basic information of instances in the instance list.
  - View details of an instance by clicking the instance name.
  - Update and delete an instance in the instance list.



Instance Management

Filter: Instance ID ▾ Search

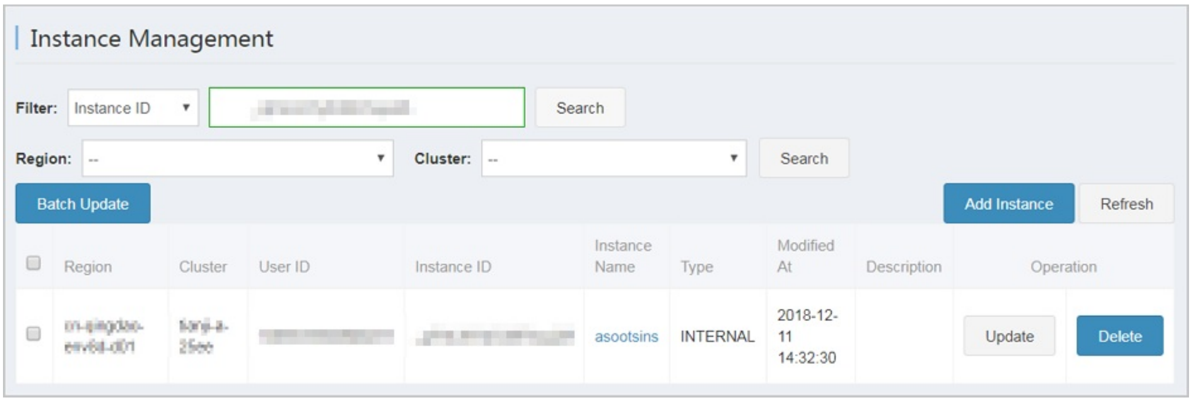
Region: [redacted] ▾ Cluster: ots-ssd-a-20181031-25ce ▾ Search

Click to view the instance information page.

□	Region	Cluster	User ID	Instance ID	Instance Name	Type	Modified At	Description	Operation	
□	[redacted]	ots-ssd-a-20181031-25ce	999999999	[redacted]	AsToo1938	PUBLIC	2018-12-27 10:21:37	AsToolBoxOts	Update	Delete

- Search for instances based on specified conditions

  You can search for an instance based on the instance name, instance ID, user ID or Apsara Stack tenant account in all clusters of all regions.



Instance Management

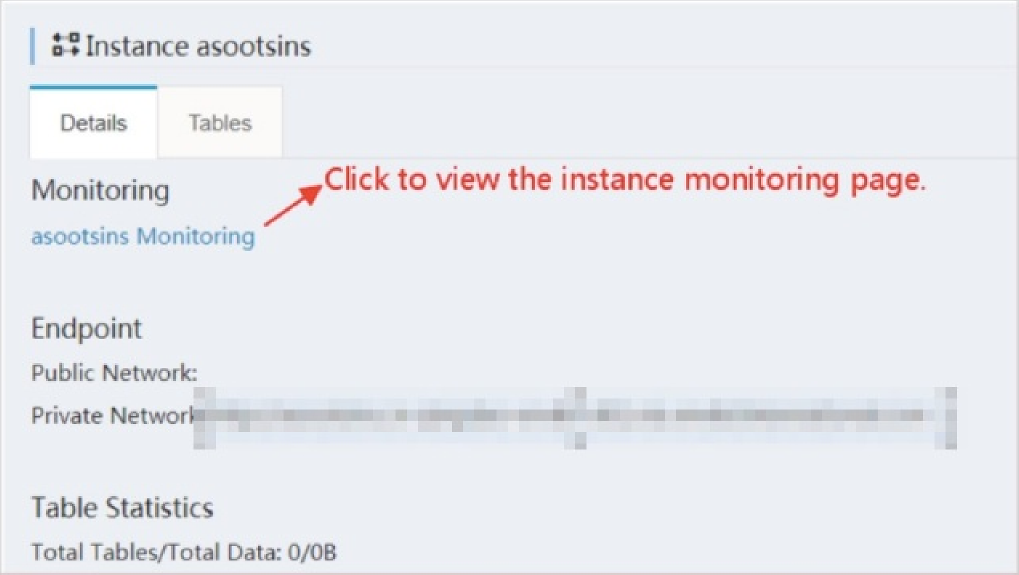
Filter: Instance ID [redacted] Search

Region: -- Cluster: -- Search

□	Region	Cluster	User ID	Instance ID	Instance Name	Type	Modified At	Description	Operation
□	[redacted]	[redacted]	[redacted]	[redacted]	asootsins	INTERNAL	2018-12-11 14:32:30		Update Delete

- View instance details
    - Instance overview

      Click the instance name. On the **Details** tab, you can view instance details such as the link for instance monitoring, the IP address of the instance for the Internet and internal network, and the statistics information of tables in the instance.



Instance asootsins

Monitoring

asootsins Monitoring

Click to view the instance monitoring page.

Endpoint

Public Network:

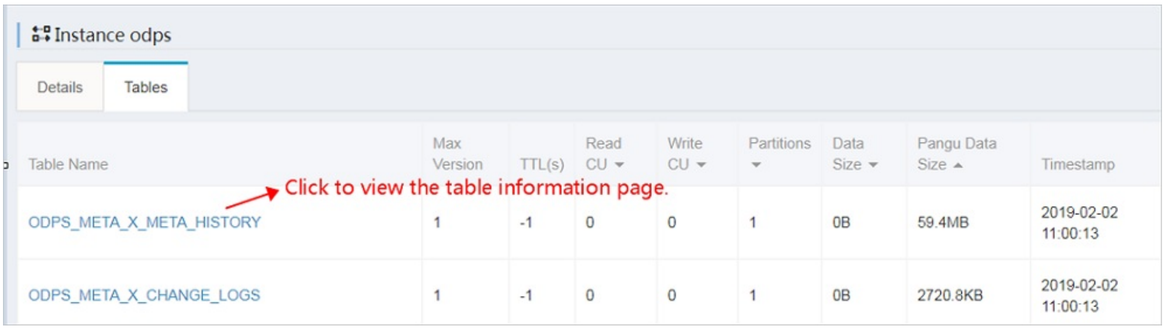
Private Network: [redacted]

Table Statistics

Total Tables/Total Data: 0/0B

- Tables information

  Click the instance name. On the **Tables** tab, you can view the maxVersion, ttl, readCU, writeCU, and timestamp of tables.



Instance odps

Click to view the table information page.

Table Name	Max Version	TTL(s)	Read CU	Write CU	Partitions	Data Size	Pangu Data Size	Timestamp
ODPS_META_X_META_HISTORY	1	-1	0	0	1	0B	59.4MB	2019-02-02 11:00:13
ODPS_META_X_CHANGE_LOGS	1	-1	0	0	1	0B	2720.8KB	2019-02-02 11:00:13

- View table details

- Details

  Click the table name. On the **Details** tab, you can view the overview information of the table, such as the number of partitions and the table size.

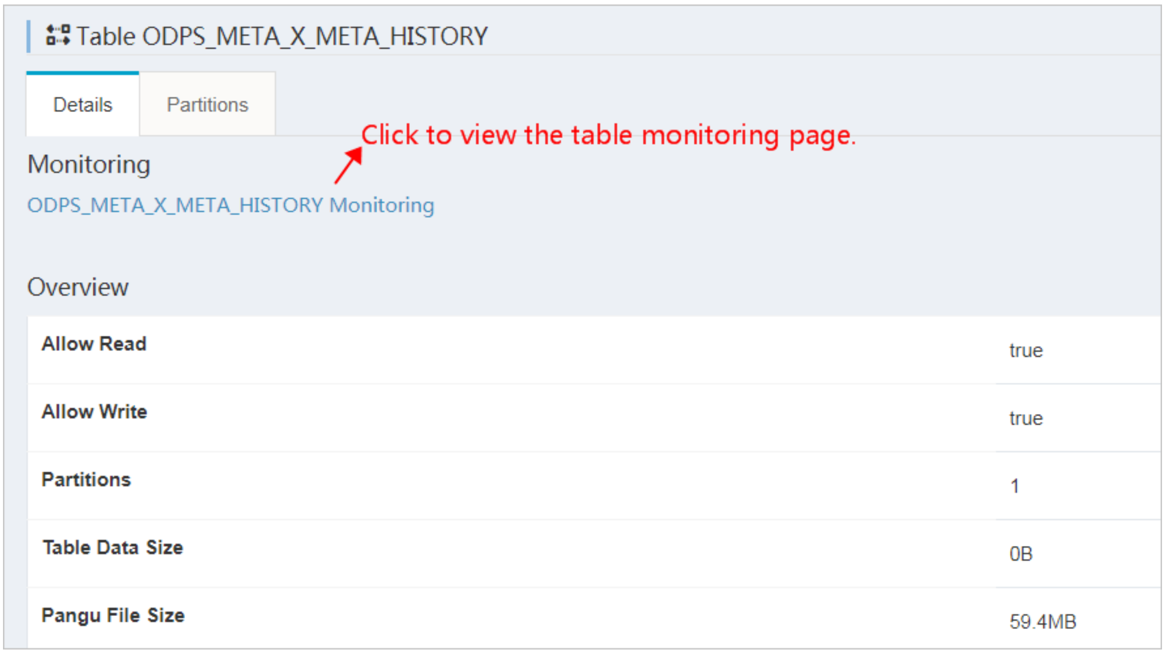


Table ODPS_META_X_META_HISTORY

Monitoring

ODPS_META_X_META_HISTORY Monitoring

Overview

Allow Read	true
Allow Write	true
Partitions	1
Table Data Size	0B
Pangu File Size	59.4MB

- Partitions

  Click the table name. On the **Partitions** tab, you can obtain the basic information of an partition, such as the partition ID and Worker information. You can also search for partitions based on the Worker name that is listed in the table or the partition ID.

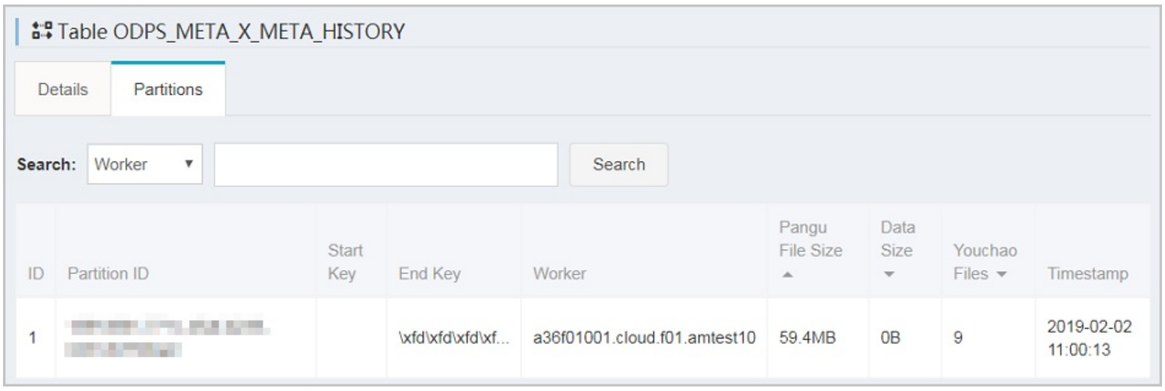


Table ODPS_META_X_META_HISTORY

ID	Partition ID	Start Key	End Key	Worker	Pangu File Size	Data Size	Youchao Files	Timestamp
1	[redacted]		\xfd\xfd\xfd\xf...	a36f01001.cloud.f01.amtest10	59.4MB	0B	9	2019-02-02 11:00:13

9.6.1.3. Cluster management

9.6.1.3.1. Cluster information

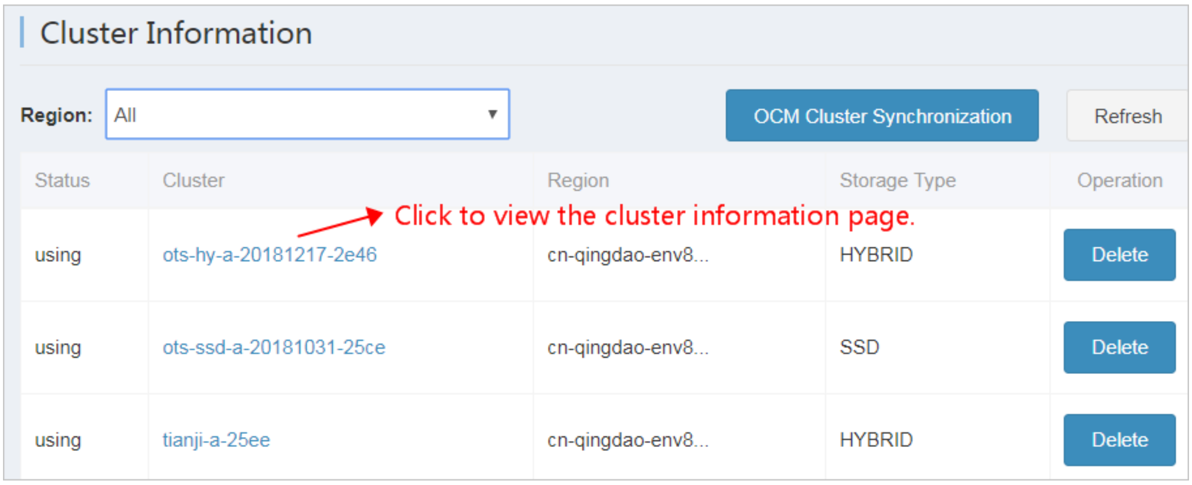
You can obtain the list of clusters, view cluster usage and top requests based on cluster information.

You can perform the following operations based on the cluster information:

- Clusters

  You can query a list of clusters in all regions or in a specified region. Perform the following operations:

- OCM cluster synchronization: An OCM service is deployed in each region of Tablestore. The OCM service contains all cluster information of a region. This function synchronizes OCM clusters with their corresponding regions in Tablestore Operations and Maintenance System to obtain all clusters in the regions.
- Cluster deletion: You can use this function to remove a cluster from Tablestore Operations and Maintenance System after you confirm that the cluster is taken offline.



Cluster Information

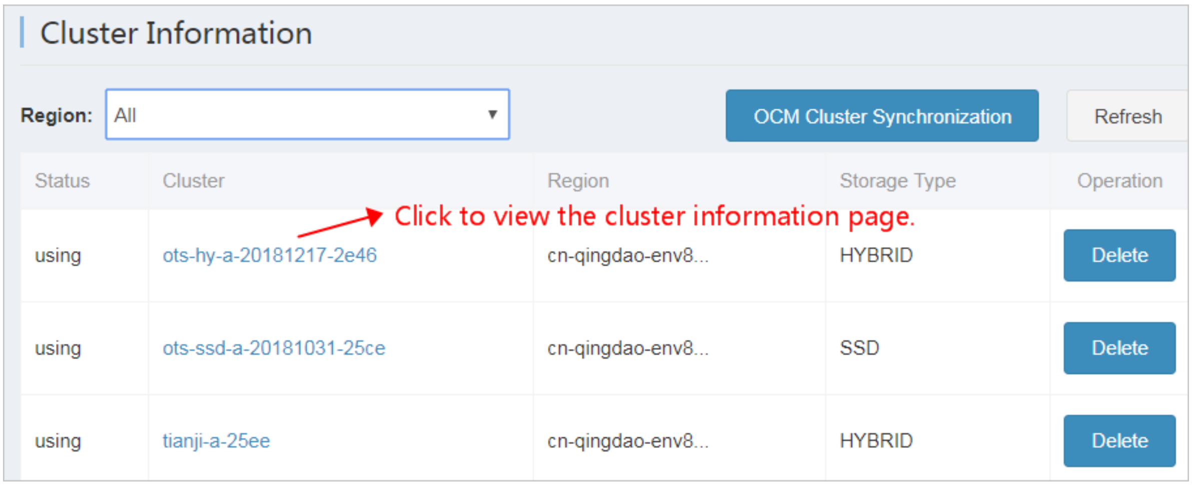
Region: All

Status	Cluster	Region	Storage Type	Operation
using	ots-hy-a-20181217-2e46	cn-qingdao-env8...	HYBRID	Delete
using	ots-ssd-a-20181031-25ce	cn-qingdao-env8...	SSD	Delete
using	tianji-a-25ee	cn-qingdao-env8...	HYBRID	Delete

Click to view the cluster information page.

- Cluster details

  Click a cluster name in the Cluster column to go to the cluster details page. You can view the detail information of the cluster, including the overview, top request, and cluster usage.



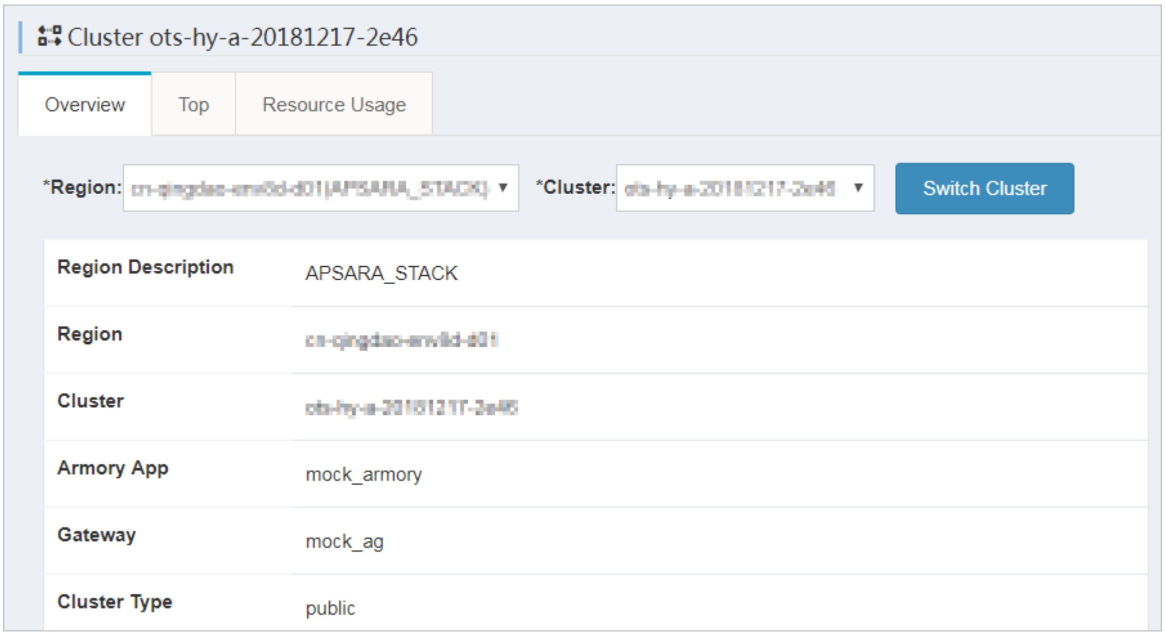
Cluster Information

Region: All

Status	Cluster	Region	Storage Type	Operation
using	ots-hy-a-20181217-2e46	cn-qingdao-env8...	HYBRID	Delete
using	ots-ssd-a-20181031-25ce	cn-qingdao-env8...	SSD	Delete
using	tianji-a-25ee	cn-qingdao-env8...	HYBRID	Delete

Click to view the cluster information page.

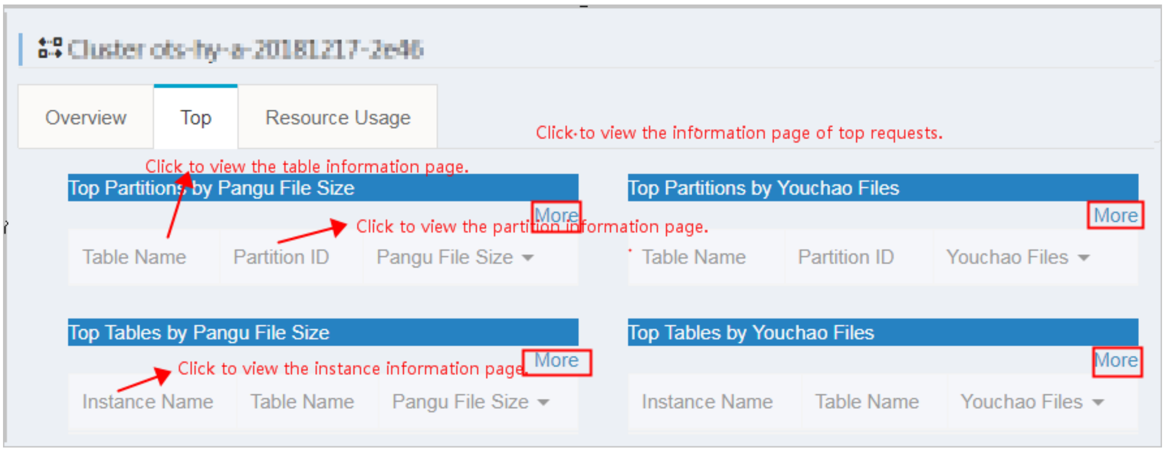
- Overview: provides the basic information of a cluster.



Region Description	APSARA_STACK
Region	[redacted]
Cluster	[redacted]
Armory App	mock_armory
Gateway	mock_ag
Cluster Type	public

- Top: provides top request information of partitions and tables.

  Click an instance name in the InstanceName column to go to the instance details page, where you can view detailed information of the instance. Click a table name in the TabelName column to go to the table details page, where you can view detail information of the table. Click a partition ID in the PartitionID column to go to the partition details page, where you can view detail information of the partition. Click **More** and you can view detail information of the top request.



Click to view the information page of top requests.

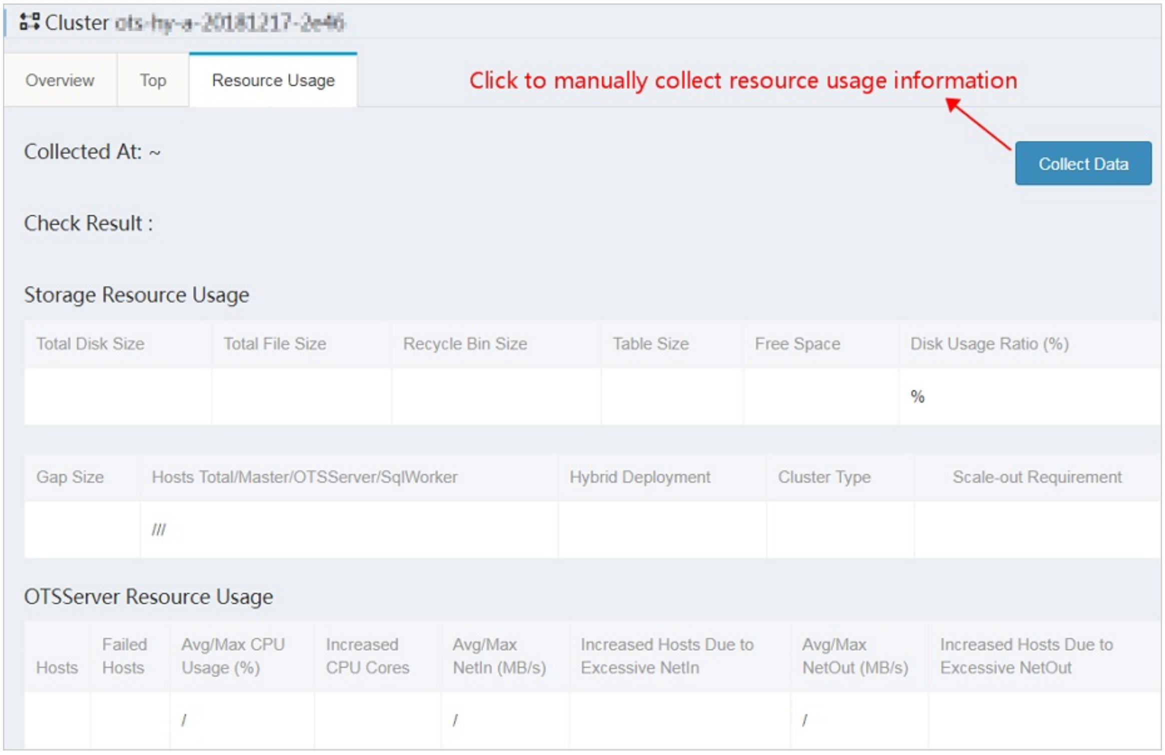
Click to view the table information page.

Click to view the partition information page.

Click to view the instance information page

- Resource Usage: provides cluster usage details. The usage statistics collection task is automatically triggered in the background at specific intervals. In special cases, you can click **Collect Data** to manually trigger the usage statistics collection task. After the usage statistics collection task is completed, refresh the page to display the latest usage statistics.

  > **Note** The usage check either succeeds or fails. In addition, you must pay special attention to the cause of a usage check failure. (The usage check failure is caused by the failure to obtain storage space, as shown in the following figure.)



Click to manually collect resource usage information

Collected At: ~

Check Result :

Storage Resource Usage

Total Disk Size	Total File Size	Recycle Bin Size	Table Size	Free Space	Disk Usage Ratio (%)
					%

Gap Size	Hosts Total/Master/OTSServer/SqlWorker	Hybrid Deployment	Cluster Type	Scale-out Requirement
	///			

OTSServer Resource Usage

Hosts	Failed Hosts	Avg/Max CPU Usage (%)	Increased CPU Cores	Avg/Max NetIn (MB/s)	Increased Hosts Due to Excessive NetIn	Avg/Max NetOut (MB/s)	Increased Hosts Due to Excessive NetOut
		/		/		/	

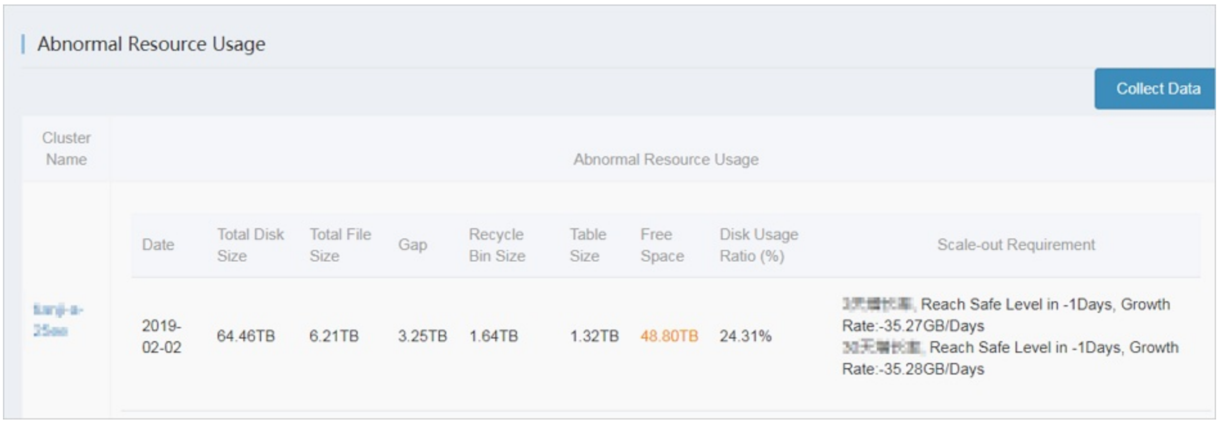
9.6.1.4. Inspection center

9.6.1.4.1. Abnormal resource usage

You can click Abnormal Resource Usage in the left-side navigation pane to find all cluster abnormalities and their causes.

You can click Abnormal Resource Usage in the left-side navigation pane to inspect cluster abnormalities in all regions. Abnormalities are displayed in red, which allows you to find abnormal clusters.

The usage statistics collection task is automatically triggered in the background at specific intervals. In special cases such as a failure in background task execution, you can click **Collect Data** to manually trigger usage statistics collection. The collection action is performed asynchronously. After the usage statistics collection task is completed, refresh the page to display the latest usage statistics.



Abnormal Resource Usage

Collect Data

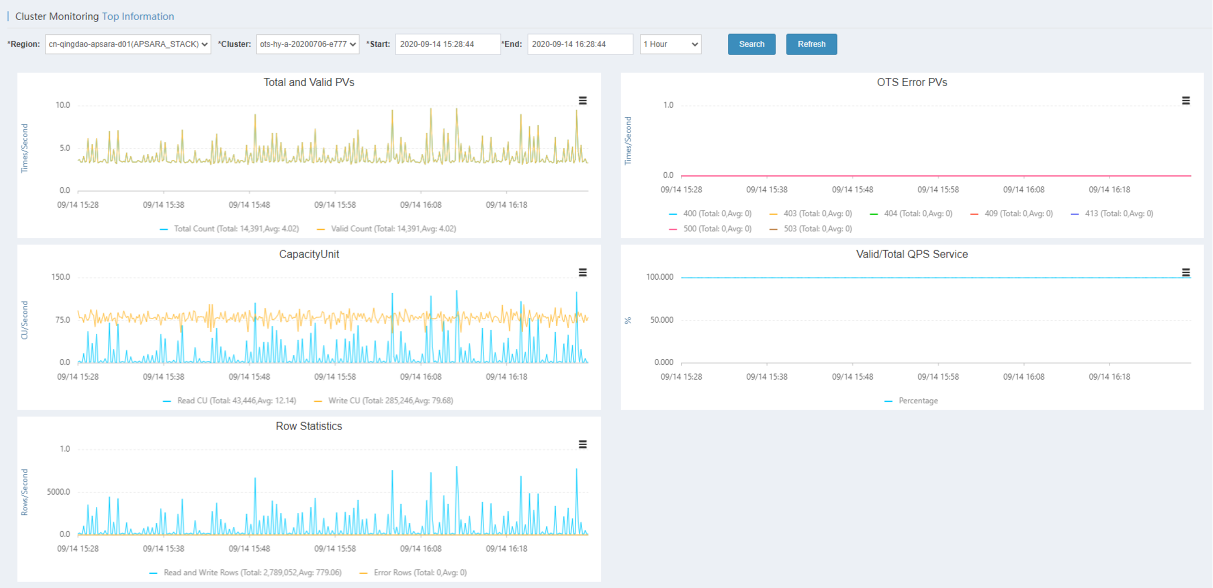
Cluster Name	Abnormal Resource Usage								
	Date	Total Disk Size	Total File Size	Gap	Recycle Bin Size	Table Size	Free Space	Disk Usage Ratio (%)	Scale-out Requirement
[redacted]	2019-02-02	64.46TB	6.21TB	3.25TB	1.64TB	1.32TB	48.80TB	24.31%	[redacted], Reach Safe Level in -1Days, Growth Rate:-35.27GB/Days [redacted], Reach Safe Level in -1Days, Growth Rate:-35.28GB/Days

9.6.1.5. Monitoring center

9.6.1.5.1. Cluster monitoring

You can determine the service status of a cluster based on a series of metrics such as cluster-level monitoring information.

You can query the cluster service metrics within a specified time range, and determine whether a cluster service is healthy based on the metrics in the following dimensions.



Cluster Monitoring Top Information

*Region: cn-qingdao-apsara-d01(APSARA_STACK) *Cluster: ots-hy-a-20200706-e777 *Start: 2020-09-14 15:28:44 *End: 2020-09-14 16:28:44 1 Hour

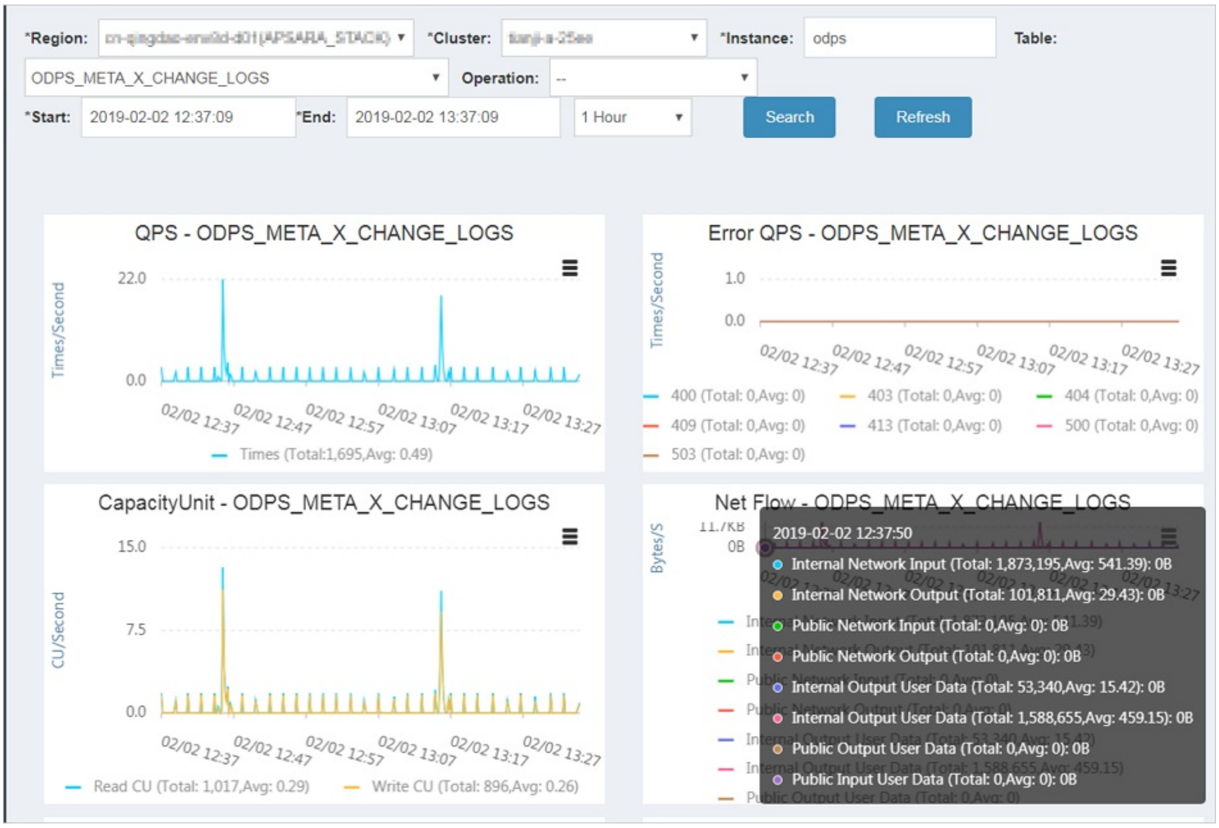
Search Refresh

9.6.1.5.2. Application monitoring

You can check the instance-level and table-level metrics to determine whether a service that belongs to a user is abnormal.

You can check the following metrics to determine whether a service for a specified user is in the healthy state.

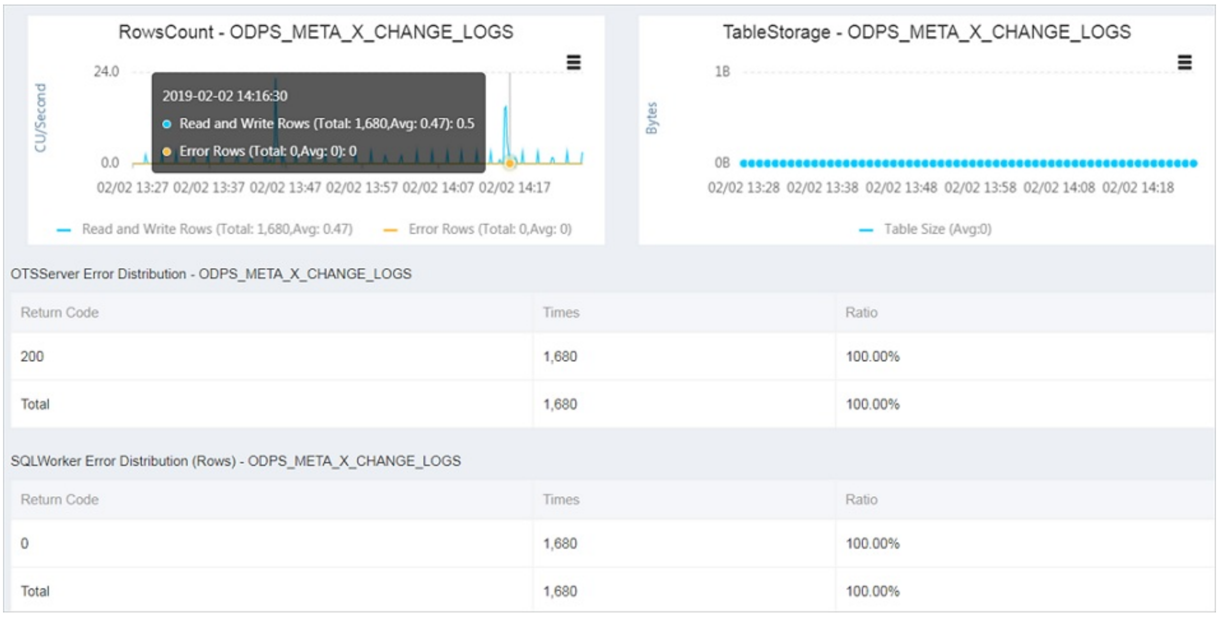
> **Note** The Instance field is required. The Table and Operation fields are optional.



*Region: [illegible] ▾ *Cluster: [illegible] ▾ *Instance: odps Table: ODPS_META_X_CHANGE_LOGS ▾ Operation: -- ▾

*Start: 2019-02-02 12:37:09 *End: 2019-02-02 13:37:09 1 Hour ▾ Search Refresh

QPS - ODPS_META_X_CHANGE_LOGS
Times/Second
22.0
0.0
02/02 12:37
02/02 12:47
02/02 12:57
02/02 13:07
02/02 13:17
02/02 13:27
Times (Total:1,695,Avg: 0.49)
Error QPS - ODPS_META_X_CHANGE_LOGS
Times/Second
1.0
0.0
02/02 12:37
02/02 12:47
02/02 12:57
02/02 13:07
02/02 13:17
02/02 13:27
400 (Total: 0,Avg: 0)
403 (Total: 0,Avg: 0)
404 (Total: 0,Avg: 0)
409 (Total: 0,Avg: 0)
413 (Total: 0,Avg: 0)
500 (Total: 0,Avg: 0)
503 (Total: 0,Avg: 0)
CapacityUnit - ODPS_META_X_CHANGE_LOGS
CU/Second
15.0
7.5
0.0
02/02 12:37
02/02 12:47
02/02 12:57
02/02 13:07
02/02 13:17
02/02 13:27
Read CU (Total: 1,017,Avg: 0.29)
Write CU (Total: 896,Avg: 0.26)
Net Flow - ODPS_META_X_CHANGE_LOGS
Bytes/S
11.7KB
0B
2019-02-02 12:37:50
Internal Network Input (Total: 1,873,195,Avg: 541.39): 0B
Internal Network Output (Total: 101,811,Avg: 29.43): 0B
Public Network Input (Total: 0,Avg: 0): 0B
Public Network Output (Total: 0,Avg: 0): 0B
Internal Output User Data (Total: 53,340,Avg: 15.42): 0B
Internal Output User Data (Total: 1,588,655,Avg: 459.15): 0B
Public Output User Data (Total: 0,Avg: 0): 0B
Public Input User Data (Total: 0,Avg: 0): 0B



RowsCount - ODPS_META_X_CHANGE_LOGS
CU/Second
24.0
0.0
2019-02-02 14:16:30
Read and Write Rows (Total: 1,680,Avg: 0.47): 0.5
Error Rows (Total: 0,Avg: 0): 0
02/02 13:27
02/02 13:37
02/02 13:47
02/02 13:57
02/02 14:07
02/02 14:17
Read and Write Rows (Total: 1,680,Avg: 0.47)
Error Rows (Total: 0,Avg: 0)
TableStorage - ODPS_META_X_CHANGE_LOGS
Bytes
1B
0B
02/02 13:28
02/02 13:38
02/02 13:48
02/02 13:58
02/02 14:08
02/02 14:18
Table Size (Avg:0)

OTSServer Error Distribution - ODPS_META_X_CHANGE_LOGS

Return Code	Times	Ratio
200	1,680	100.00%
Total	1,680	100.00%

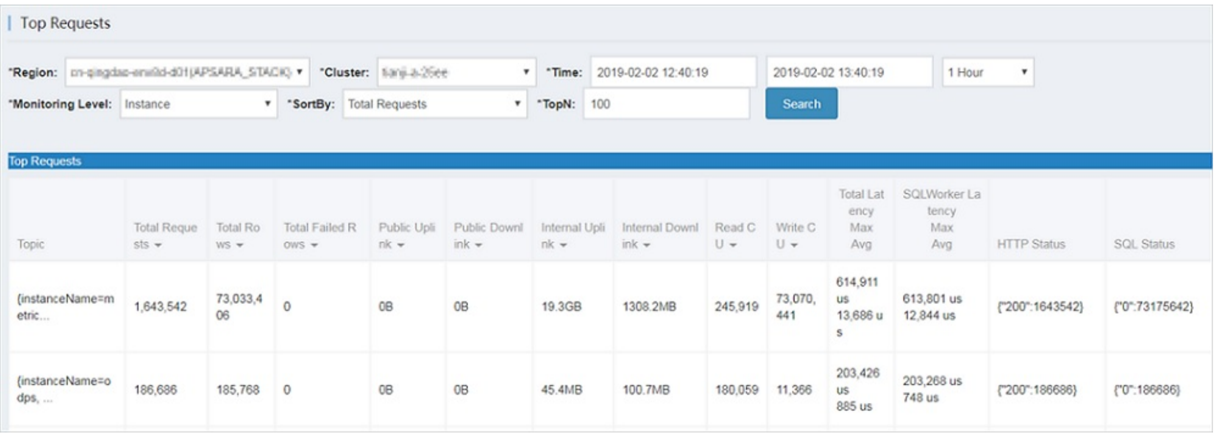
SQLWorker Error Distribution (Rows) - ODPS_META_X_CHANGE_LOGS

Return Code	Times	Ratio
0	1,680	100.00%
Total	1,680	100.00%

9.6.1.5.3. Top requests

You can view the top request distribution of clusters by monitoring level or dimension.

The following monitoring levels are supported for top requests: Instance, Instance-Operation, Instance-Table, and Instance-Table-Operation. You can view the top request details of a cluster based on 13 different metrics such as the total number of requests and the total number of rows.



Top Requests

*Region: [redacted] *Cluster: [redacted] *Time: 2019-02-02 12:40:19 2019-02-02 13:40:19 1 Hour

*Monitoring Level: Instance *SortBy: Total Requests *TopN: 100

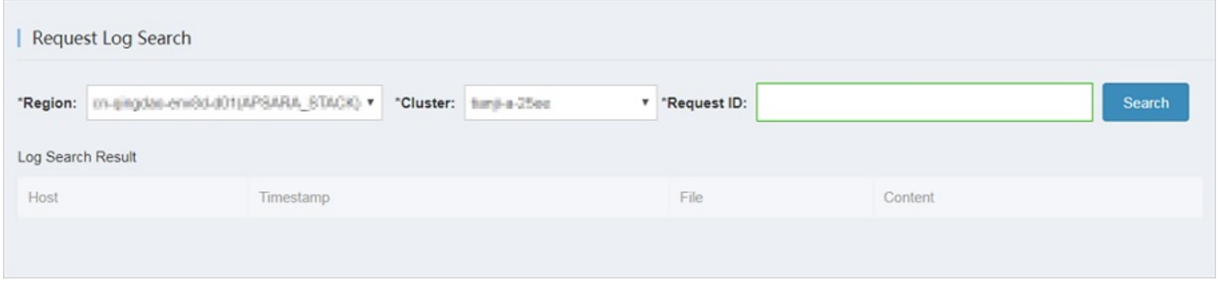
Top Requests

Topic	Total Requests	Total Rows	Total Failed Rows	Public Uplink	Public Downlink	Internal Uplink	Internal Downlink	Read CU	Write CU	Total Latency Max Avg	SQLWorker Latency Max Avg	HTTP Status	SQL Status
{instanceName=metric...	1,643,542	73,033,406	0	0B	0B	19.3GB	1308.2MB	245,919	73,070,441	614,911 us 13,686 us	613,801 us 12,844 us	{"200":1643542}	{"0":73175642}
{instanceName=odps, ...	186,686	185,768	0	0B	0B	45.4MB	100.7MB	180,059	11,366	203,426 us 885 us	203,268 us 748 us	{"200":186686}	{"0":186686}

9.6.1.5.4. Request log search

You can search for request logs by using request IDs to assist problem investigation.

You can query all logs associated with a region, cluster, and request ID.



Request Log Search

*Region: [redacted] *Cluster: [redacted] *Request ID:

Log Search Result

Host	Timestamp	File	Content

9.6.1.6. System management

9.6.1.6.1. Task management

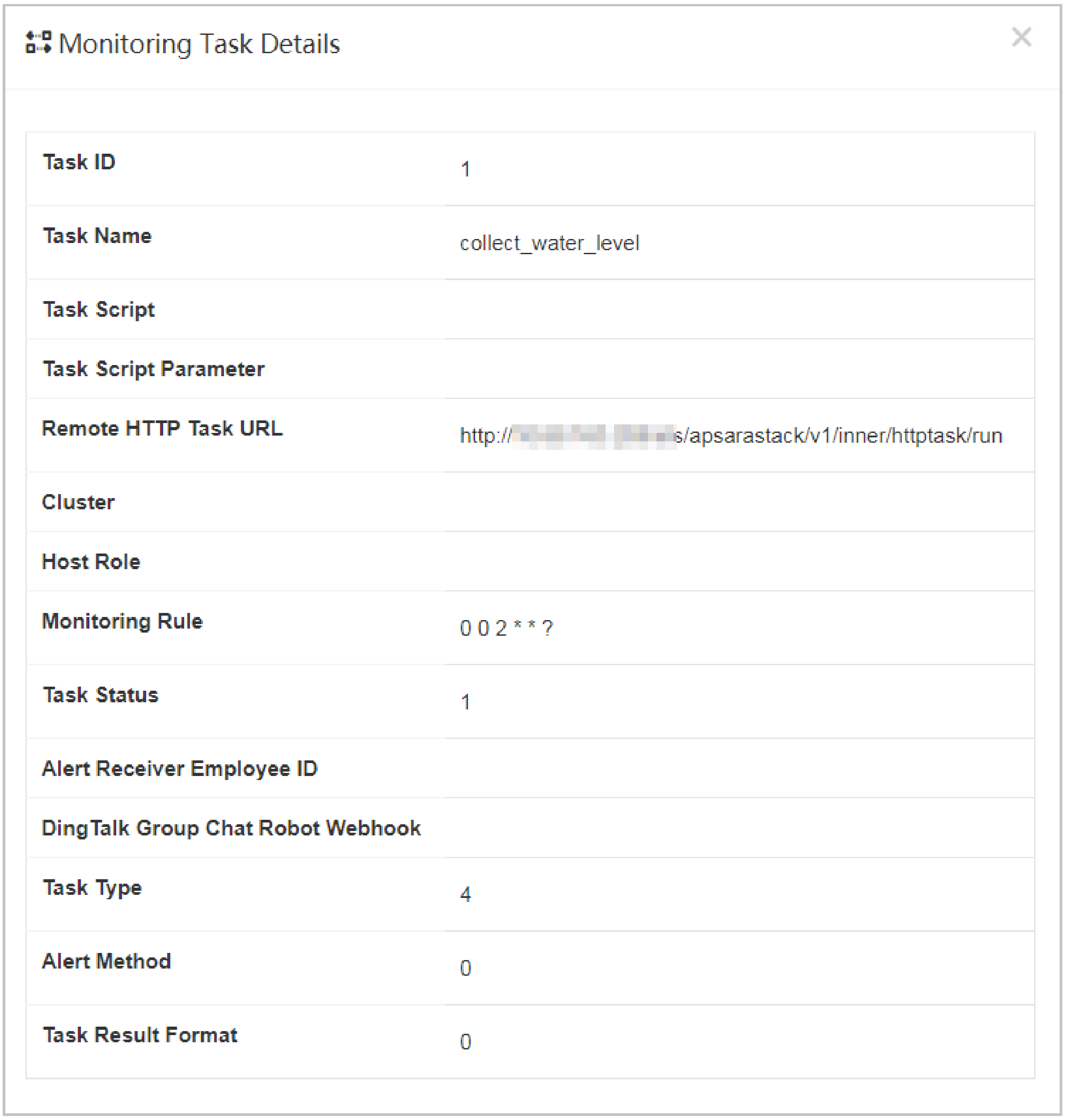
Background tasks are managed by Tablestore Operations and Maintenance System.

After Tablestore Operations and Maintenance System is deployed in the Apsara Stack environment, the background tasks that collect usage statistics are automatically integrated.

You can perform the following operations on background tasks:

- View task details such as the specific parameters and running time of each task.

  Click **Details** corresponding to a task to view the task details. The following figure shows a monitoring rule displayed on the task details page. The task collects usage statistics at 02:00:00 every day.



Monitoring Task Details

Task ID	1
Task Name	collect_water_level
Task Script	
Task Script Parameter	
Remote HTTP Task URL	http://[redacted]s/apsarastack/v1/inner/httptask/run
Cluster	
Host Role	
Monitoring Rule	0 0 2 * * ?
Task Status	1
Alert Receiver Employee ID	
DingTalk Group Chat Robot Webhook	
Task Type	4
Alert Method	0
Task Result Format	0

- Enable or disable a task.

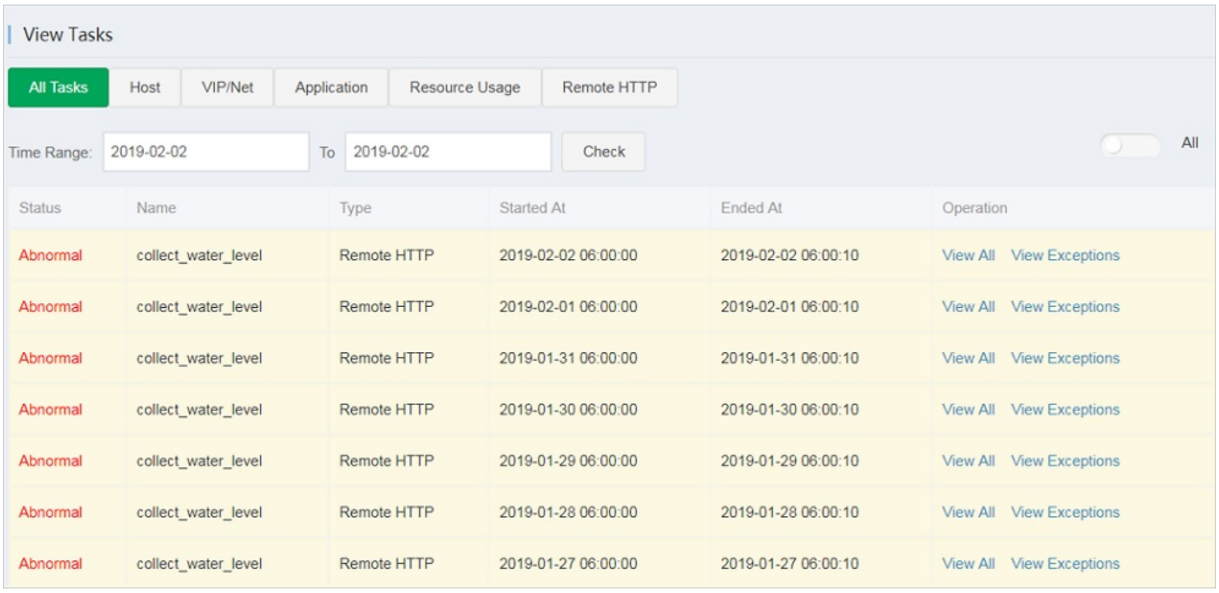
> Note Disabled tasks no longer run automatically.

- Run a task immediately.

9.6.1.6.2. View tasks

You can view the execution status of background tasks and find the causes of task exceptions.

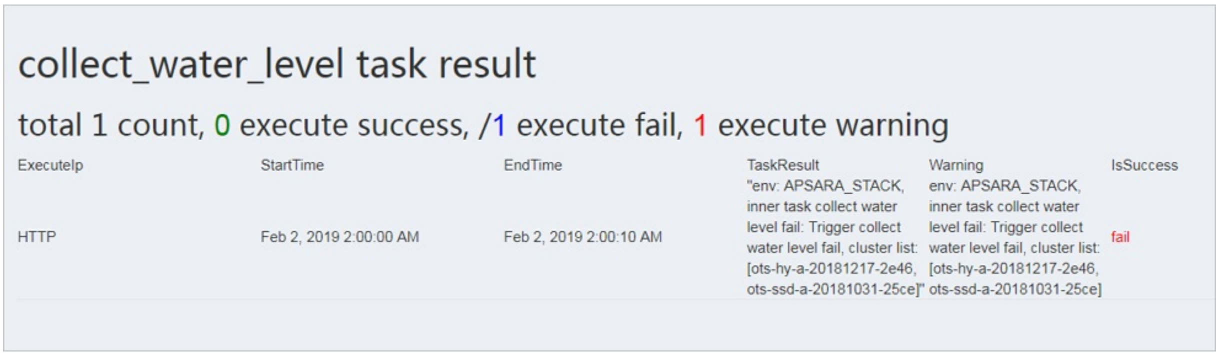
The following figure shows the execution status of background tasks in Tablestore Operations and Maintenance System. You can view the succeeded or failed tasks.



View Tasks

Status	Name	Type	Started At	Ended At	Operation
Abnormal	collect_water_level	Remote HTTP	2019-02-02 06:00:00	2019-02-02 06:00:10	View All View Exceptions
Abnormal	collect_water_level	Remote HTTP	2019-02-01 06:00:00	2019-02-01 06:00:10	View All View Exceptions
Abnormal	collect_water_level	Remote HTTP	2019-01-31 06:00:00	2019-01-31 06:00:10	View All View Exceptions
Abnormal	collect_water_level	Remote HTTP	2019-01-30 06:00:00	2019-01-30 06:00:10	View All View Exceptions
Abnormal	collect_water_level	Remote HTTP	2019-01-29 06:00:00	2019-01-29 06:00:10	View All View Exceptions
Abnormal	collect_water_level	Remote HTTP	2019-01-28 06:00:00	2019-01-28 06:00:10	View All View Exceptions
Abnormal	collect_water_level	Remote HTTP	2019-01-27 06:00:00	2019-01-27 06:00:10	View All View Exceptions

Click **View All** or **View Abnormal** in the Operation column corresponding to the abnormal task to view the specific cause of a task failure, as shown in the following figure.



collect_water_level task result

total 1 count, 0 execute success, /1 execute fail, 1 execute warning

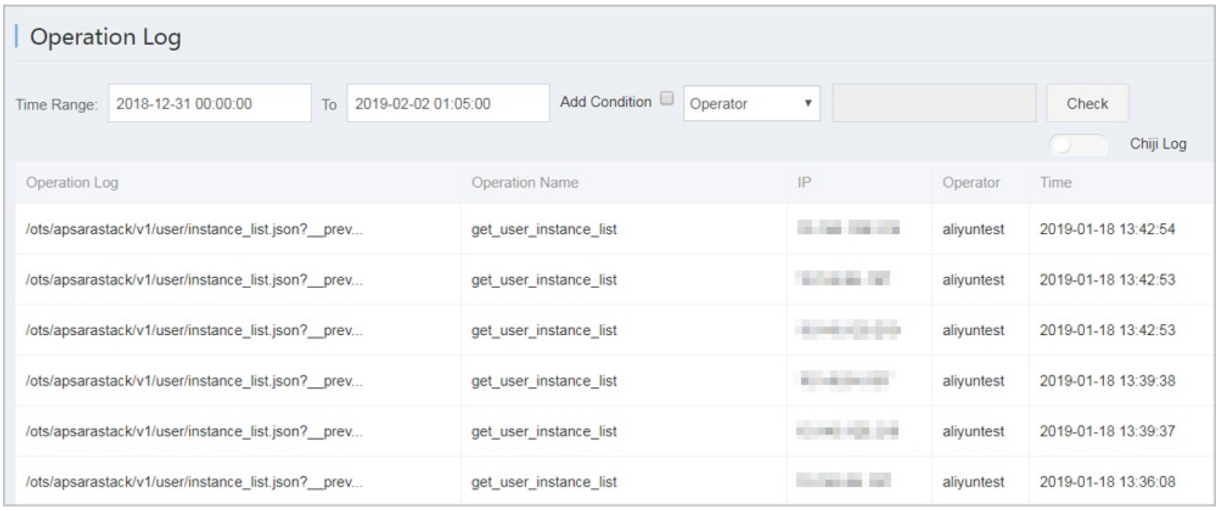
ExecuteIp	StartTime	EndTime	TaskResult	Warning	IsSuccess
HTTP	Feb 2, 2019 2:00:00 AM	Feb 2, 2019 2:00:10 AM	"env: APSARA_STACK, inner task collect water level fail: Trigger collect water level fail, cluster list: [ots-hy-a-20181217-2e46, ots-ssd-a-20181031-25ce]"	env: APSARA_STACK, inner task collect water level fail: Trigger collect water level fail, cluster list: [ots-hy-a-20181217-2e46, ots-ssd-a-20181031-25ce]	fail

9.6.1.7. Platform audit

9.6.1.7.1. Operation logs

You can view the management and control operation logs of Storage Operations and Maintenance System.

The **Operation Log** page provides the operation logs of Tablestore Operations and Maintenance System. You can query audit records generated within a specified time range and filter the records to obtain information about the platform status.



Operation Log

Time Range: 2018-12-31 00:00:00 To 2019-02-02 01:05:00 Add Condition □ Operator ▾ Check

Chiji Log

Operation Log	Operation Name	IP	Operator	Time
/ots/apsarastack/v1/user/instance_list.json?__prev...	get_user_instance_list	[redacted]	aliyuntest	2019-01-18 13:42:54
/ots/apsarastack/v1/user/instance_list.json?__prev...	get_user_instance_list	[redacted]	aliyuntest	2019-01-18 13:42:53
/ots/apsarastack/v1/user/instance_list.json?__prev...	get_user_instance_list	[redacted]	aliyuntest	2019-01-18 13:42:53
/ots/apsarastack/v1/user/instance_list.json?__prev...	get_user_instance_list	[redacted]	aliyuntest	2019-01-18 13:39:38
/ots/apsarastack/v1/user/instance_list.json?__prev...	get_user_instance_list	[redacted]	aliyuntest	2019-01-18 13:39:37
/ots/apsarastack/v1/user/instance_list.json?__prev...	get_user_instance_list	[redacted]	aliyuntest	2019-01-18 13:36:08

9.6.2. Cluster environments

This topic describes the environment and service information of Tablestore.

Two environments are provided for Tablestore: the internal environment for cloud services such as MaxCompute, Log Service, or StreamSQL, and the external environment deployed for users.

Some cloud services use both environments. For example, metadata of StreamSQL is stored in the internal environment, but its user data is stored in the external environment.

Tablestore services include TableStoreOCM, TableStoreInner/TableStore, TableStorePortal, chiji, and TableStoreSqlInner/TableStoreSql.

- TableStoreOCM: the tool used to manage information about clusters, users, and instances
- TableStoreInner/TableStore: the Tablestore data service node
- TableStorePortal: the background of the Tablestore O&M platform
- chiji: the Tablestore O&M platform used for fault location
- TableStoreSqlInner/TableStoreSql: the Tablestore background tool

9.6.3. System roles

This topic describes the functions of system roles.

- TableStoreOCM
  - OCMInit: the OCM initialization tool used to create tables and bind POP APIs
  - OCM: the service node of OCM
  - ServiceTest: the service test image of OCM
- TableStoreInner/TableStore
  - InitCluster: the process of adding cluster information to OCM, including the domain name, cluster type, and pre-configured Tablestore account information
  - LogSearchAgent: the log collection node of Tablestore
  - MeteringServer: the metering node that is available only in Tablestore
  - MonitorAgent: the data collection node of the Tablestore monitoring system
  - MonitorAgg: the data aggregation node of the Tablestore monitoring system

  - OTSAlertChecker: the alerting module of Tablestore
  - OTSFrontServer: the frontend server of Tablestore, which can be NGINX, OTS Server, or Replication Server
  - OTSServer: the fronted service of Tablestore
  - OTSTEngine: the NGINX service for Tablestore frontend servers
  - PortalAgServer: the background service of Tablestore Operations and Maintenance System
  - ServiceTest: the test service that runs scheduled smoke tests
  - SQLOnlineReplicationServer: the disaster recovery service of Tablestore
  - SQLOnlineWorker: the application that was used to generate alerts but no longer provides services
  - TableStoreAdmin: all O&M tools of Tablestore, including the splitting and merging tools

- TableStorePortal
  - PortalApiServer: the background service of Tablestore Operations and Maintenance System

- TableStoreSqlInner/TableStoreSql
  - Tools: the background tools of Tablestore such as sqlonline_console
  - UpgradeSql: the background hot upgrade tool of Tablestore

9.6.4. Pre-partition a table

9.6.4.1. Pre-partitioning

This topic describes the rules and methods of pre-partitioning.

When you create a table, Tablestore automatically creates a partition for the table. This partition can be configured to automatically split based on the data size or data access load when your business develops. A table that has only one partition may be unable to provide sufficient service capabilities during a stress test or data import. In this scenario, you must pre-partition the table.

Pre-partitioning rules

You can estimate the required number of partitions based on the standard size of 10 GB per partition. However, other factors such as the number of hosts and concurrent write operations by developers must be considered. We recommend that the total number of partitions do not exceed 256. If data can be written into the table evenly, you can partition the table equally based on the number of partitions required.

> **Note** When data is written into the table, the system automatically splits the table to ensure sufficient partitions are available when the data increases.

Pre-partitioning methods

You can use split_merge.py to pre-partition a data table. You can obtain split_merge.py from */apsara/TableStoreAdmin/split* on the host of TableStoreAdmin in TableStoreInner.

You can use any of the following methods to partition a data table:

> **Note** You can also use the following methods to partition a table that already has data.

- Specify a split point

  ```
  python2.7 split_merge.py split_table -p point1 point2 ... table name
  ```

- Specify the number of partitions and the partition key format
  - The partition key is of the int type.

    ```
    python2.7 split_merge.py split_table -n: number of partitions --key_digit: table name
    ```

  - The partition key starts with an MD5 hash in lowercase. The MD5 hash can contain digits and lowercase letters from a to f.

    ```
    python2.7 split_merge.py split_table -n: number of partitions --key_hex_lower: table name
    ```

  - The partition key starts with an MD5 hash in uppercase. The MD5 hash can contain digits and uppercase letters from A to F.

    ```
    python2.7 split_merge.py split_table -n: number of partitions --key_hex_upper: table name
    ```

  - The partition key is Base64-encoded, and can contain the plus sign (+), forward slash (/), digits and letters.

    ```
    python2.7 split_merge.py split_table -n: number of partitions --key_base64: table name
    ```

  - -- only_plan: generates split points but does not split the table. -- force: directly splits the table without manual confirmation.

    ```
    python2.7 split_merge.py split_table -n: number of partitions --key_digit --only_plan: table name
    ```

- Split a partition based on the existing data

  ```
  python2.7 split_merge.py split_partition -n PART_COUNT (number of partitions) partition_id
  ```

9.6.4.2. View partitions

You can view the partitions of a data table in Tablestore Operations and Maintenance System.

On the Tablestore Operations and Maintenance System, find a table in the specified instance. Click the table name to view details of the table. On the **Partitions** tab, you can view the information of all partitions in the table. The information contains the partition ID, range, worker, Apsara Distributed File System file size, and data size. The partition size displayed may not be the current partition size because the data is updated only after the system merges files. The Apsara Distributed File System file size is the compressed data size. The actual storage space is three times the file size because the data is stored in three copies.

9.7. ApsaraDB RDS

9.7.1. Architecture

9.7.1.1. System architecture

9.7.1.1.1. Backup system

ApsaraDB RDS can back up databases at any time and restore them to a specific point in time based on the backup policy, which makes the data more traceable.

Automatic backup

ApsaraDB RDS for MySQL supports both physical and logical backups.

You can flexibly configure the backup start time within off-peak hours. All backup files are retained for seven days.

Temporary backup

You can create temporary backup files when necessary. Temporary backup files are retained for seven days.

Log management

ApsaraDB RDS for MySQL generates binlogs that you can download for local incremental backup.

Instance cloning

A cloned instance is a new instance whose data and settings are the same as those of the primary instance. This feature allows you to restore data of the primary instance or create multiple instances that are the same as the primary instance.

9.7.1.1.2. Data migration system

ApsaraDB RDS provides Data Transmission Service (DTS) to help you migrate databases.

Replicate databases between instances

ApsaraDB RDS allows you to migrate databases from one instance to another.

Migrate data to or from RDS instances

ApsaraDB RDS provides professional tools and migration wizards to help you migrate data to or from RDS instances.

Download backup files

ApsaraDB RDS retains backup files for seven days. During this period, you can log on to the RDS console to download the files.

9.7.1.1.3. Monitoring system

ApsaraDB RDS provides multi-dimensional monitoring services across the physical, network, and application layers to ensure business availability.

Performance monitoring

ApsaraDB RDS provides nearly 20 metrics for system performance monitoring, such as disk capacity, input/output operations per second (IOPS), connections, CPU utilization, network traffic, transactions per second (TPS), queries per second (QPS), and cache hit rate. You can obtain the running status information of instances within the past year.

SQL auditing

The system records the SQL statements and related information sent to ApsaraDB RDS instances, such as the connection IP address, database name, access account, execution time, and number of records returned. You can use SQL auditing to locate problems and check instance security.

Threshold alerts

ApsaraDB RDS provides alert SMS notifications in the event of exceptions in instance status or performance.

These exceptions include instance locking, disk capacity, IOPS, connections, and CPU. You can configure alert thresholds and up to 50 alert contacts (of which five are effective at a time). When an instance exceeds the threshold, an SMS notification is sent to the alert contacts.

Web operation logs

The system records all modification operations in the ApsaraDB RDS console for administrators to check. These logs are retained for up to 30 days.

9.7.1.1.4. Control system

If a host or instance stops responding, it switches services over within 30 seconds after the high-availability (HA) component detects an exception. This ensures that applications run normally.

9.7.1.1.5. Task scheduling system

You can use the ApsaraDB RDS console or API operations to create and delete instances, or switch instances between the internal network and Internet. All instance operations are scheduled, traced, and displayed as tasks.

9.7.2. Log on to the Apsara Uni-manager Operations Console

This topic describes how to log on to the Apsara Uni-manager Operations Console.

Prerequisites

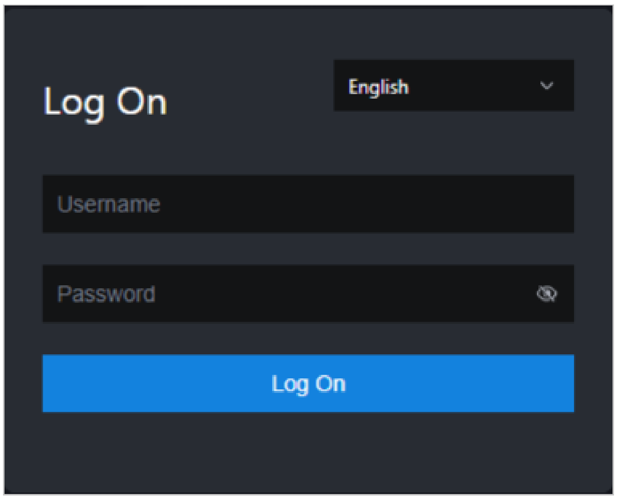
- The URL, username, and password that are required to log on to the Apsara Uni-manager Operations Console are obtained from the deployment personnel or administrators.

  The URL of the Apsara Uni-manager Operations Console is in the format of *region-id*.ops.console.*intranet-domain-id*.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL. Then, press the Enter key.



> Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   > Note To obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console, contact the deployment personnel or administrators.

   If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username as prompted.

   To enhance security, make sure that the password meets the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password is 10 to 20 characters in length.
4. Click **Log On**.

9.7.3. Manage instances

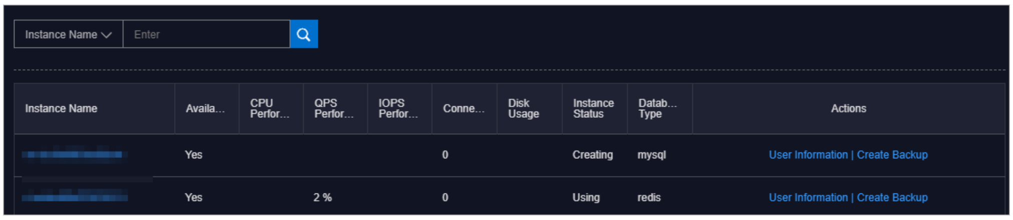
This topic describes how to manage ApsaraDB RDS instances. You can view instance details, logs, and user information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the top navigation bar, click O&M. In the left-side navigation pane, choose **Product Management > RDS**.
3. On the **Instance Management** tab of the **RDS** page, you can perform the following operations:
   - View instances

     View the instances that belong to your account on the **Instance Management** tab, as shown in Instances.

Instances



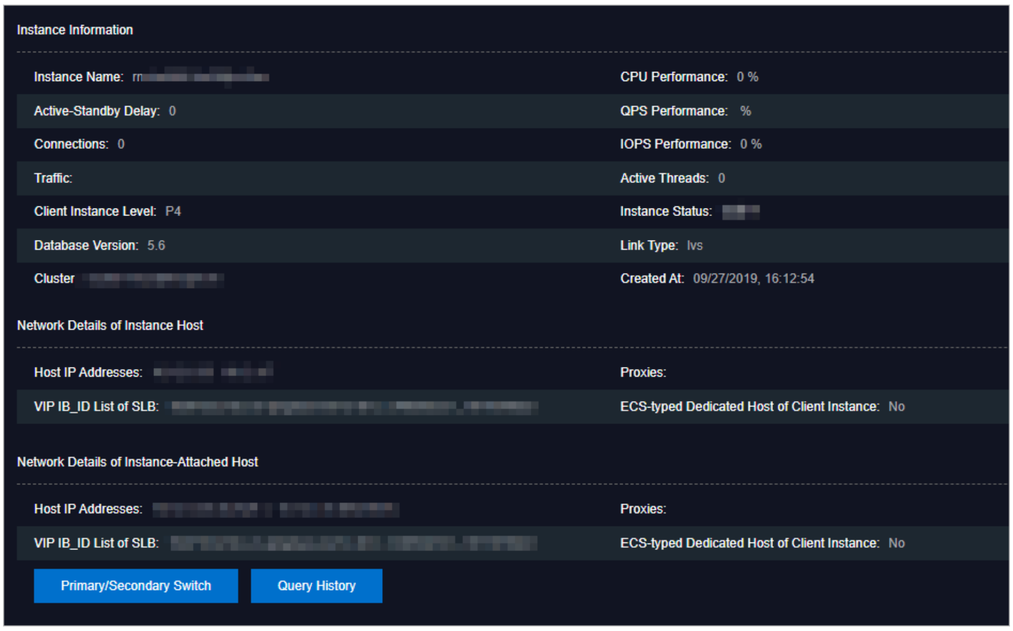
Instance Name	Availa...	CPU Perfor...	QPS Perfor...	IOPS Perfor...	Conne...	Disk Usage	Instance Status	Datab... Type	Actions
[redacted]	Yes				0		Creating	mysql	User Information | Create Backup
[redacted]	Yes		2 %		0		Using	redis	User Information | Create Backup

- View instance details

  Click the ID of an instance to view its details, as shown in Instance details. You can switch your service between primary and secondary instances and query history operations on this page.

  > **Note** We recommend that you do not perform forced switchover, because it may result in data loss if data is not synchronized between the primary and secondary instances.

Instance details



Instance Information

Instance Name: [redacted]	CPU Performance: 0 %
Active-Standby Delay: 0	QPS Performance: %
Connections: 0	IOPS Performance: 0 %
Traffic:	Active Threads: 0
Client Instance Level: P4	Instance Status: [redacted]
Database Version: 5.6	Link Type: lvs
Cluster [redacted]	Created At: 09/27/2019, 16:12:54

Network Details of Instance Host

Host IP Addresses: [redacted]	Proxies:
VIP IB_ID List of SLB: [redacted]	ECS-typed Dedicated Host of Client Instance: No

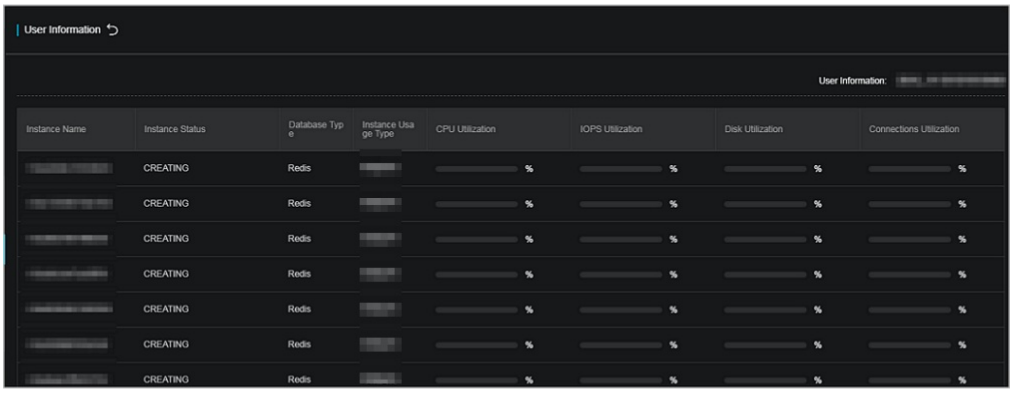
Network Details of Instance-Attached Host

Host IP Addresses: [redacted]	Proxies:
VIP IB_ID List of SLB: [redacted]	ECS-typed Dedicated Host of Client Instance: No

- **View user information**

  Click **User Information** in the **Actions** column corresponding to an instance, as shown in User information.

User information



User Information

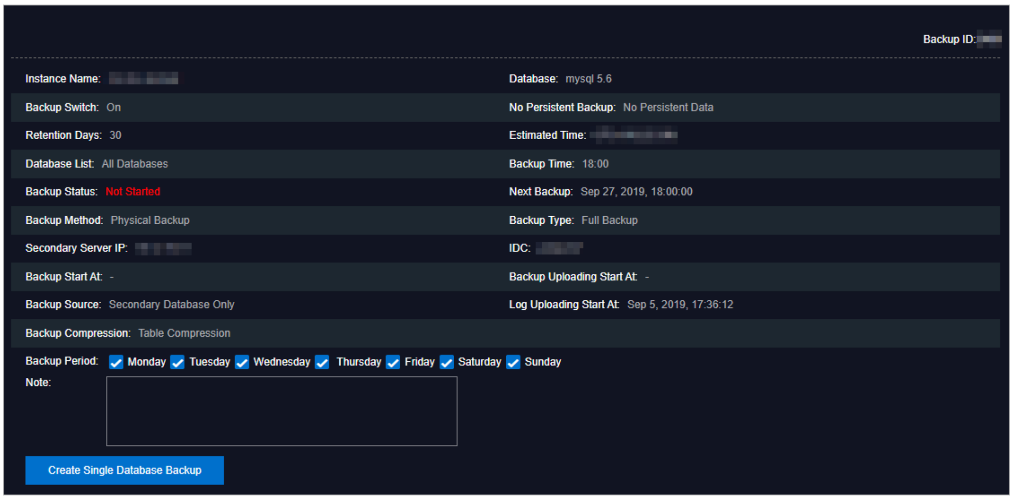
User Information: [redacted]

Instance Name	Instance Status	Database Type	Instance Usage Type	CPU Utilization	IOPS Utilization	Disk Utilization	Connections Utilization
[redacted]	CREATING	Redis	[redacted]	%	%	%	%
[redacted]	CREATING	Redis	[redacted]	%	%	%	%
[redacted]	CREATING	Redis	[redacted]	%	%	%	%
[redacted]	CREATING	Redis	[redacted]	%	%	%	%
[redacted]	CREATING	Redis	[redacted]	%	%	%	%
[redacted]	CREATING	Redis	[redacted]	%	%	%	%
[redacted]	CREATING	Redis	[redacted]	%	%	%	%

- **Create backups**

  For ApsaraDB RDS for MySQL instances, click **Create Backup** in the **Actions** column to view the backup information, as shown in Backup information. You can also click **Create Single Database Backup** on the Backup Information page to back up a single database.

  Backup information



Backup ID: [redacted]

Instance Name: [redacted]	Database: mysql 5.6
Backup Switch: On	No Persistent Backup: No Persistent Data
Retention Days: 30	Estimated Time: [redacted]
Database List: All Databases	Backup Time: 18:00
Backup Status: Not Started	Next Backup: Sep 27, 2019, 18:00:00
Backup Method: Physical Backup	Backup Type: Full Backup
Secondary Server IP: [redacted]	IDC: [redacted]
Backup Start At: -	Backup Uploading Start At: -
Backup Source: Secondary Database Only	Log Uploading Start At: Sep 5, 2019, 17:36:12
Backup Compression: Table Compression	

Backup Period: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday

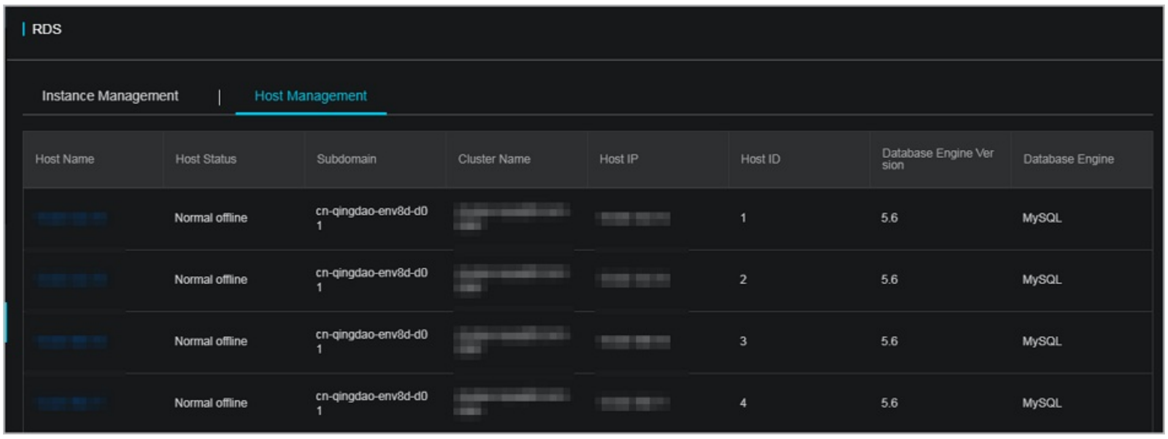
Note:

9.7.4. Manage hosts

This topic describes how to view and manage hosts.

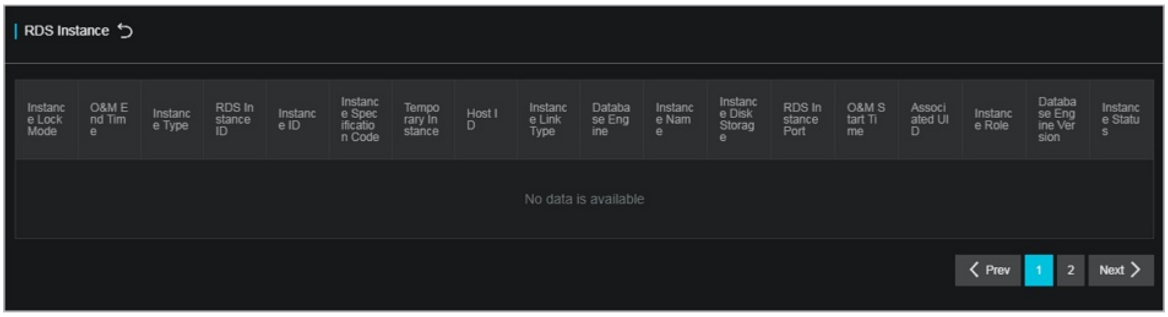
Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. In the left-side navigation pane, choose **Product Management > RDS**.
3. On the **Host Management** tab of the **RDS** page, you can view information of all hosts.



Host Name	Host Status	Subdomain	Cluster Name	Host IP	Host ID	Database Engine Version	Database Engine
[redacted]	Normal offline	cn-qingdao-env8d-d01	[redacted]	[redacted]	1	5.6	MySQL
[redacted]	Normal offline	cn-qingdao-env8d-d01	[redacted]	[redacted]	2	5.6	MySQL
[redacted]	Normal offline	cn-qingdao-env8d-d01	[redacted]	[redacted]	3	5.6	MySQL
[redacted]	Normal offline	cn-qingdao-env8d-d01	[redacted]	[redacted]	4	5.6	MySQL

4. Click a hostname to go to the **RDS Instance** page. You can view all instances on this host.



RDS Instance

Instance Lock Mode	O&M End Time	Instance Type	RDS Instance ID	Instance ID	Instance Specification Code	Temporary Instance	Host ID	Instance Link Type	Database Engine	Instance Name	Instance Disk Storage	RDS Instance Port	O&M Start Time	Associated UID	Instance Role	Database Engine Version	Instance Status

No data is available

9.7.5. Security maintenance

9.7.5.1. Network security maintenance

Network security maintenance consists of device and network security maintenance.

Device security

Check network devices and enable their security management protocols and configurations of devices.

Check for timely updates to secure versions of network device software.

For more information about the security maintenance method, see the device documentation.

Network security

Based on your network considerations, select the intrusion detection system (IDS) or intrusion prevention system (IPS) to detect abnormal Internet and Intranet traffic and protect against attacks.

9.7.5.2. Account password maintenance

Account passwords include RDS system passwords and device passwords.

To ensure account security, you must periodically change the system and device passwords, and use passwords with high complexity.

9.7.6. Redline V4.3.3 O&M description

9.7.6.1. Services provided by Redline Enterprise

This topic describes the services provided by Redline Enterprise.

Redline Enterprise provides the following services:

- redline-perf.LogWorker#
- redline-perf.OpenApi#
- redline-perf.PerfMaster#
- redline-perf.PerfWorker#

Note

- redline-perf.DbInit is discontinued.
- The collection agent of UE is deployed on physical machines in other modes.

9.7.6.2. Paths of files in the Docker container of redline-perf

This topic describes the paths of files in the Docker container of redline-perf.

PerfMaster, PerfWorker, and LogWorker

The following table describes the mapping relationships between the preceding data collection services and clusters.

Service	Cluster
PerfMaster	master
PerfWorker	perf
LogWorker	log

Paths:

- Root path: */home/admin/redline-perf/*
- Path of database data in the Docker container: */home/admin/redline-perf/ignite*
- Paths of database data on the host

Node	Path
PerfMaster node	*/cloud/data/redline-perf/PerfMaster#/perf-master/home/admin/redline-perf/ignite/*
PerfWorker node	*/cloud/data/redline-perf/PerfWorker#/perf-worker/home/admin/redline-perf/ignite/*
LogWorker node	*/cloud/data/redline-perf/LogWorker#/log-worker/home/admin/redline-perf/ignite/*

- Path of log data in the Docker container: */home/admin/redline-perf/log*

> **Note**
>
> - `app.log` is the main program log, which contains the log entries that record the extract, transform, load (ETL), storage, data retrieval API operation, and data aggregation to minute granularity.
> - `datax.log` is the synchronization module log, which contains the log entries that record the operations of synchronizing metadata from the metadatabase and pushing real-time tables to Cloud Monitor.

- Paths of log data on the host

Node	Path
PerfMaster node	*/cloud/data/redline-perf/PerfMaster#/perf-master/home/admin/redline-perf/log/*
PerfWorker node	*/cloud/data/redline-perf/PerfWorker#/perf-worker/home/admin/redline-perf/log/*
LogWorker node	*/cloud/data/redline-perf/LogWorker#/log-worker/home/admin/redline-perf/log/*

OpenAPI

This is an end-to-end gateway service.

Paths:

- Root path: */home/admin/dll-service-aliyun-com*
- Path of log data in the Docker container: */home/admin/dll-service-aliyun-com/logs*
- Path of log data on the host: */cloud/data/redline-perf/OpenApi#/open-api/home/admin/dll-service-aliyun-com/logs*

9.7.6.3. Perform environment checks

This topic describes how to perform environment checks.

Prepare the script for batch operations

1. Run the following commands on a jumper server to prepare the script for batch operations:

```
curl "http://localhost:7070/api/v3/column/m.ip?m.sr.id=redline-perf.PerfMaster%23" | grep ip | awk -F '"
' '{print $(NF-1)}' > masterhosts
curl "http://localhost:7070/api/v3/column/m.ip?m.sr.id=redline-perf.PerfWorker%23" | grep ip | awk -F '
"' '{print $(NF-1)}' > perfworkerhosts
curl "http://localhost:7070/api/v3/column/m.ip?m.sr.id=redline-perf.LogWorker%23" | grep ip | awk -F '"
' '{print $(NF-1)}' > logworkerhosts
cat perfworkerhosts logworkerhosts masterhosts  | sort -u > allhosts
```

2. Run the following command to install parallel-ssh (pssh). Skip this step if pssh has been installed.

```
wget https://parallel-ssh.googlecode.com/files/pssh-2.3.1.tar.gz
# If the jump server cannot be connected to the Internet, you can download the installation file to another machine and upload the file to the jump server.
tar zxvf pssh-2.3.1.tar.gz
cd pssh-2.3.1
python setup.py install
```

Check node connectivity

After you install pssh, check whether all nodes are running normally.

1. (Required) Check the communication information between LogWorker nodes.
   1. Run the following command on the jumper server:

      ```
      pssh -h logworkerhosts -p 1 -P 'docker ps |grep redline | grep LogWorker|awk '"'"'{ print $1}'"'"' | xargs -I ID docker exec ID curl 'http://127.0.0.1:8080/admin/makeBaseline?igniteCluster=log''
      ```

   2. Check whether the number of nodes displayed in the ONLINE server nodes section is consistent with the number of deployed nodes. If the number is inconsistent or a message of NOT IN BASELINE is returned, fix this issue. For more information, see Fix connection failures.
2. (Required) Check the communication information between PerfWorker nodes.
   1. Run the following command on the jumper server:

      ```
      pssh -h perfworkerhosts -p 1 -P 'docker ps |grep redline | grep PerfWorker|awk '"'"'{ print $1}'"'"' | xargs -I ID docker exec ID curl 'http://127.0.0.1:8080/admin/makeBaseline?igniteCluster=perf''
      ```

   2. Check whether the number of nodes displayed in the ONLINE server nodes section is consistent with the number of deployed nodes. If the number is inconsistent or a message of NOT IN BASELINE is returned, fix this issue. For more information, see Fix connection failures.
3. (Required) Check the communication information between PerfMaster nodes.
   1. Run the following command on the jumper server:

      ```
      pssh -h masterhosts -p 1 -P 'docker ps |grep redline | grep PerfMaster|awk '"'"'{ print $1}'"'"' | xargs -I ID docker exec ID curl 'http://127.0.0.1:8080/admin/makeBaseline?igniteCluster=master''
      ```

   2. Check whether the number of nodes displayed in the ONLINE server nodes section is consistent with the number of deployed nodes. If the number is inconsistent or a message of NOT IN BASELINE is returned, fix this issue. For more information, see Fix connection failures.
4. (Required) Check whether clusters are active.
   1. Run the following command on the jumper server:

      ```
      pssh -h allhosts -p 1 -P 'docker ps |grep redline | grep -v Open|awk '"'"'{ print $1}'"'"' | xargs -I ID sh -c "echo ID && docker exec ID tail -n 50 ./log/app.log |grep '"'deactived'"'"'
      ```

   2. Check whether log entries that include deactived are returned. If yes, go to the corresponding Docker container and activate the clusters in the deactived state. For more information, see Activate clusters in the deactived state.

Check for program exceptions

(Required) Check application logs for exceptions.

1. Run the following command on the jumper server:

```
pssh -h allhosts -p 1 -P 'docker ps |grep redline | grep -v Open|awk '"'"'{ print $1}'"'"' | xargs -I ID sh -c "ec
ho ID && docker exec ID tail -n 100 ./log/app.log |grep -C 10 '"'Exception'"'"'
```

2. If exception logs are returned, fix this issue. For more information, see Troubleshoot program exceptions.
3. If this issue cannot be fixed by using the solutions described in Troubleshoot program exceptions, contact development personnel or reset node data. For more information, see Reset node data.

9.7.6.4. O&M operations

9.7.6.4.1. Scale in or out a cluster

This topic describes how to scale in or out a cluster.

Determine whether scale-out is required

- Check the diagnostic information of an instance in the Apsara Uni-manager Management Console. If the data records of the last 3 hours are displayed after more than 5 seconds, you may need to add nodes. More nodes can increase the response speed. You can balance the return on investment (ROI) of hardware based on your needs.
- Ten nodes can support 3,000 host nodes of ApsaraDB RDS for MySQL instances. A single ApsaraDB RDS for MySQL instance can contain more than one host node.

Add a node

1. Add a node and start it.

   > Note You can add multiple nodes at a time.

2. Connect to a node that assumes a master role.
3. Run the `curl http://127.0.0.1:8080/admin/makeBaseline?apply=false` command to check whether the returned node information meets the expectation.
4. If yes, run the `curl http://127.0.0.1:8080/admin/makeBaseline?apply=true` command.

Remove a node

1. Remove a node.

   > Note You can remove only a single node each time.

2. Connect to a node that assumes a master role.
3. Run the `curl http://127.0.0.1:8080/admin/makeBaseline?apply=false` command to check whether the returned node information meets the expectation.
4. If yes, run the `curl http://127.0.0.1:8080/admin/makeBaseline?apply=true` command.
5. Wait 30 minutes for data to be balanced among the remaining nodes and then continue to remove other nodes based on your needs.

9.7.6.4.2. Upgrade or restart a cluster

This topic describes how to upgrade or restart a cluster.

Procedure

1. Connect to a PerfMaster node and run the following commands to disable its database. If no `success` message is returned, repeat the following commands until a `success` message is returned.

   ```
   curl "http://127.0.0.1:8080/admin/deactivateIgnite?igniteCluster=perf"
   curl "http://127.0.0.1:8080/admin/deactivateIgnite?igniteCluster=log"
   curl "http://127.0.0.1:8080/admin/deactivateIgnite?igniteCluster=master"
   ```

2. Wait 2 minutes and upgrade or restart the cluster after data is stored to disks.
3. After the upgrade or restart is complete, perform environment checks. For more information, see Perform environment checks.

9.7.6.4.3. Fix connection failures

This topic describes how to fix connection failures.

Fix the failure of missing nodes in the communication information

1. Connect to a missing node and run the following command:

   ```
   ps aux|grep java|grep -v grep|awk '{ print $2}'|xargs kill -9
   ```

2. Wait 3 minutes and check node connectivity again.

Fix the NOT IN BASELINE failure in the communication information

Run the following command on a PerfMaster node:

```
curl "http://127.0.0.1:8080/admin/makeBaseline?igniteCluster=${cluster}&apply=true"
```

Note `${cluster}` must be replaced with the cluster to which the node belongs, which can be master, perf, or log.

9.7.6.4.4. Activate clusters in the deactived state

This topic describes how to activate the clusters in the deactived state.

Run the following command on a PerfMaster node:

```
curl "http://127.0.0.1:8080/admin/activateIgnite?igniteCluster=${cluster}"
```

Note `${cluster}` must be replaced with the cluster to which the node belongs, which can be master, perf, or log.

9.7.6.4.5. Troubleshoot program exceptions

This topic describes how to troubleshoot program exceptions.

Troubleshoot the exception of "partition has been lostPart"

LogWorker node

```
### Connect to a Docker container of LogWorker and run the following reset commands:
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=TABLE_LOG_AUDIT_SQLS"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=TABLE_LOG_ERROR_SQLS"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=TABLE_LOG_SLOW_SQLS"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=TABLE_LOG_AUDIT_SQL_TEMPLATES"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=TABLE_LOG_AUDIT_SQLS_ROUTE_INFO"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=CACHE_CODEC"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=CACHE_CODEC_LOCK"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=CACHE_CODEC_ATOMIC_LONG"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=ignite-sys-atomic-cache@default-ds-group"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=ignite-sys-atomic-cache@default-volatile-ds-group"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=log&cacheName=NOTIFY_LOG_IGNITE_SHUTTING_DOWN"
```

PerfWorker node

```
### Connect to a Docker container of PerfWorker and run the following reset commands:
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=perf&cacheName=CACHE_CODEC"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=perf&cacheName=CACHE_CODEC_LOCK"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=perf&cacheName=CACHE_CODEC_ATOMIC_LONG"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=perf&cacheName=NOTIFY_PERF_IGNITE_SHUTTING_DOWN"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=perf&cacheName=MONITOR_ALERT_HIS_CACHE"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=perf&cacheName=MONITOR_ALERT_STATUS_INFO_CACHE"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=perf&cacheName=CACHE_REDLINE_SNAPSHOT"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=perf&cacheName=seconds-level"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=perf&cacheName=minutes-level"
```

PerfMaster node

```
### Connect to a Docker container of PerfMaster and run the following reset commands:
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=CACHE_TS_CACHE_NAME"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=NOTIFY_MASTER_IGNITE_SHUTTING_DOWN"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=LOCK_MASTER_COMPETING"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=CLUSTER_COMMAND"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=CACHE_CODEC"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=CACHE_CODEC_LOCK"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=CACHE_CODEC_ATOMIC_LONG"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=NODE_EXECUTE_COMMAND_RECORD"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=IGNITE_PERF_LOG_METADATA"
curl "http://127.0.0.1:8080/admin/resetLostPartitions?igniteCluster=master&cacheName=CHECKPOINT_CACHE_NAME"
```

Troubleshoot the exception of "Failed to perform WAL operation"

If a message of Failed to perform WAL operation is returned, contact technical personnel or reset node data. For more information, see Reset node data.

9.7.6.4.6. Reset node data

This article describes how to reset node data.

Precautions

This operation deletes all data of a specific node. Monitoring data stored on the node is deleted and cannot be recovered. Proceed with caution.

Procedure

1. Connect to the node or Docker container whose data you want to reset and run the following command:

   ```
   touch log/HOLD_START && ps aux|grep java|grep -v grep|awk '{ print $2}'|xargs kill -9 && rm -rf ignite/* && sleep 60 && rm -f log/HOLD_START &
   ```

2. Wait 3 minutes and run the following commands:

   ```
   curl "http://127.0.0.1:8080/admin/activateIgnite?igniteCluster=${cluster}"
   curl "http://127.0.0.1:8080/admin/makeBaseline?igniteCluster=${cluster}&apply=true"
   ```

   > **Note** `${cluster}` must be replaced with the cluster to which the node belongs, which can be master, perf, or log.

9.8. AnalyticDB for PostgreSQL

9.8.1. Overview

Purpose

This guide summarizes possible problems that you may encounter during O&M operations and provides solutions for you.

If you encounter system problems not covered in this guide, you can submit a ticket to Alibaba Cloud for technical support.

Requirements

You must possess IT skills including computer network knowledge, computer operation knowledge, problem analysis, and troubleshooting.

Additionally, you must pass the pre-job training of the Alibaba Cloud system to learn necessary Alibaba Cloud system knowledge, including but not limited to system principles, networking, features, and the use of maintenance tools.

Note that during maintenance operations, you must comply with operating procedures to ensure personal and system security. User data must be kept strictly confidential and must not be copied or disseminated without the written consent of the users.

Precautions

To ensure a stable system and avoid unexpected events, you must follow the following guidelines.

- Hierarchical permission management

  Permissions on networks, devices, systems, and data are granted based on the services and roles of the O&M personnel to prevent system faults caused by unauthorized operations.

- System security

  Before performing any system operations, you must be aware of their impacts.

  You must record all problems encountered during operations for problem analysis and troubleshooting.

- Personal and data security
  - You must take safety measures in accordance with the device manuals when operating electrical equipment.
  - You must use secure devices to access the business network.
  - Unauthorized data replication and dissemination are prohibited.

Support

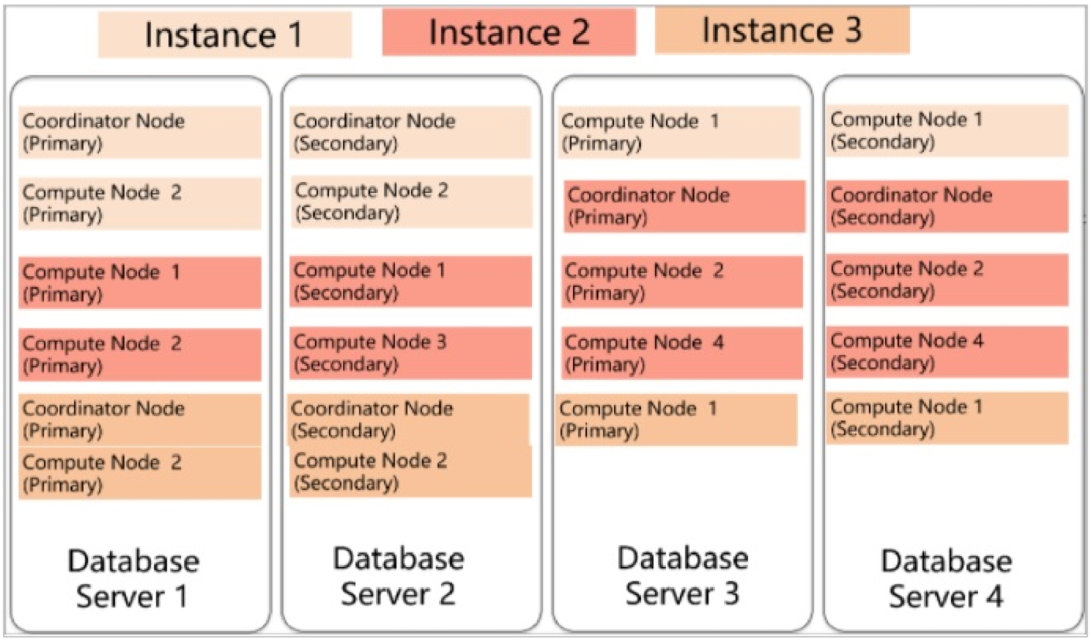
You can contact Alibaba Cloud technical support for help.

9.8.2. Architecture

The following figure shows the system architecture of AnalyticDB for PostgreSQL.

System architecture

System architecture


Instance 1
Instance 2
Instance 3
Coordinator Node (Primary)
Compute Node 2 (Primary)
Compute Node 1 (Primary)
Compute Node 2 (Primary)
Coordinator Node (Primary)
Compute Node 2 (Primary)
Database Server 1
Coordinator Node (Secondary)
Compute Node 2 (Secondary)
Compute Node 1 (Secondary)
Compute Node 3 (Secondary)
Coordinator Node (Secondary)
Compute Node 2 (Secondary)
Database Server 2
Compute Node 1 (Primary)
Coordinator Node (Primary)
Compute Node 2 (Primary)
Compute Node 4 (Primary)
Compute Node 1 (Primary)
Database Server 3
Compute Node 1 (Secondary)
Coordinator Node (Secondary)
Compute Node 2 (Secondary)
Compute Node 4 (Secondary)
Compute Node 1 (Secondary)
Database Server 4

AnalyticDB for PostgreSQL consists of two major components: the coordinator node and compute nodes.

The coordinator node is used to access applications. The coordinator node accepts connection and SQL query requests from clients and dispatches computing tasks to compute nodes. The system will deploy a secondary node of the coordinator node on an independent physical server to replicate data from the primary node for failover. The secondary node cannot connect to compute nodes or accept external links.

Compute nodes are independent data nodes in AnalyticDB for PostgreSQL. Each compute node stores a part of data, and all compute nodes work together to execute computing tasks with parallel processing. Each compute node consists of a primary node and a secondary node for failover.

9.8.3. Routine maintenance

9.8.3.1. Check for data skew on a regular basis

You must check for data skew on a regular basis during maintenance to prevent the instance from being read-only due to excessive data in some compute nodes.

You can use the following methods to locate data skew. The procedure is as follows.

1. For a single table or database, you can view the space occupied within each compute node to determine whether data has been skewed.

   i. Execute the following statement to determine whether the data in a database has been skewed:

   ```
   SELECT pg_size_pretty(pg_database_size('postgres')) FROM gp_dist_random('gp_id');
   ```

   You can view the space occupied by the dbname database in each compute node after the statement is executed. If the space occupied in one or more compute nodes is significantly greater than that of other compute nodes, it indicates the data in this database is skewed.

   ii. Execute the following statement to determine whether the data in a table has been skewed:

   ```
   SELECT pg_size_pretty(pg_relation_size('tblname')) FROM gp_dist_random('gp_id');
   ```

   Using the preceding statement, you can view the space occupied by the tblname table within each compute node after the statement is executed. If the space occupied within one or more compute nodes is significantly greater than that of other compute nodes, it indicates the data in this table is skewed. You must modify the partition key to redistribute the data.

2. You can use the system views to determine whether data has been skewed.

   i. Execute the following statement to check whether the storage space is skewed. The principle of this method is similar to that of the preceding space-viewing method:

   ```
   SELECT * FROM gp_toolkit.gp_skew_coefficients
   ```

   You can use the view to check the data volume of rows in a table. The larger the table, the more time it will take for the check to complete.

   ii. Use the gp_toolkit.gp_skew_idle_fractions view to calculate the percentage of idle system resources during a table scan to check whether the data is skewed:

   ```
   SELECT * FROM gp_toolkit.gp_skew_idle_fractions
   ```

9.8.3.2. Execute VACUUM and ANALYZE statements

You can execute `VACUUM` and `ANALYZE` statements on a regular basis for frequently updated tables and databases. You can also execute `VACUUM` and `ANALYZE` statements after you have performed a large number of update or write operations to prevent the operations from consuming excessive resources and storage space.

9.8.4. Security maintenance

9.8.4.1. Network security maintenance

Regular maintenance will help ensure the security of networks and devices.

Device security

Check network devices and enable the security management protocols and configurations for the devices you want to secure. Check for up-to-date versions of network device software and update the software to more secure versions in a timely manner. For more information about security maintenance methods, see the product documentation of each device.

Network security

You can select the intrusion detection system (IDS) or intrusion prevention system (IPS) based on the network status to check public and internal traffic, and defend the network against abnormal behaviors and attacks.

9.8.4.2. Account password maintenance

Account passwords include the superuser password of AnalyticDB for PostgreSQL and the password of the host operating system.

To ensure account security, use complex passwords and periodically change the passwords of systems and devices.

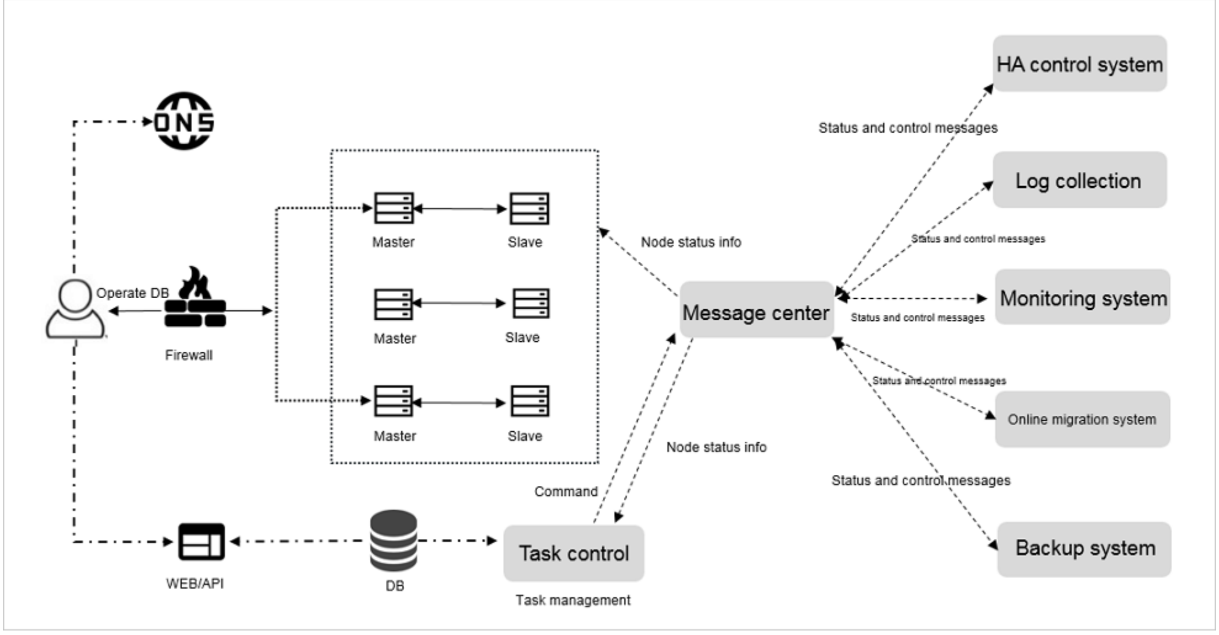
9.9. KVStore for Redis

9.9.1. O&M tool

The Apsara Uni-manager Operations Console is of the Apsara Stack unified intelligent operation and maintenance (O&M) platform. The platform provides the following features to manage ApsaraDB for Redis instances:

- Instance management: allows you to view instance details, instance logs, and user information.
- Host management: allows you to view and manage hosts.

9.9.2. Architecture diagram



9.9.3. Log on to the Apsara Uni-manager Operations Console

This topic describes how to log on to the Apsara Uni-manager Operations Console.

Prerequisites

- The URL, username, and password that are required to log on to the Apsara Uni-manager Operations Console are obtained from the deployment personnel or administrators.

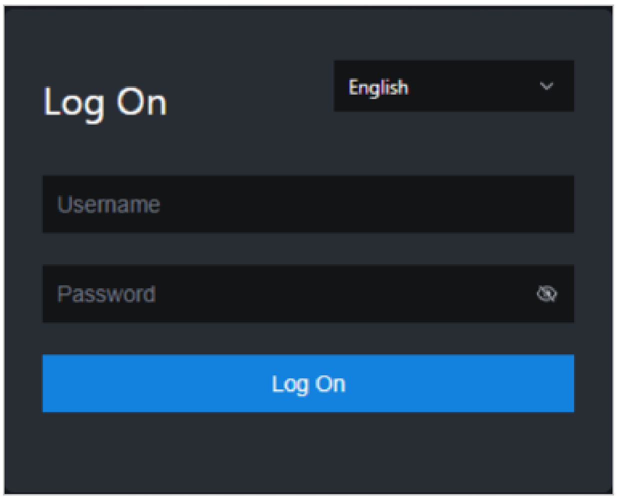
  The URL of the Apsara Uni-manager Operations Console is in the format of *region-id*.ops.console.*intranet-domain-id*.

- A browser is available. We recommend that you use Google Chrome.

Procedure

i. Open your browser.

ii. In the address bar, enter the URL. Then, press the Enter key.



> Note You can select a language from the drop-down list in the upper-right corner of the page.

iii. Enter your username and password.

> Note To obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console, contact the deployment personnel or administrators.

If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username as prompted.

To enhance security, make sure that the password meets the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password is 10 to 20 characters in length.

iv. Click **Log On**.

9.9.4. Manage ApsaraDB for Redis instances

This topic describes how to manage ApsaraDB for Redis instances. You can view instance details, logs, and user information.

Procedure

1. Log on to the Apsara Uni-manager Operations Console.
2. On the **Instance Management** tab of the **RDS** page, you can perform the following operations:
   - View the list of instances.

     On the **Instance Management** tab, you can view the instances under your account.

- Query the details of an instance

  Click the ID of a specific instance to view the details of the instance.

- **User Information**

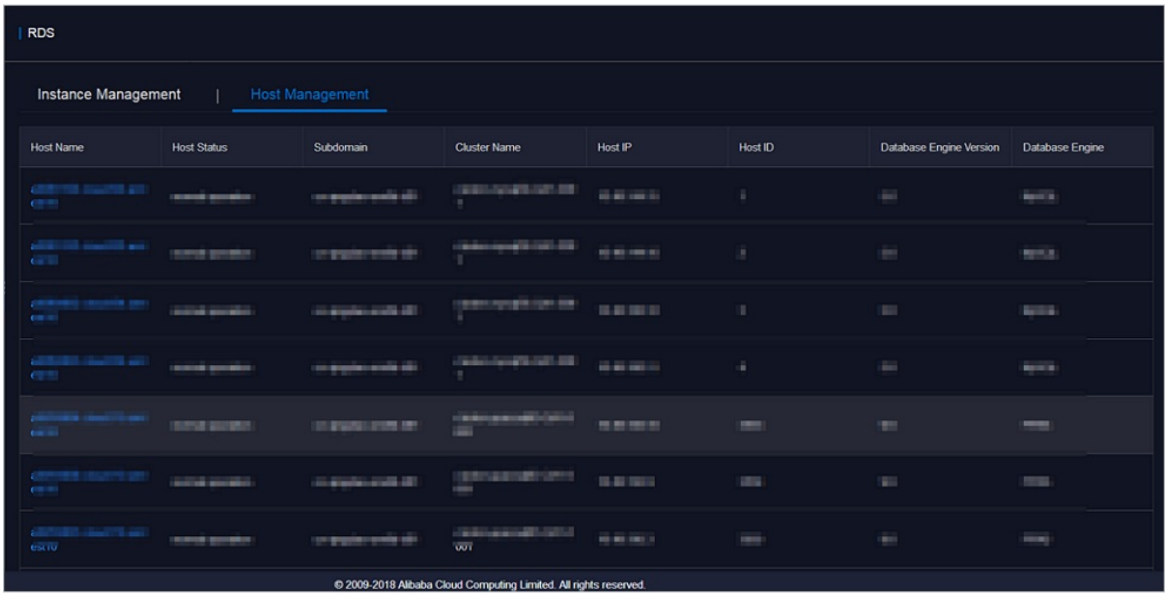
  Click **User Information** in the **Actions** column.

9.9.5. Manage hosts

You can view and manage hosts.

Procedure

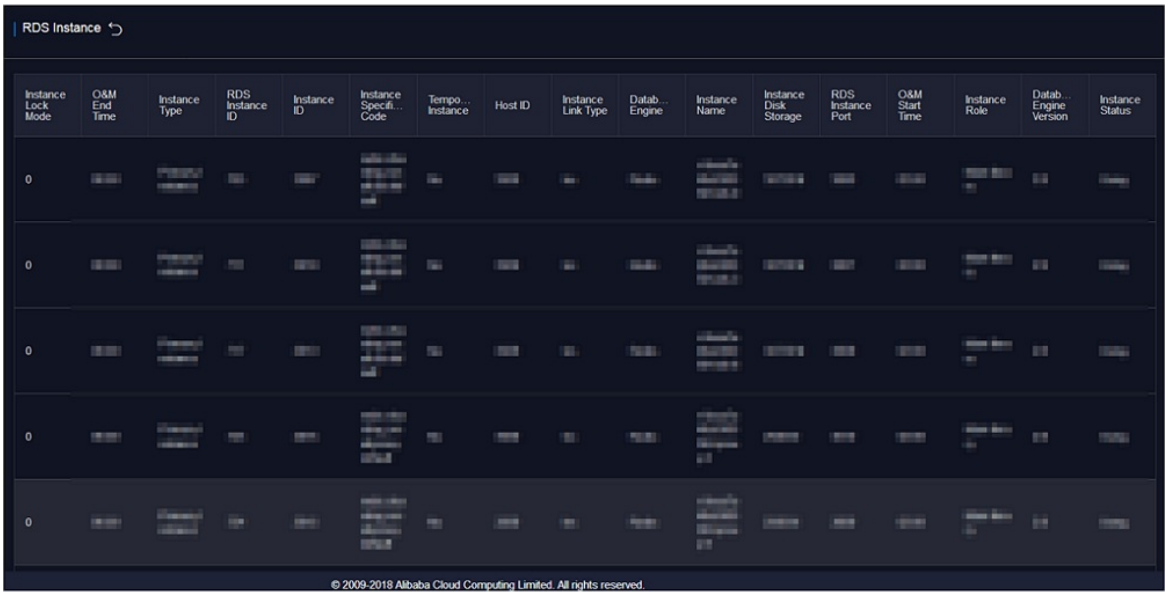
1. Log on to the Apsara Uni-manager Operations Console.
2. On the **Host Management** tab of the **RDS** page, you can view information of all hosts.



Host Name	Host Status	Subdomain	Cluster Name	Host IP	Host ID	Database Engine Version	Database Engine
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

© 2009-2018 Alibaba Cloud Computing Limited. All rights reserved.

3. Click a hostname to go to the **RDS Instance** page. You can view all instances on this host.



Instance Lock Mode	O&M End Time	Instance Type	RDS Instance ID	Instance ID	Instance Specifi... Code	Tempo... Instance	Host ID	Instance Link Type	Datab... Engine	Instance Name	Instance Disk Storage	RDS Instance Port	O&M Start Time	Instance Role	Datab... Engine Version	Instance Status
0	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
0	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
0	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
0	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
0	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

© 2009-2018 Alibaba Cloud Computing Limited. All rights reserved.

9.9.6. Security maintenance

9.9.6.1. Network security maintenance

Network security maintenance involves device security and network security.

Device security

Check network devices, and enable security management protocols and configurations for these devices.

Check software versions of network devices and update them to more secure versions in time.

For more information about security maintenance methods, see documents of related devices.

Network security

Based on your network conditions, select the intrusion detection system (IDS) or intrusion prevention system (IPS) to detect abnormal Internet and intranet traffic and protect against abnormal behavior and attacks in real time.

9.9.6.2. Password maintenance

Passwords include system passwords and device passwords in KVStore for Redis.

To secure your account, you must periodically change the system and device passwords, and use complex passwords.

9.10. ApsaraDB for MongoDB

9.10.1. Service architecture

9.10.1.1. System architecture

9.10.1.1.1. Backup system

Automatic backup

ApsaraDB for MongoDB supports both physical backup and logical backup.

You can flexibly configure the backup start time based on the service off-peak hours. All backup files are retained for seven days.

Temporary backup

You can initiate a temporary backup as required. The backup files are retained for seven days.

Log management

ApsaraDB for MongoDB generates operation logs and allows you to download them. You can use the operation logs for local incremental backup.

Data backtracking

ApsaraDB for MongoDB can use backup files and logs to generate a temporary instance for any time point within the past seven days. After verifying that the data in the temporary instance is correct, you can use the temporary instance to restore data to the specified time point.

Creating a temporary instance does not affect the running of the current instance.

Only one temporary instance can be created for each ApsaraDB for MongoDB instance at a time. A temporary instance is valid for 48 hours. You can create a maximum of 10 temporary instances for an ApsaraDB for MongoDB instance each day.

9.10.1.1.2. Data migration system

Database replication between instances

ApsaraDB for MongoDB allows you to easily migrate databases from one instance to another.

Data migration to or from ApsaraDB for MongoDB

ApsaraDB for MongoDB provides a professional tool and a migration wizard to help you migrate data to or from ApsaraDB for MongoDB.

Backup file download

ApsaraDB for MongoDB retains backup files for seven days. During this period, you can log on to the ApsaraDB for MongoDB console to download the backup files.

9.10.1.1.3. Monitoring system

Performance monitoring

ApsaraDB for MongoDB provides nearly 20 metrics for monitoring system performance, such as the disk capacity, IOPS, number of connections, CPU utilization, network traffic, transactions per second (TPS), queries per second (QPS), and cache hit rate. You can obtain such status information for an ApsaraDB for MongoDB instance within the past one year.

SQL auditing

The system records SQL statements and additional information sent to ApsaraDB for MongoDB instances, such as the IP addresses of connections, database names, access accounts, execution time, and number of records returned. You can use SQL auditing to locate problems and check instance security.

Threshold alerting

ApsaraDB for MongoDB provides short message service (SMS) notifications to indicate status or performance exceptions that occur in ApsaraDB for MongoDB instances.

These exceptions include instance locking, disk capacity, IOPS, connection quantity, and CPU exceptions. You can configure alert thresholds and up to 50 alert recipients (of which five are effective at a time). If a metric of an ApsaraDB for MongoDB instance exceeds a specific threshold, an SMS notification is sent to alert the recipients.

Web operation logging

The system logs all modification operations in the ApsaraDB for MongoDB console for administrators to check. These logs are retained for a maximum of 30 days.

9.10.1.1.4. Control system

If a host or an instance crashes, the ApsaraDB for MongoDB high-availability (HA) component fails services over within 30 seconds after the exception is detected. This guarantees that applications run properly and ApsaraDB for MongoDB is highly available.

9.10.1.1.5. Task scheduling system

You can use the ApsaraDB for MongoDB console or APIs to create or delete instances or switch instances between the intranet and Internet. All instance operations are scheduled, traced, and displayed as tasks.

9.10.2. ApsaraDB for MongoDB O&M overview

The Apsara Uni-manager Operations Console provides the following O&M features for ApsaraDB for MongoDB:

- Instance management: allows you to view instance details, instance logs, and user information.
- Host management: allows you to view and manage hosts.

9.10.3. Log on to the Apsara Uni-manager Operations Console

This topic describes how to log on to the Apsara Uni-manager Operations Console.

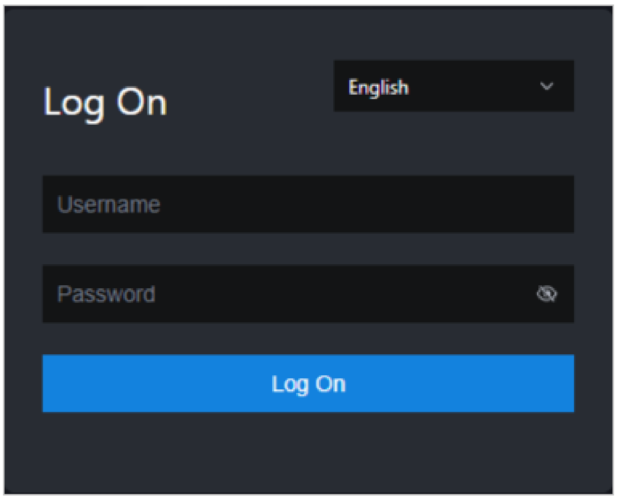
Prerequisites

- The URL, username, and password that are required to log on to the Apsara Uni-manager Operations Console are obtained from the deployment personnel or administrators.

  The URL of the Apsara Uni-manager Operations Console is in the format of *region-id*.ops.console.*intranet-domain-id*.
- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL. Then, press the Enter key.



> Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

> Note To obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console, contact the deployment personnel or administrators.

If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username as prompted.

To enhance security, make sure that the password meets the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password is 10 to 20 characters in length.

4. Click **Log On**.

9.10.4. Security maintenance

9.10.4.1. Network security maintenance

Network security maintenance is aimed at ensuring device security and network security.

Device security

Check network devices, and enable security management protocols and configurations of devices.

Check for up-to-date versions of network device software and update the software to more secure versions in a timely manner.

For more information about the security maintenance method, see the product document of each device.

Network security

Select the intrusion detection system (IDS) or intrusion prevention system (IPS) based on the network status to check Internet and intranet traffic and defend the network against abnormal behaviors and attacks.

9.10.4.2. Account password maintenance

Account passwords include the ApsaraDB for MongoDB system and device passwords.

To ensure account security, change the system and device passwords periodically, and use passwords that meet the complexity requirements.

9.11. ApsaraDB for OceanBase

9.11.1. Overview

Purpose

This document is a guide for you to perform operations and maintenance (O&M) tasks such as routine inspections, monitoring, and maintenance on ApsaraDB for OceanBase clusters. These tasks ensure the long-term stable running of the system.

You can follow the instructions in this guide to handle the issues that are identified during the maintenance. If you encounter system issues that are not covered in this guide, contact technical support.

Requirements

You must acquire IT skills, including knowledge for computer networks, knowledge for computer operations, issue analysis, and troubleshooting. You must pass the pre-job training to learn the knowledge for the Apsara Stack system. The required knowledge for the system includes, but is not limited to, system principles, networking, features, and the usage of maintenance tools.

Note that during maintenance, you must comply with operation procedures to ensure personal safety and system security. User data must be kept strictly confidential and must not be copied or disseminated without the written consent of the users.

Introduction to O&M commands and tools

Apsara Stack Operations console for ApsaraDB for OceanBase

The Apsara Stack Operations console for ApsaraDB for OceanBase is a cloud management platform for ApsaraDB for OceanBase. ApsaraDB for OceanBase is a financial-grade distributed relational database service. The console provides a wide range of modules that allow you to implement various features. For example, you can use the modules to manage resources, capacities, clusters, and instance lifecycles. You can also use the modules to monitor performance based on real-time computing and to implement API-related features. These modules provide ApsaraDB for OceanBase cloud services and simplify O&M operations.

Considerations

To ensure a stable system and avoid unexpected events, you must follow these guidelines:

- Hierarchical permission management

O&M engineers are granted with only the network, device, system, and data permissions that are required to fulfill their duties. This prevents system faults that are caused by unauthorized operations.

- System security

  Before you perform operations on the system, you must be aware of the impacts of the operations on the system. This ensures that the system is not affected by the high-risk operations. You must record the details about the issues that you encounter during the operations for issue analysis and troubleshooting.

- Personal safety and data security
  - You must take safety measures to ensure personal safety based on device manuals when you use electrical equipment.
  - You must use secure devices to access the business network.
  - Unauthorized data replication and dissemination are prohibited.

Technical support

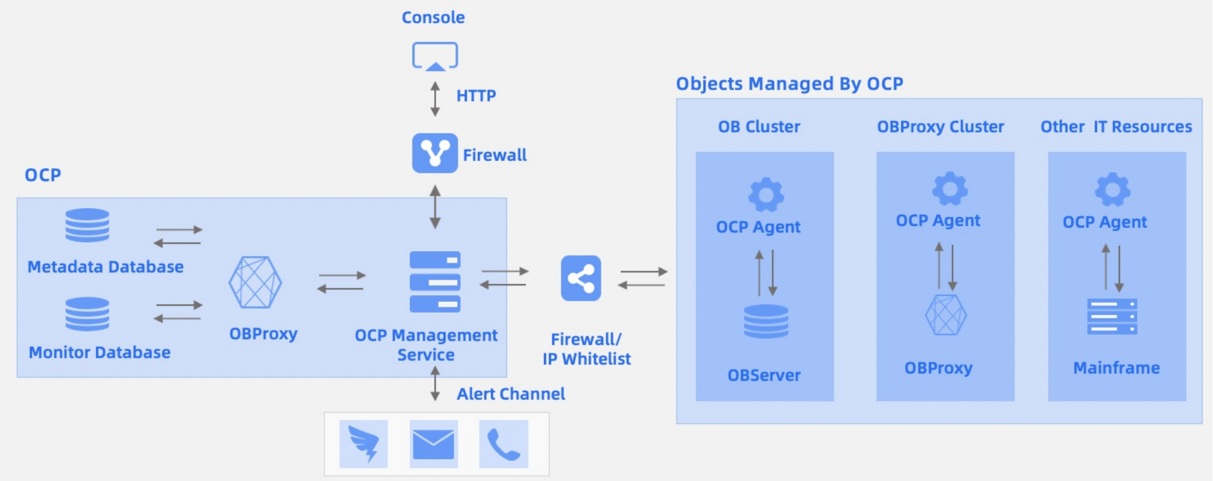
You can contact technical support for help during the maintenance.

9.11.2. Architecture

9.11.2.1. Architecture

OceanBase Cloud Platform (OCP) has the following five modules: Management Agent, Management Service, Metadata Repository, Management Console, and OBProxy.

The following figure shows the system architecture of OCP.



The system consists of the following five modules:

- Management Agent

Management agents are installed on each host that is monitored in the computing environment. The monitored hosts include physical hosts and virtual hosts. These agent programs are deployed and upgraded in a unified manner by using OCP. They are used to control the startup and shutdown of hosts, remotely execute tasks, and collect metrics. Then, the Management Agent module provides the details of availability, metrics, and task status to the Management Service module of OCP.

- Management Service

This module is a large Java-based application. Management Service integrates with the Management Agent and Metadata Repository modules to collect and store the data of related remote hosts. Management Service also communicates with ApsaraDB for OceanBase clusters. This allows you to remotely execute O&amp;M commands to manage the related clusters.

- Metadata Repository

Metadata Repository is also known as metadatabase or MetaDB. It stores all data that is collected by management agents. Metadata Repository stores the information of hosts, database clusters, tenants, database instances, database users, scheduling tasks, and software versions.

Before you install OCP, a metadata repository must be available.

- Management Console

The management console provides a web interface. This allows you to access, monitor, and manage all database clusters. The management console also provides data dashboards. You can view important information after you log on to the management console.

- OBProxy

An OBProxy is a proxy that you can use to connect to ApsaraDB for OceanBase. OCP management programs send requests to databases, and OBProxies send the routes of the requests to Apsara Stack clusters. Then, OBProxies send the returned information to Management Service of OCP.

9.11.2.2. Deployment solutions

9.11.2.2.1. Create a cluster

You can create a cluster based on your business requirements.

Prerequisites

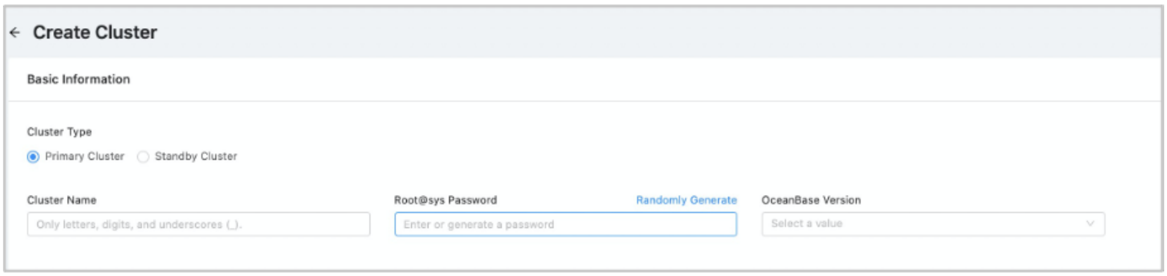
You are authorized to perform the Create Cluster operation.

Procedure

1. Log on to OceanBase Cloud Platform (OCP), find the entry of Create Cluster based on the actual business scenario.

   - If you do not have a cluster, a message appears on the **Cluster Overview** page. In the message that appears, click **Create Cluster**.
   - If you have clusters, click **Create Cluster** in the upper-right corner of the **Cluster Overview** page.

2. On the **Create Cluster** page, set the required parameters in the Basic Information section.



← Create Cluster

Basic Information

Cluster Type

● Primary Cluster ○ Standby Cluster

Cluster Name	Root@sys Password (Randomly Generate)	OceanBase Version
Only letters, digits, and underscores (_).	Enter or generate a password	Select a value

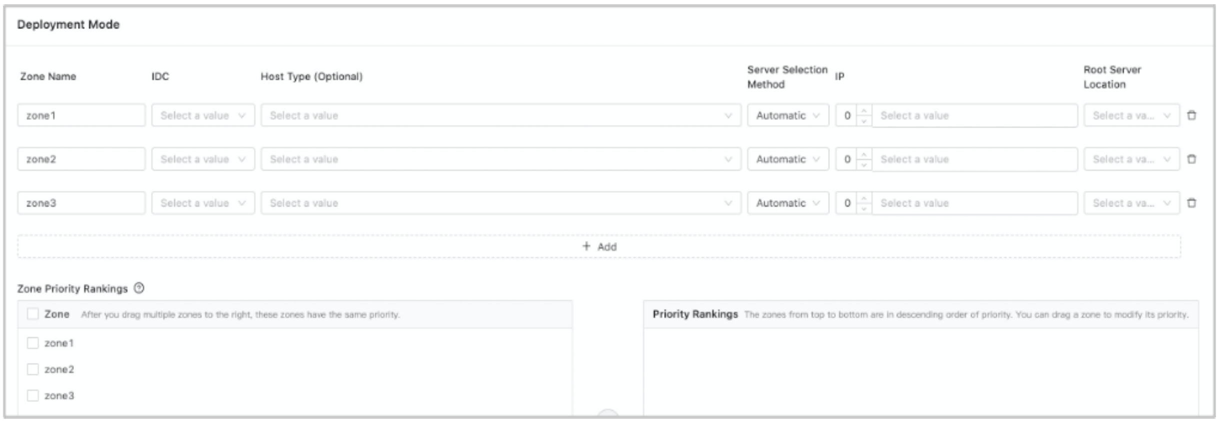
The following table describes the parameters.

Parameter	Description
Cluster Type	Valid values: **Primary Cluster** and **Standby Cluster**. If you select **Standby Cluster**, you must make sure that you have an existing primary cluster.
Cluster Name	The name of the cluster to be managed. The cluster name must be 2 to 48 characters in length and can contain letters, digits, and underscores (_). It must start with a letter.
Root@sys Password	You can enter or randomly generate a password. The password must meet the following requirements: ● The length ranges from 8 bits to 32 bits. ● At least two numbers, two uppercase letters, two lowercase letters, and two special characters are included. The following special characters are supported: ._+@#$%)
OceanBase Version	You can select an existing OceanBase version from the drop-down list. You can also click **Add Version** in the lower part of the list to upload an OceanBase version.

3. Set the required parameters in the Deployment Mode section.

By default, three zones are added. If you want to deploy a cluster with more than three zones, you can click **Add** to add a zone.

If you want to deploy less than three zones in a cluster, you can click the delete icon of a zone.



Deployment Mode

Zone Name	IDC	Host Type (Optional)	Server Selection Method	IP		Root Server Location
zone1	Select a value	Select a value	Automatic	0	Select a value	Select a va...
zone2	Select a value	Select a value	Automatic	0	Select a value	Select a va...
zone3	Select a value	Select a value	Automatic	0	Select a value	Select a va...

Zone Priority Rankings

□ Zone After you drag multiple zones to the right, these zones have the same priority.

□ zone1
□ zone2
□ zone3

Priority Rankings The zones from top to bottom are in descending order of priority. You can drag a zone to modify its priority.

The following table describes the required parameters of a zone.

Parameter	Description
Zone Name	You can use the default name or customize a name. The zone name must be 2 to 962 characters in length and can contain letters, digits, and underscores (_). It must start with a letter.
IDC	The data center where the zone resides. Zones must be deployed in the same data center.
Host Type (Optional)	Optional. If you select a host type, the host list is filtered based on the selected host type.
Server Selection Method	Valid values: **Automatic** and **Manual**.
IP	You can select multiple IP addresses. If you set **Machine Selection Method** to **Automatic**, you only need to enter the number of hosts. Then, OCP automatically selects the corresponding number of available hosts. If you set **Machine Selection Method** to **Manual**, you must select several IP addresses from the list.
Root Server Location	You can select an IP address as the host where the root server resides.

Parameter	Description
Zone Priority Rankings	The priority rankings of the zones. The rankings indicate the distribution priority of partition replicas in the tenant. The left-side list box displays all zones of the current cluster. You can select one or more zones from the left-side list box and add them to the right-side list box. By default, the zones that are selected earlier have a higher priority than the zones that are selected later. Multiple zones that are selected at a time have the same priority. After selected zones are added to the right-side list box, you can modify the order by dragging the zones. The zones in the higher part of the list have a higher priority.

4. Click **Submit**.
5. In the **Confirm Information** dialog box, verify your settings, and then click **OK**.

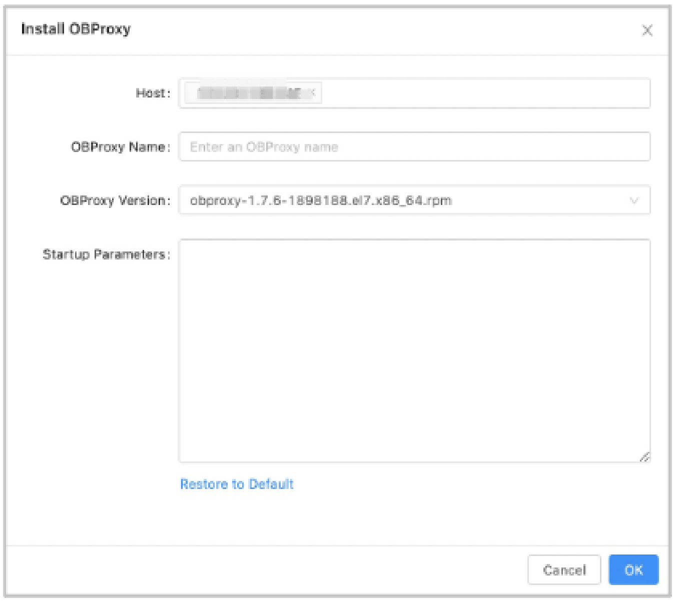
9.11.2.2.2. Install OBProxy

In the upper-right corner of the page, click Return to Old Version to go to the OBProxy page and install OBProxy.

Procedure

1. In the navigation pane, choose **Maintenance** to go to the **OBProxy** page.
2. Click **Install OBProxy**.

3. In the dialog box that appears, specify the following parameters:



Install OBProxy

Host: [redacted]

OBProxy Name: Enter an OBProxy name

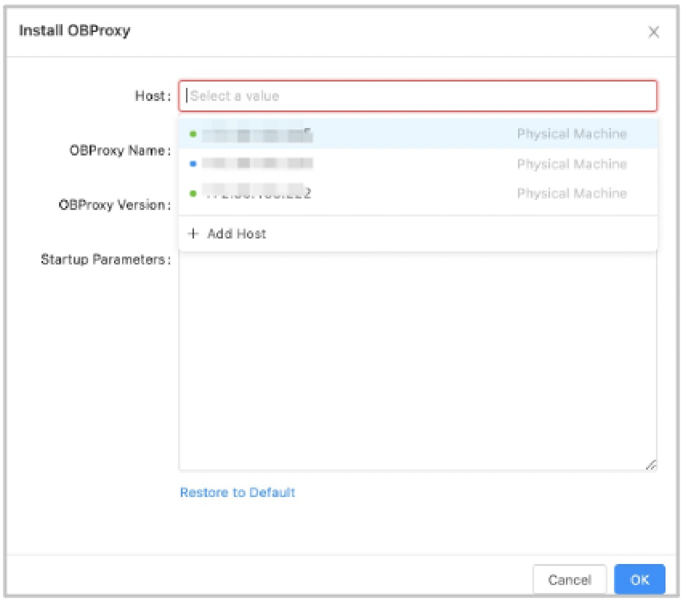
OBProxy Version: obproxy-1.7.6-1898188.el7.x86_64.rpm

Startup Parameters:

Restore to Default

Cancel OK

- **Host**: Select a host from the drop-down list, or click **Add Host** to add a new host.



Install OBProxy

Host: Select a value

- ● [redacted] Physical Machine
- ● [redacted] Physical Machine
- ● [redacted] Physical Machine
- + Add Host

OBProxy Name:

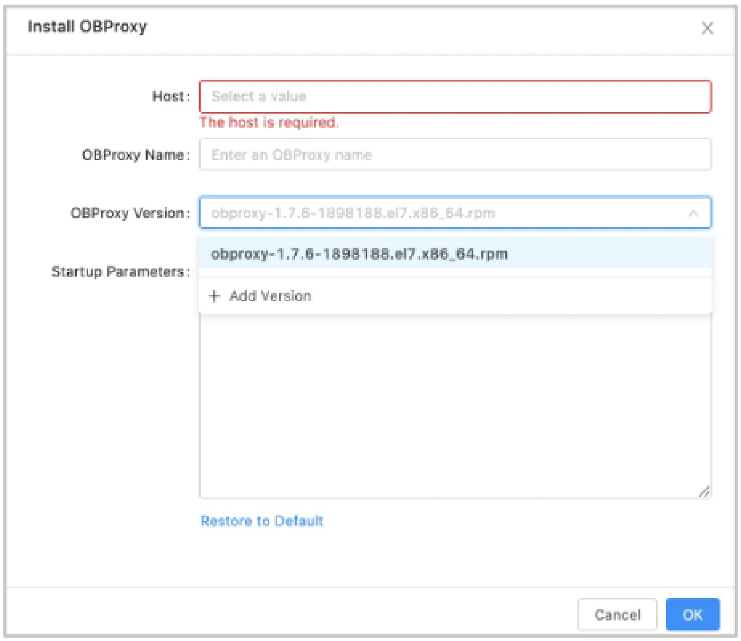
OBProxy Version:

Startup Parameters:

Restore to Default

Cancel OK

- OBProxy Version: Select an OBProxy version from the drop-down list, or click **Add Version** and click **Upload** in the dialog box that appears, to upload the corresponding OBProxy file.



Install OBProxy

Host: Select a value

The host is required.

OBProxy Name: Enter an OBProxy name

OBProxy Version: obproxy-1.7.6-1898188.el7.x86_64.rpm

obproxy-1.7.6-1898188.el7.x86_64.rpm

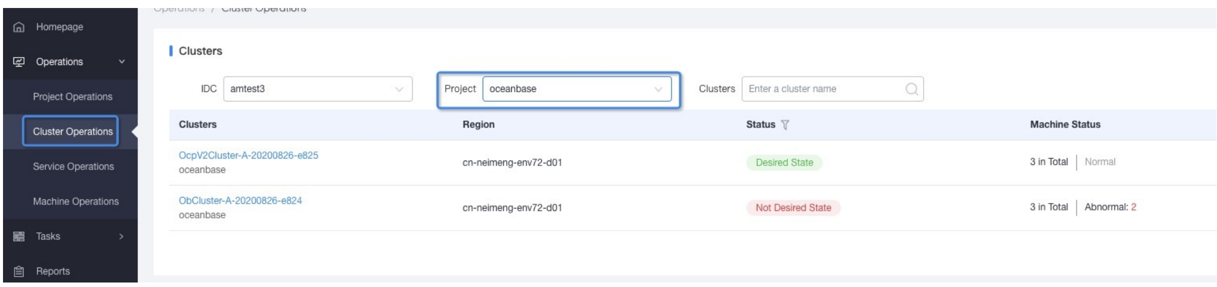
Startup Parameters:

4. Click **OK**. This will generate an OBProxy operations task. You can choose **System Management > Tasks** to check the installation progress.

9.11.2.3. OCP V2.0 components and their features

9.11.2.3.1. Components and their features

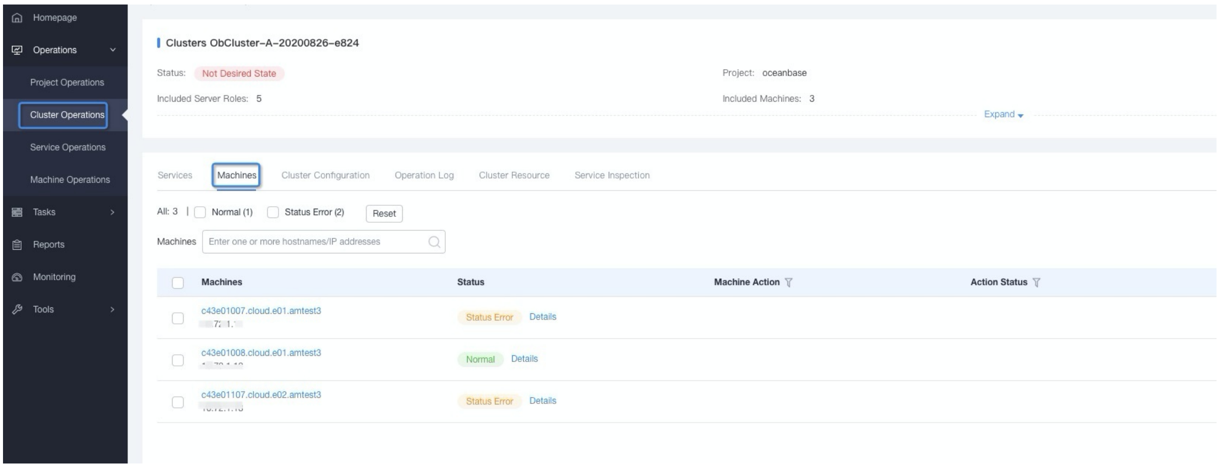
ApsaraDB for OceanBase consists of database nodes and a management node. The database nodes are OBServers that are deployed on multiple physical servers. The management node is OceanBase Cloud Platform (OCP). The management components of OCP V2.0 are deployed as Docker containers on physical servers. You can obtain the information about each server from the Apsara Infrastructure Management Framework portal, such as hosts and IP addresses.



Clusters

IDC: amtest3 | Project: oceanbase | Clusters: Enter a cluster name

Clusters	Region	Status	Machine Status
OcpV2Cluster-A-20200826-e825 oceanbase	cn-neimeng-env72-d01	Desired State	3 in Total | Normal
ObCluster-A-20200826-e824 oceanbase	cn-neimeng-env72-d01	Not Desired State	3 in Total | Abnormal: 2



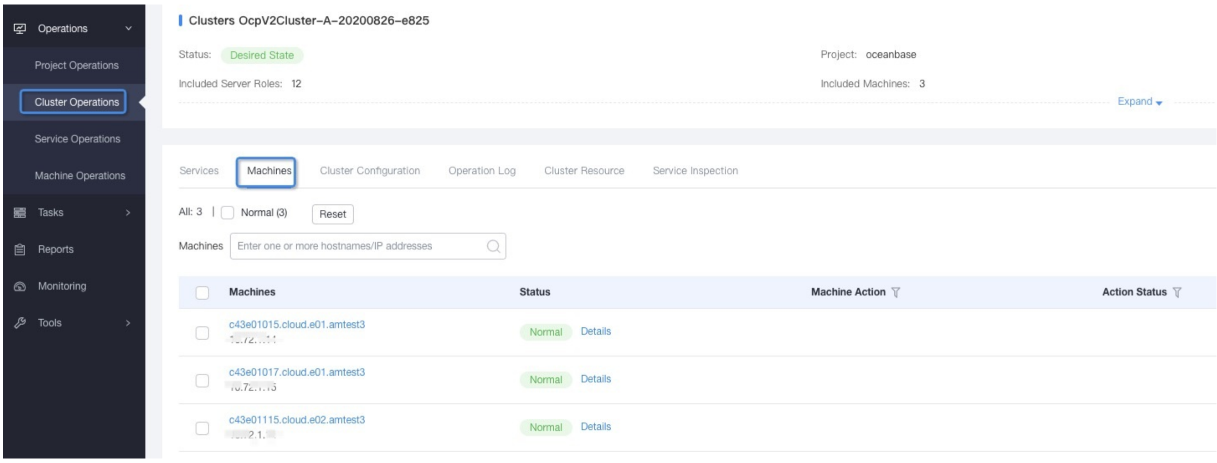
Clusters ObCluster-A-20200826-e824

Status: Not Desired State
Project: oceanbase
Included Server Roles: 5
Included Machines: 3

All: 3 | □ Normal (1) □ Status Error (2)

Machines: Enter one or more hostnames/IP addresses

□	Machines	Status	Machine Action	Action Status
□	c43e01007.cloud.e01.amtest3 [redacted]	Status Error Details		
□	c43e01008.cloud.e01.amtest3 [redacted]	Normal Details		
□	c43e01107.cloud.e02.amtest3 [redacted]	Status Error Details		



Clusters OcpV2Cluster-A-20200826-e825

Status: Desired State
Project: oceanbase
Included Server Roles: 12
Included Machines: 3

All: 3 | □ Normal (3)

Machines: Enter one or more hostnames/IP addresses

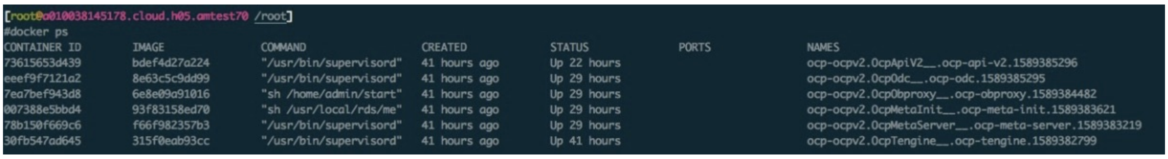
□	Machines	Status	Machine Action	Action Status
□	c43e01015.cloud.e01.amtest3 [redacted]	Normal Details		
□	c43e01017.cloud.e01.amtest3 [redacted]	Normal Details		
□	c43e01115.cloud.e02.amtest3 [redacted]	Normal Details		

OCP V2.0 consists of the testimage component and the following feature components: OcpMetaServer, OcpMetaInit, OcpObproxy, OcpApiV2, OcpOdc, and OcpTengine. The testimage component is used for automated tests. Each component is deployed as a Docker container.

You can run the commands in the following steps to manage Docker containers:

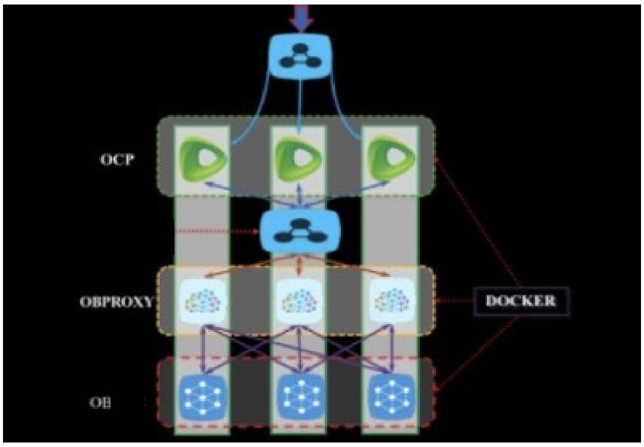
1. Log on to your server of Apsara Stack.
2. Log on to the physical server of OCP V2.0 over Secure Shell (SSH).
3. Run the following command to view all the processes of the components: docker ps.
4. Run the following command to view the logs of a Docker container: docker logs ${containerID}. The logs record the information about the startup and running of the container.

5. Run the following command to go to a Docker container: docker exec -ti ${containerID} bash.
6. Run the following command to restart a Docker container: docker restart ${containerID}.



```
[root@a010038145178.cloud.h05.amtest70 /root]
#docker ps
CONTAINER ID       IMAGE              COMMAND                 CREATED           STATUS             PORTS              NAMES
73615653d439       bdef4d27a224       "/usr/bin/supervisord"  41 hours ago      Up 22 hours                           ocp-ocpv2.OcpApiV2__.ocp-api-v2.1589385296
eeef9f7121a2       8e63c5c9dd99       "/usr/bin/supervisord"  41 hours ago      Up 29 hours                           ocp-ocpv2.OcpOdc__.ocp-odc.1589385295
7ea7bef943d8       6e8e09a91016       "sh /home/admin/start"  41 hours ago      Up 29 hours                           ocp-ocpv2.OcpObproxy__.ocp-obproxy.1589384482
007388e5bbd4       93f83158ed70       "sh /usr/local/rds/me"  41 hours ago      Up 29 hours                           ocp-ocpv2.OcpMetaInit__.ocp-meta-init.1589383621
78b150f669c6       f66f982357b3       "/usr/bin/supervisord"  41 hours ago      Up 29 hours                           ocp-ocpv2.OcpMetaServer__.ocp-meta-server.1589383219
30fb547ad645       315f0eab93cc       "/usr/bin/supervisord"  41 hours ago      Up 41 hours                           ocp-ocpv2.OcpTengine__.ocp-tengine.1589382799
```

OCP V2.0 architecture



9.11.2.3.2. OcpMetaServer

Feature description

This component functions as a metadatabase of the management components and tools for ApsaraDB for OceanBase. You can create an ApsaraDB for OceanBase cluster where three nodes and three replicas are deployed. This cluster can be used to provide metadatabase services.

Related commands

Command	Description	Impact
ps -ef | grep observer | grep -v grep	Views the OBServer process.	None.
su - admin -c "cd /home/admin/oceanbase; ulimit -s 10240; ulimit -c unlimited; LD_LIBRARY_PATH=/home/admin/oceanbase/lib:/usr/local/lib:/usr/lib:/usr/lib64:/usr/local/lib64: LD_PRELOAD="" /home/admin/oceanbase/bin/observer"	Starts the OBServer process.	An error occurs if the OBServer process already exists.
tail -f /home/admin/oceanbase/log/observer.log	Views the OBServer log.	None.
ps -ef | grep -E "ob_[a]gent|obstat" | grep -v grep | grep -v observer	Views the OBAgent process.	None.

Command	Description	Impact
/home/admin/obztools_agent/ob_agent.py stop agent -f	Stops the OBAgent service.	Stops monitoring ApsaraDB for OceanBase clusters and generating cluster alerts.
/home/admin/obztools_agent/ob_agent.py start agent	Starts the OBAgent service.	None.
tail -f /home/admin/obztools_agent/log/*.log	Views the OBAgent log.	None.

9.11.2.3.3. OcpMetaInit

Feature description

You can use this ApsaraDB for OceanBase component to initialize the clusters in the metadatabase, modify system parameters, and create metadata tenants that are required to provide services.

9.11.2.3.4. OcpObproxy

Feature description

This component functions as the OBProxy that you can use to access the metadata in the metadatabase clusters of ApsaraDB for OceanBase.

Related commands

Command	Description	Impact
ps -ef | grep obproxy | grep -v grep	Views the OBProxy process.	None
cd /home/admin/obproxy && ./bin/obproxy	Starts the OBProxy process.	None
tail -f /home/admin/obproxy/log/obproxy. *.log	Views the OBProxy log.	None

9.11.2.3.5. OcpApiV2

Feature description

This component is a service node of ApsaraDB for OceanBase OCP V2.0. The component provides features such as service management, O&M, monitoring, alerting, and backup and restoration.

Related commands

Command	Description	Impact
ps -ef | grep ocp-server.jar | grep -v grep	Views the process of the OCP server.	None
tail -f /home/admin/logs/ocp/ocp.*.log	Views the log of the OCP server.	None
ps -ef | grep -E "ob_|monitor" | grep -v grep	Views the process that collects monitoring data in OCP.	None
tail -f /home/admin/obztools_agent/log/*.log	Views the log that records the collected monitoring data in OCP.	None

9.11.2.3.6. OcpTengine

Feature description

This component functions as a frontend reverse proxy for the management components and tools of ApsaraDB for OceanBase. The component provides HTTPS proxy services.

Related commands

Command	Description	Impact
ps -ef | grep nginx | grep -v grep	Views the Tengine process.	None.
/opt/taobao/tengine/bin/tengine -c /opt/taobao/tengine/conf/nginx_https_sm.conf	Starts the Tengine process.	An error occurs if the Tengine process already exists.
tail -f /home/admin/logs/access.*.log tail -f /home/admin/logs/error.*.log	Views the log of the Tengine process.	None.

9.11.3. Routine maintenance

9.11.3.1. Log on to the ApsaraDB for OceanBase O&M console

This topic describes how to use the Apsara Uni-manager Operations Console to log on to the ApsaraDB for OceanBase O&M console. The Google Chrome browser is used in an example in this topic.

Prerequisites

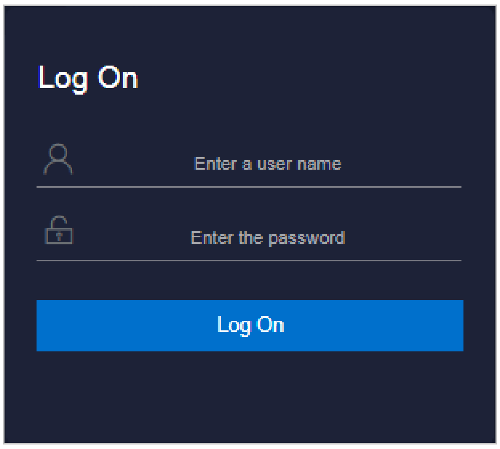
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. In the address bar, enter the URL *region-id*.aso.*intranet-domain-id*.com and press the Enter key.



> Note You can select a language from the drop-down list in the upper-right corner of the page.

2. Enter your username and password.

> Note Obtain the username and password for logging on to the ASO console from the deployment personnel or an administrator.

When you log on to the ASO console for the first time, you must change the password of your username as prompted.

To enhance security, a password must meet the following requirements:

- It must contain uppercase and lowercase letters.
- It must contain digits.
- It must contain special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- It must be 10 to 20 characters in length.

3. Click **Log On** to go to the **ASO** console.

4. In the left-side navigation pane, click **Product Management**. Then, choose **Products > Database Services** and click **OceanBase Cloud Platform**. You are directed to the ApsaraDB for OceanBase O&M console.

9.11.3.2. View performance metrics

9.11.3.2.1. Description of performance metrics

In ApsaraDB for OceanBase, network packets are divided into two types. The network packets of one type are transferred over a remote procedure call (RPC) protocol. The RPC protocol is used as an internal communication protocol in ApsaraDB for OceanBase. The network packets of the other type are used to send SQL requests and are transferred over the MySQL protocol. The statistics about the two types of network packets are collected in a separate way.

In an OBServer, multiple queues are used to process different requests. After the OBServer receives network packets, the server sends the packets to the relevant queues.

Performance metric	Description
QPS	The number of SELECT executions per second.
TPS	The number of INSERT, REPLACE, UPDATE, and DELETE executions per second.
ACTIVE_SESSION	The number of active connections.
QPS_RT	The execution time of the SELECT statements. The statistics are collected in real time.
TPS_RT	The average execution time of each transaction.
SQL_DISTRIBUTED_COUNT	The number of executions for distributed SQL statements.
SQL_LOCAL_COUNT	The number of executions for the SQL statements that are executed in the on-premises environment.
SQL_REMOTE_COUNT	The number of executions for the SQL statements that are executed in the remote environment.
INNER_SQL_CONNECTION_EXECUTE_COUNT	The number of executions for the SQL requests that are sent over the RPC protocol.
INNER_SQL_ CONNECTION_EXECUTE_RT	The execution time of the SQL requests that are sent over the RPC protocol.
BLOCK_CACHE_HIT_PERCENT	The cache hit percentage for the block cache.
BLOCK_INDEX_CACHE_HIT_PERCENT	The cache hit percentage for the block index cache.
BLOOM_FILTER_CACHE_HIT_PERCENT	The cache hit percentage for the Bloom filter cache.
BLOOM_FILTER_FILT_PERCENT	The cache interception percentage for the Bloom filter cache.
CLOG_CACHE_HIT_PERCENT	The cache hit percentage for the commit log cache.
LOCATION_CACHE_HIT_PERCENT	The cache hit percentage for the location cache.
LOCATION_CACHE_PROXY_HIT_PERCENT	The cache hit percentage for the OBProxy location cache.
PLAN_CACHE_HIT_RATE	The cache hit percentage for the SQL plan cache.

Performance metric	Description
ROW_CACHE_HIT_PERCENT	The cache hit percentage for the row cache.
MYSQL_PACKET_IN	The number of the received MySQL requests.
MYSQL_PACKET_OUT	The number of the delivered MySQL requests.
MYSQL_PACKET_IN_BYTES	The number of bytes in the received MySQL request.
MYSQL_PACKET_OUT_BYTES	The number of bytes in the delivered MySQL request.
MYSQL_DELIVER_FAIL	The number of MySQL requests that failed to be delivered.
RPC_DELIVER_FAIL	The number of RPC requests that failed to be delivered.
RPC_PACKET_IN	The number of the received RPC requests.
RPC_PACKET_OUT	The number of the delivered RPC requests.
RPC_PACKET_IN_BYTES	The number of bytes in the received RPC request.
RPC_PACKET_OUT_BYTES	The number of bytes in the delivered RPC request.
RPC_NET_FRAME_RT	The delay of an RPC network packet at the network layer. The delay is the interval between the time when the packet is received and the time when the packet is distributed to the relevant queue.
RPC_NET_RT	The delay of a network packet. The delay is the interval between the time when the packet is sent and the time when the packet is received. Note that the sending time and the receiving time are recorded on different servers. For example, if a network packet is sent from Server A to Server B, the sending time is recorded on Server A and the receiving time is recorded on Server B.
REQUEST_DEQUEUE_COUNT	The number of requests that are sent to the queue.
REQUEST_ENQUEUE_COUNT	The number of requests that are moved out of the queue.
REQUEST_QUEUE_TIME	The interval between the time when a request is received and the time when the request starts to be processed.
TRANS_COMMIT_LOG_SYNC_COUNT	The number of commit logs for the transaction.

Performance metric	Description
TRANS_COMMT_LOG_SYNC_RT	The interval between the time when the commit logs are submitted and the time when the logs are synchronized to a majority of replicas.
TRANS_COMMT_COUNT	The number of transaction commits.
TRANS_MULTI_PARTITION_COUNT	The number of transactions that are executed across partitions.
TRANS_ROLLBACK_COUNT	The number of transaction rollbacks.
TRANS_SINGLE_PARTITION_COUNT	The number of transactions that are executed in a single partition.
TRANS_START_COUNT	The number of times that transactions are started. The number includes the number of times that the transaction is automatically committed.
TRANS_SYSTEM_TRANS_COUNT	The number of executions for system transactions. This number also indicates the number of SQL statement executions. Note that the SQL statements are executed to retrieve data from ApsaraDB for OceanBase and manage metadata in ApsaraDB for OceanBase.
TRANS_TIMEOUT_COUNT	The number of time-out transactions.
TRANS_USER_TRANS_COUNT	The number of user transactions.
TRANS_COMMIT_RT	The time that is consumed in the commit phase of the transaction.
TRANS_ROLLBACK_RT	The time that is consumed in the rollback phase of the transaction.
TRANS_RT	The total consumption time of the transaction. The time period starts from the time when the transaction starts to be performed and ends at the time when the transaction is completed.
MEMSTORE_READ_LOCK_FAIL_COUNT	The number of times that data failed to be read from the lock in the MemStore.
MEMSTORE_READ_LOCK_SUCC_COUNT	The number of times that data was read from the lock in the MemStore.
MEMSTORE_WRITE_LOCK_FAIL_COUNT	The number of times that data failed to be written to the lock in the MemStore.
MEMSTORE_WRITE_LOCK_SUCC_COUNT	The number of times that data was written to the lock in the MemStore.

Performance metric	Description
MEMSTORE_READ_LOCK_WAIT_TIME	The waiting time to read data from the lock in the MemStore.
MEMSTORE_ WRITE_LOCK_WAIT_TIME	The waiting time to write data to the lock in the MemStore.
MEMSTORE_APPLY_FAIL_COUNT	The number of times that data failed to be written to the MemStore.
MEMSTORE_ APPLY_SUCC_COUNT	The number of times that data were written to the MemStore.
MEMSTORE_GET_FAIL_COUNT	The number of times that GET queries failed to retrieve data from the MemStore.
MEMSTORE_GET_SUCC_COUNT	The number of times that GET queries retrieved data from the MemStore as expected.
MEMSTORE_SCAN_FAIL_COUNT	The number of times that scan queries failed to retrieve data from the MemStore.
MEMSTORE_SCAN_SUCC_COUNT	The number of times that scan queries retrieved data from the MemStore as expected.
MEMSTORE_APPLY_RT	The time that is consumed by writing data to the MemStore.
MEMSTORE_GET_RT	The time that is consumed by GET requests. The requests are sent to retrieve data from the MemStore.
MEMSTORE_SCAN_RT	The time that is consumed by scan query requests. The requests are sent to retrieve data from the MemStore.
MEMSTORE_ROW_COUNT	The number of rows in the MemStore.
IO_READ_COUNT	The number of data reads in the I/O operations.
IO_WRITE_COUNT	The number of data writes in the I/O operations.
IO_READ_RT	The time that is consumed by the data reads in the I/O operations.
IO_WRITE_RT	The time that is consumed by the data writes in the I/O operations.
IO_READ_SIZE	The number of bytes that are read in the I/O operations.
IO_WRITE_SIZE	The number of bytes that are written in the I/O operations.

Performance metric	Description
IO_PREFETCH_MICRO_BLOCK_COUNT	The number of micro-blocks that are pre-read in the I/O operations.
IO_PREFETCH_UNCOMPRESS_MICRO_BLOCK_COUNT	The number of uncompressed micro-blocks that are pre-read in the I/O operations.
IO_READ_MICRO_INDEX_COUNT	The number of times that the micro-block indexes are read in the I/O operations.
IO_PREFETCH_MICRO_BLOCK_SIZE	The number of bytes in the micro-blocks that are pre-read in the I/O operations.
IO_PREFETCH_UNCOMPRESS_MICRO_BLOCK_SIZE	The number of bytes in the uncompressed micro-blocks that are pre-read in the I/O operations.
IO_READ_MICRO_INDEX_SIZE	The number of bytes for the micro-block indexes that are read in the I/O operations.
PARTITION_TABLE_OPERATOR_GET_COUNT	The number of times that the partitioned table receives GET requests.
PARTITION_TABLE_OPERATOR_GET_RT	The response time of the GET requests for the partitioned table.
REFRESH_SCHEMA_COUNT	The number of times that the table schema is updated.
REFRESH_SCHEMA_RT	The time that is consumed to update the table schema.
CLOG_CB_RT	The consumption time of callbacks in the commit logs.
CLOG_COUNT	The number of commit logs.
CLOG_EVENT_RT	The number of events in the commit logs, such as takeover and revoke events.
CLOG_FLUSH_TASK	The number of tasks in the commit logs. In the tasks, the data records are flushed to disks.
CLOG_GROUP_SIZE	The statistics about the group commits in the commit logs.
CLOG_READ	The statistics about the data reads in the commit logs. Note that data is read from disks.
CLOG_RPC_RT	The statistics about the RPC requests in the commit logs.
CLOG_RT	The statistics about the response time in the commit logs.

Performance metric	Description
CLOG_SIZE	The statistics about the sizes in the commit logs.
ACTIVE_MEMSTORE_USED	The memory space that is occupied by the active MemStore.
MAJOR_FREEZE_TRIGGER	The threshold that triggers the major freeze operation.
CPU_USAGE	The current CPU utilization for the tenant.
MIN_CPU_SIZE	The minimum number of CPU cores for the tenant.
MAX_CPU_SIZE	The maximum number of CPU cores for the tenant.
LOCATION_CACHE_PROXY_HIT	The number of cache hits for the OBProxy location cache.
LOCATION_CACHE_PROXY_MISS	The number of cache misses for the OBProxy location cache.
LOCATION_CACHE_RENEW_COUNT	The number of updates in the location cache.
LOCATION_CACHE_RPC_SUCC_COUNT	The number of RPC requests that retrieved data from the location cache as expected.
MEMORY_USAGE	The current memory usage of the tenant.
MIN_MEMORY_SIZE	The minimum memory space of the tenant.
MAX_MEMORY_SIZE	The maximum memory space of the tenant.
MEMSTORE_LIMIT	The maximum memory space for the incremental data that is stored in the MemStore.
TOTAL_MEMSTORE_USED	The total memory space that is occupied by the MemStore.
DATA_SIZE	The total data size of the tenant.
DISK_USAGE	The disk usage.
LEADER_DATA_SIZE	The data size of the server where the leader partition resides.
ABORT_LOG_REPLAY_RT	The duration in which the abort logs are replayed in the memory during the two-phase commit process.
CLEAR_LOG_REPLAY_RT	The duration in which the clear logs are replayed in the memory during the two-phase commit process.

Performance metric	Description
COMMIT_LOG_REPLAY_RT	The duration in which the commit logs are replayed in the memory during the two-phase commit process.
PREPARE_LOG_REPLAY_RT	The duration in which the prepare logs are replayed in the memory during the two-phase commit process.
REDO_LOG_REPLAY_RT	The duration in which the redo logs are replayed in the memory during the two-phase commit process.
PLAN_CACHE_MEM_HOLD	The memory space that can be occupied by the SQL plan cache.
PLAN_CACHE_MEM_USED	The actual memory space that is occupied by the SQL plan cache.
PLAN_CACHE_PLAN_NUM	The number of SQL plans in the SQL plan cache.
PLAN_CACHE_SQL_NUM	The number of executed SQL statements that are recorded the SQL plan cache.
PLAN_CACHE_STMTKEY_NUM	The number of declared keys that are recorded in the SQL plan cache.
RE_SUBMITTED_FREEZE_TASK_COUNT	The number of freeze tasks that are resubmitted.
RE_SUBMITTED_OFFLINE_TASK_COUNT	The number of tasks that are resubmitted to disable objects.
RE_SUBMITTED_TRANS_TASK_COUNT	The number of transaction tasks that are resubmitted.

9.11.3.3. View alert events

This topic describes how to view the details of an alert event.

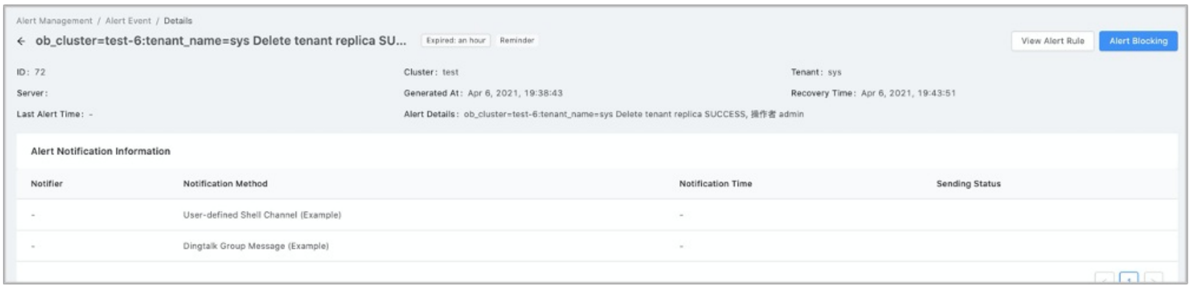
Alert event list

You can view and query all events in the alert event list. The alert event list supports multiple search conditions. You can enter a keyword to match the alert overview, alert details, and values of all tags. For example, If you set Source to OceanBase, you can enter a keyword to match the values of tags. The tags include cluster group, cluster, tenant, and host IP address.

Alert event details

In the alert event list, click an alert to go to the details page of the alert event. Then, you can perform the following operations:

- View the details of the alert event.



Alert Management / Alert Event / Details

ob_cluster=test-6:tenant_name=sys Delete tenant replica SU... Expired: an hour Reminder

ID: 72

Cluster: test

Tenant: sys

Server:

Generated At: Apr 6, 2021, 19:38:43

Recovery Time: Apr 6, 2021, 19:43:51

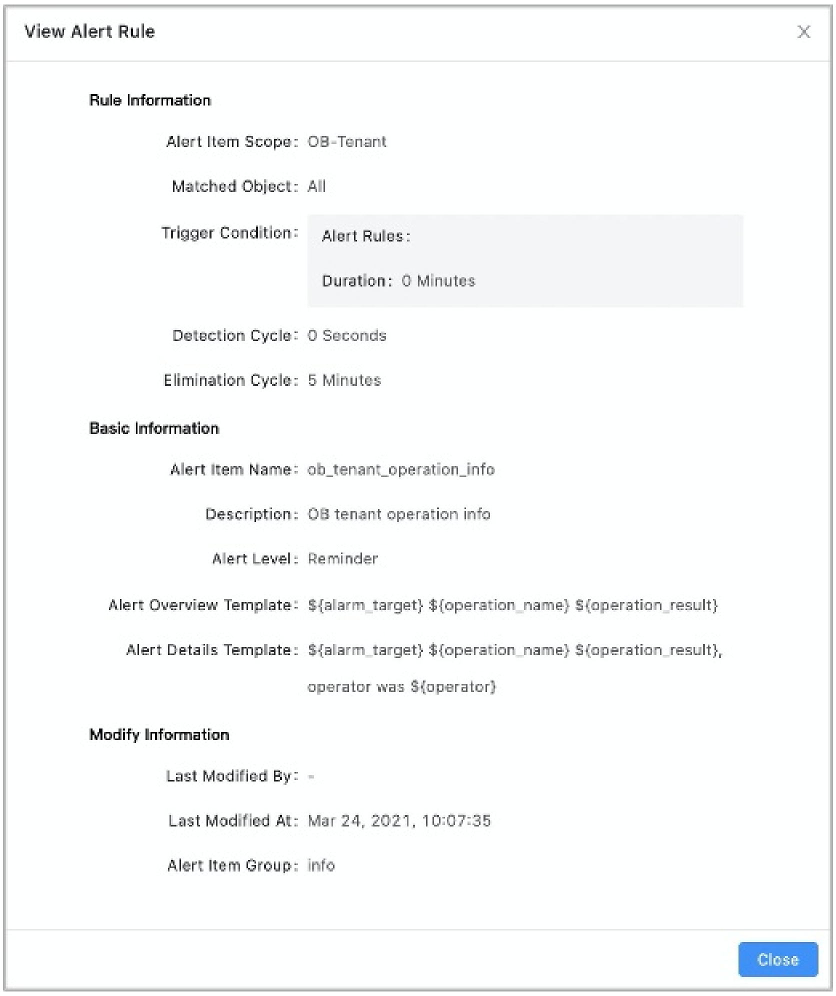
Last Alert Time: -

Alert Details: ob_cluster=test-6:tenant_name=sys Delete tenant replica SUCCESS, 操作者 admin

Alert Notification Information

Notifier	Notification Method	Notification Time	Sending Status
-	User-defined Shell Channel (Example)	-	
-	Dingtalk Group Message (Example)	-	

- Click **View Alert Rule** in the upper-right corner to view the alert rule.



View Alert Rule

Rule Information

Alert Item Scope: OB-Tenant

Matched Object: All

Trigger Condition: Alert Rules:

Duration: 0 Minutes

Detection Cycle: 0 Seconds

Elimination Cycle: 5 Minutes

Basic Information

Alert Item Name: ob_tenant_operation_info

Description: OB tenant operation info

Alert Level: Reminder

Alert Overview Template: ${alarm_target} ${operation_name} ${operation_result}

Alert Details Template: ${alarm_target} ${operation_name} ${operation_result}, operator was ${operator}

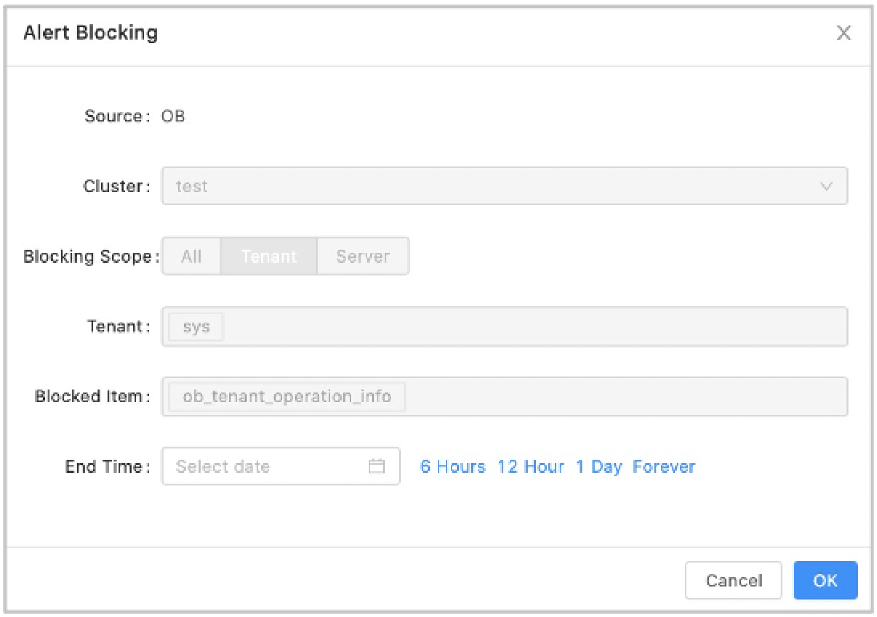
Modify Information

Last Modified By: -

Last Modified At: Mar 24, 2021, 10:07:35

Alert Item Group: info

- Click **Alert Blocking** in the upper-right corner to block the alert.


Alert Blocking

Source: OB

Cluster: test

Blocking Scope: All Tenant Server

Tenant: sys

Blocked Item: ob_tenant_operation_info

End Time: Select date

- View the notification records of the alert.

9.11.3.4. Upgrade the version of a cluster

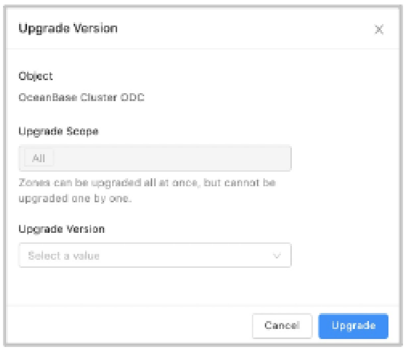
When a new cluster version is available, you can upgrade the version for the cluster that you manage.

Prerequisites

The current logon account must have the cluster management permissions.

Procedure

1. Log on to OceanBase Cloud Platform (OCP). By default, the **Cluster Overview** page appears after you log on to OPC.
2. In the **Clusters** section of the **Cluster Overview** page, select the cluster that you want to manage, and then click the cluster name.
3. Click the icon in the upper-right corner of the **Overview** page and select **Upgrade Version**.
4. In the **Upgrade Version** dialog box, select the version to be upgraded.


Upgrade Version

Object
OceanBase Cluster ODC

Upgrade Scope
All

Zones can be upgraded all at once, but cannot be upgraded one by one.

Upgrade Version
Select a value

If the version to be upgraded is not uploaded to OCP, you can click **Add Version** in the lower part of the **Upgrade Version** list to upload the related package.

5. Click **Upgrade**.
6. In the **Confirm Upgrade Path** dialog box, click **OK**.

9.11.4. Security maintenance

9.11.4.1. Network security maintenance

Network security maintenance helps you ensure device and network security.

- Device security
    - Check network devices and enable security management protocols and configurations for these devices.
    - Check up-to-date versions of network device software and update the software to a secure version in a timely manner.
    - For more information about the security maintenance method, see the product documentation of each device.
- Network security

  Based on your network conditions, select the intrusion detection system (IDS) or intrusion prevention system (IPS) to detect abnormal traffic from the Internet or internal networks. This protects services against abnormal behaviors and attacks in real time.

9.11.4.2. Account password maintenance

Account passwords include system tenant passwords, service tenant passwords, and device passwords of ApsaraDB for OceanBase clusters. To ensure account security, you must use complex passwords for your system tenants and devices and change the passwords on a regular basis.

9.11.4.3. Establish a fault response mechanism

Designate the owners for handling various types of faults

The O&M engineers of ApsaraDB for OceanBase must establish a fault emergency response mechanism. This ensures that the services can be resumed in a timely manner after a fault or a security issue occurs.

Stock-up mechanism

A stock-up mechanism must be established for fragile hardware devices to ensure that hardware faults are rectified in a timely manner. This mitigates the negative impacts of hardware faults.

Technical support

After a system fault is detected during routine maintenance, you can use the O&M platform of ApsaraDB for OceanBase to check fault details. Then, you can analyze the fault causes and rectify the fault based on detailed analysis. If the fault cannot be rectified, you can collect related information such as system information and fault symptoms, and contact technical support.

After you rectify a fault, analyze its causes, review the troubleshooting process, and make improvements.

9.11.5. Backup and recovery

9.11.5.1. Overview

The backup and recovery feature of OceanBase Cloud Platform (OCP) supports full backup and incremental backup for ApsaraDB for OceanBase clusters and tenants. The log backup, full recovery, and incomplete recovery features are supported.

The following procedure shows how to back up and recover data in OCP:

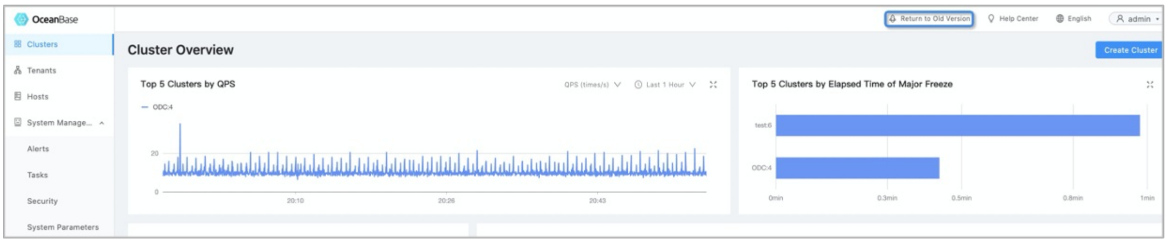
1. Create backup and recovery configuration files.
2. Upload and install backup and recovery agents.
3. Create a backup scheduling task for a cluster.
4. View the result of the backup task that is initiated by the scheduling task.
5. Initiate a recovery task.
6. Connect to the recovered tenant and view the recovered data.

9.11.5.2. Go to the Backup and Recovery page

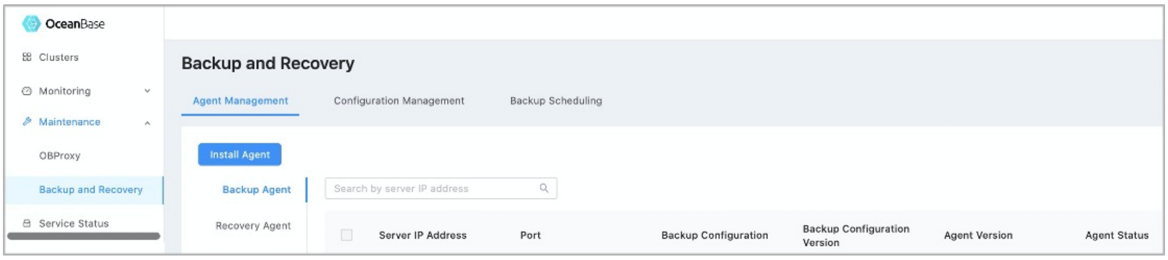
The Backup and Recovery page is displayed in the old version of OceanBase Cloud Platform (OCP). To use the backup and recovery features, you must switch the OCP version to the old version. On the Backup and Recovery page, you can perform O&amp;M operations, use the backup scheduling feature, and view tasks.

Procedure

1. Log on to OCP.
2. In the upper-right corner of the page, click **Return to Old Version**.



3. In the left-side navigation pane, choose **Maintenance > Backup and Recovery**.



□	Server IP Address	Port	Backup Configuration	Backup Configuration Version	Agent Version	Agent Status

9.11.5.3. Preparations

Before you back up and recover data, you must prepare metadatabases and storage media.

Create a metadatabase for backup and recovery

When you install OCP based on Docker images, four versions of metadatabases are created by default within a metadatabase tenant. The versions are backup1472, backup147x, backup21, and backup2230. You can select to use these four versions based on your ApsaraDB for OceanBase version.

Prepare a storage medium

You can select Object Storage Service (OSS) or Network File System (NFS) as the storage medium for backup and recovery. NFS is applicable to independent external scenarios, and OSS is applicable to Apsara Stack scenarios.

OSS configuration

You must obtain the following settings to set the required parameters when you perform related operations on the Configuration Management tab:

- OSS account
- Bucket
- Endpoint
- AccessKey pair: An AccessKey pair is composed of an AccessKey ID and an AccessKey secret. The AccessKey pair is used to perform access identity verification.

NFS configuration

The backup agent, recovery agent, OceanBase Cloud Platform (OCP), and the ApsaraDB for OceanBase cluster to be restored must have access to the specified NFS directory for backup and recovery. Therefore, the NFS directory must be mounted to these hosts. The mounted on-premises directory must be the same as the directory in the backup configuration file.

- NFS server configuration

In this example, the directory name is obbackup.

```
yum install -y nfs-utils portmap
service nfs start
echo '/obbackup *(rw,all_squash,anonuid=500,anongid=500)' >/etc/exports
chmod 777 /obbackup
service nfs restart
exportfs
```

- NFS client configuration

The backup agent, recovery agent, OCP, and the ApsaraDB for OceanBase cluster to be restored must be mounted as a NFS client. Otherwise, data cannot be recovered.

```
showmount -e 11.166.84.52 #The IP address is an example IP address.
mkdir /obbackup
chmod 777 /obbackup
mount -o soft 11.166.84.52:/docker /obbackup
```

9.11.5.4. Manage backup and recovery configuration files

9.11.5.4.1. Add a backup configuration file

This topic describes how to add a backup configuration file.

Prerequisites

- A metadatabase for backup and recovery is created.
- A storage medium is prepared.

Procedure

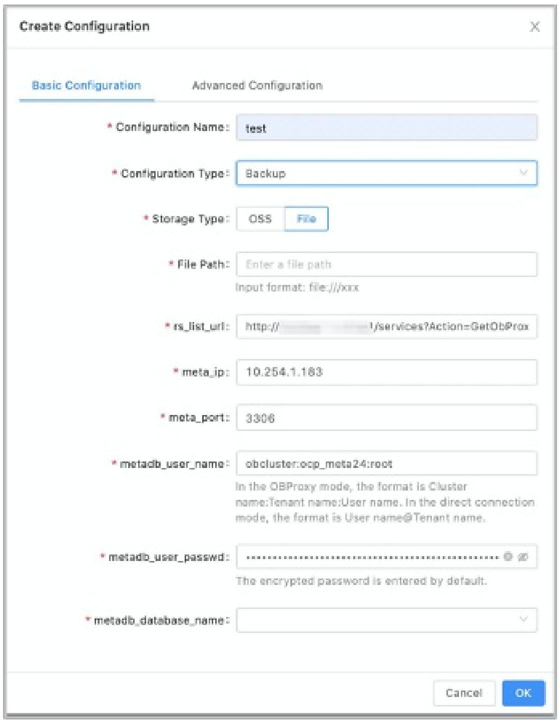
1. Log on to OceanBase Cloud Platform (OCP).
2. Switch to the old version of OCP and open the Backup and Recovery page.
3. On the **Configuration Management** tab, click **Create Configuration** in the upper-left corner.
4. Set the required parameters on the **Basic Configuration** tab.
   1. Set the **Configuration Name** parameter.
   2. Set **Configuration Type** to **Backup**.
   3. Set the **Storage Type** parameter.

By default, the database information of the OCP metadatabase is automatically filled in. The OCP database includes a backup and recovery metadatabase. Modify the settings based on the actual metadatabase.

- If you set Storage type to **OSS**, you must set the File Path, access_key_id, secret_access_key, rs_list_url, meta_ip, meta_port, metadb_user_name, metadb_user_passwd, and metadb_database_name parameters. Some parameters are automatically set, confirm whether the settings are correct.
- If you set Storage type to **File**, you only need to enter the related information of the mounted NFS file.

Parameter	Description
File path	The OSS file path or the file path where the NFS file is mounted.
host	The endpoint.
access_key_id	The AccessKey ID of the OSS account.
secret_access_key	The AccessKey secret of the OSS account.
rs_list_url	The RS List URL provided by current OCP is filled by default.

Parameter	Description
meta_ip	The IP address of the backup and recovery metadatabase.
meta_port	The port number of the backup and recovery metadatabase.
metadb_user_name	The username of the backup and recovery metadatabase.
metadb_user_passwd	The password of the backup and recovery metadatabase.
metadb_database_name	Select an appropriate metadatabase as prompted.



Create Configuration

* Configuration Name: test

* Configuration Type: Backup

* Storage Type: OSS [✓ File]

* File Path: Enter a file path

Input format: file:///xxx

* rs_list_url: http://[redacted]1/services?Action=GetObProx

* meta_ip: 10.254.1.183

* meta_port: 3306

* metadb_user_name: obcluster:ocp_meta24:root

In the OBProxy mode, the format is Cluster name:Tenant name:User name. In the direct connection mode, the format is User name@Tenant name.

* metadb_user_passwd: ••

The encrypted password is entered by default.

* metadb_database_name:

5. (Optional) On the **Advanced Configuration** tab, set the required parameters of **Advanced Configuration**. The parameters of Advanced Configuration are automatically set. You do not need to modify the related settings.

6. Click **OK**.

9.11.5.4.2. Add a recovery configuration file

This topic describes how to add a recovery configuration file.

Prerequisites

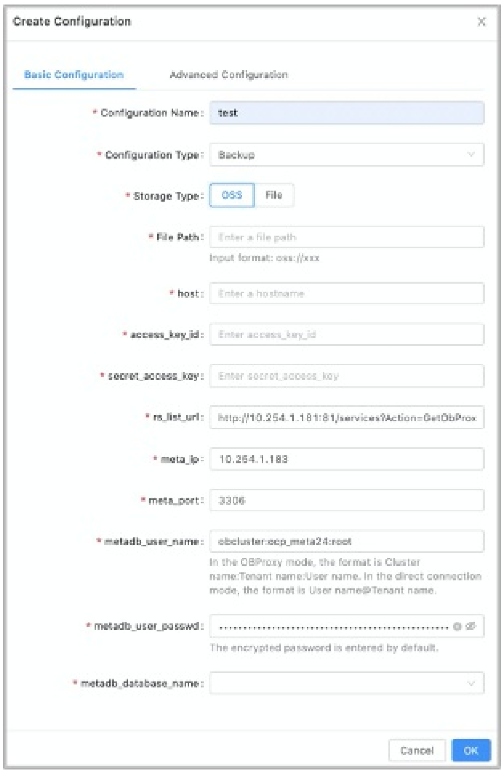
- A metadatabase for backup and recovery is created.
- A storage medium is prepared.

Procedure

1. Log on to OceanBase Cloud Platform (OCP).
2. Switch to the old version of OCP and open the Backup and Recovery page.
3. On the **Configuration Management** tab, click **Create Configuration** in the upper-left corner.
4. Set the required parameters on the **Basic Configuration** tab.
    i. Set the **Configuration Name** parameter.
    ii. Set **Configuration Type** to **Recovery**.
    iii. Set the required parameters.

By default, the database information of the OCP metadatabase is automatically filled in. The OCP database includes a backup and recovery metadatabase. Modify the settings based on the actual metadatabase.

Parameter	Description
ocpMetaDb.clusterName	The name of the cluster where the backup and recovery metadatabase resides. The cluster must be managed by OCP.
ocpMetaDb.tenantName	The tenant to which the backup and recovery metadatabase belongs.
ocpMetaDb.userName	The username of the backup and recovery metadatabase.
ocpMetaDb.dbName	Select an appropriate metadatabase as prompted.
ocpMetaDb.encryptedPassword	The password of the backup and recovery metadatabase.
ocpMetaDb.configUrl	The configUrl of the cluster where the backup and recovery metadatabase resides. This parameter is automatically set and you do not need to modify the related settings.



Create Configuration

Basic Configuration | Advanced Configuration

* Configuration Name: test
* Configuration Type: Backup
* Storage Type: OSS | File
* File Path: Enter a file path
Input format: oss://xxx
* host: Enter a hostname
* access_key_id: Enter access_key_id
* secret_access_key: Enter secret_access_key
* rs_list_url: http://10.254.1.181:81/services?Action=GetObProx
* meta_ip: 10.254.1.183
* meta_port: 3306
* metadb_user_name: obcluster:ocp_meta24:root
In the OBProxy mode, the format is Cluster name:Tenant name:User name. In the direct connection mode, the format is User name@Tenant name.
* metadb_user_passwd: ··
The encrypted password is entered by default.
* metadb_database_name:

5. (Optional) On the **Advanced Configuration** tab, set the required parameters of **Advanced Configuration**. The parameters of Advanced Configuration are automatically set. You do not need to modify the related settings.

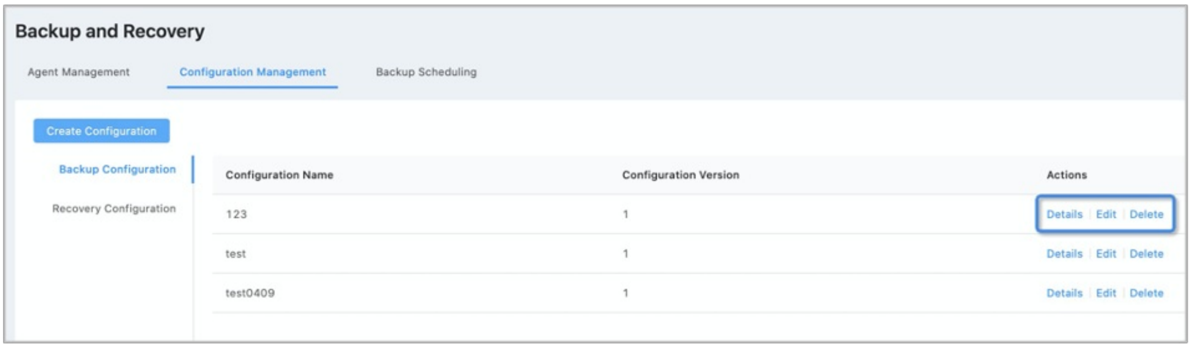
6. Click **OK**.

9.11.5.4.3. Manage a configuration file

The related parameters in backup and recovery configuration files must be correctly set. Otherwise, the related backup and recovery agents cannot work as required. This results in failed backup and recovery.

You can manage your configuration files on the Configuration Management tab based on your business requirements. You can perform the following operations on a configuration file:

- **View the details of the configuration file.**
- **Modify the configurations.**
- **Delete a backup or recovery configuration file.**



Backup and Recovery

Configuration Name	Configuration Version	Actions
123	1	Details | Edit | Delete
test	1	Details | Edit | Delete
test0409	1	Details | Edit | Delete

9.11.5.5. Install backup and recovery agents

9.11.5.5.1. Install backup and recovery agents

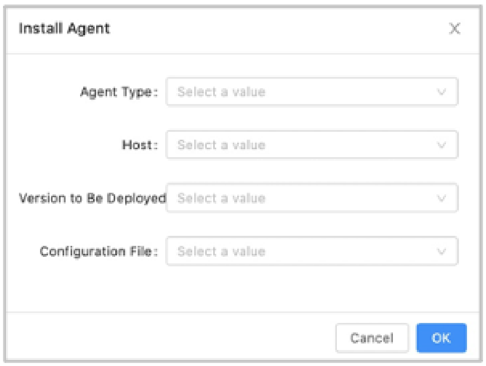
This topic describes how to install backup and recovery agents.

Prerequisites

A host is required to install a backup or recovery agent. Make sure that an idle host is available. If no available hosts are available, you can add a host on the **Host Management** page of the new version of OceanBase Cloud Platform (OCP) based on the related documentation of **Host Management**.

Procedure

1. Log on to OCP.
2. Switch to the old version of OCP and open the Backup and Recovery page.
3. On the **Agent Management** tab, click **Install Agent**.
4. Set the **Agent Type** parameter and specify a host.
5. Set the **Version to Be Deployed** parameter. If no versions are available, you can click Add Version to upload a new installation package.
6. The related backup or recovery configuration file is automatically filtered based on the specified deployment version. If no configuration files are available, add a backup configuration file first.
7. Click OK.



Install Agent

Agent Type: Select a value

Host: Select a value

Version to Be Deployed: Select a value

Configuration File: Select a value

8. After you click OK, a dialog box appears on the page. You can click the link to view the progress.

The progress page is displayed in the new version of OCP. After you view the progress, you need to switch back to the old version. Then, you can perform related O&amp;M operations on the agent.

The process of installing a recovery agent is the same as that of the backup agent. Both backup and recovery agents can be installed on the same host. However, a version is based on the version number of the agent installed first. Different versions cannot be separately specified.

9.11.5.5.2. Manage backup and recovery agents

Installed backup and recovery agents are displayed on the Agent Management tab of the Backup and Recovery page. You can perform some common O&amp;M operations on these installed agents.

You can perform the following operations:

- View the task history of an agent. In the **Task History** column, click **View** to view the historical O&amp;M status of the agent.

- Restart an agent.
- Delete an agent.
- Upgrade an agent.
- Update the configurations of an agent.

  If you want to update the configuration file of an agent, you can modify the configurations on the **Configuration Management** tab, and then update the configurations. The system automatically pushes the latest configurations to the agent side.

9.11.5.6. Run backup tasks

9.11.5.6.1. Cluster backup scheduling

After you create a backup configuration file and a recovery configuration file, and install a backup agent, you can back up your data as needed.

The following backup granularities are supported:

- A specified cluster within current OceanBase Cloud Platform (OCP) can be backed up.
- A specified tenant of a specified cluster can be backed up.

The following two backup modes are supported:

- Automatic, periodic backup scheduling: The system automatically performs periodic backup based on preset backup configuration rules.
- Manual backup: You can manually back up your data as needed.

Create a cluster backup schedule

Prerequisites

- The backup configuration file of the related version is created.
- A backup agent is installed.

Procedure

1. Log on to OCP.
2. In the upper-right corner of the page, click **Return to Old Version**.
3. In the left-side navigation pane, click **Clusters**.
4. Click **Cluster Backup** in the **Actions** column of a specified cluster.
5. Set the required parameters.
   i. Set the Backup Mode and Backup Cycle parameters.
      - The valid values of the Backup Mode parameter are Backup By Week and Backup By Month.
      - The backup cycle can be set to the specified day or day of the week for backup based on the specified backup mode.
   ii. Set the Backup Configuration parameter.
      - Only the backup configuration files of the related version are displayed in the drop-down list.

- If no backup configuration files are available, create a backup configuration file before you configure a cluster backup schedule.

iii. Set the Back Start Time parameter.

iv. Confirm whether to initiate incremental backup. Incremental backup is log backup.

6. Click **Submit**.

Manage a cluster backup schedule

After you create a cluster backup schedule, the system automatically initiates backup tasks based on the preset cycle and time. You can modify the backup scheduling tasks based on your business requirements. The following operations are supported to manage your schedules:

- Suspend a backup scheduling task.

  Click Suspend in the Actions column of a specified backup scheduling task to suspend the task.

- Rerun a backup scheduling task.

  Click Rerun in the Actions column of a specified backup scheduling task to rerun the task. Then, the system automatically initiates backup tasks based on the preset cycle and time.

View the backup history of a cluster.

On the **Backup Scheduling** tab of the **Backup and Recovery** page, you can view the basic information of all scheduling tasks. The information includes the cluster name, tenant name, backup mode, backup cycle, current scheduling task status, baseline backup task status, incremental backup task, and initiator.

Click a cluster name to view the backup scheduling history, baseline backup history, incremental backup history, and recovery history of the specified cluster. On the Backup Scheduling History tab, you can filter by the status of backup scheduling tasks.

- Backup Scheduling History: The Backup Scheduling History tab displays the task name, ID, cluster, initiator, status, progress, start time, and end time.
- Baseline Backup History: The **Baseline Backup History** tab displays the task ID, backup type, task type, number of tasks, cluster, tenant, start time, end time, data version, backup URL, backup status, and backup size. You can specify a backup task to initiate a data recovery.
- Incremental Backup History: The **Incremental Backup History** tab displays the cluster name, tenant whitelist, majorVersion, backup URL, agentServerIp, location, latency (seconds), status, stop status, and error message.

9.11.5.6.2. Tenant backup scheduling

You cannot back up a tenant and the related cluster at the same time.

Only one tenant backup schedule can be created in a cluster.

- If no backup schedules are available, you can create a cluster backup schedule or a tenant backup schedule.
- If a cluster backup schedule is created, all tenants in the cluster follow the scheduling configuration of the cluster by default. You cannot configure a tenant scheduling task.

- If a tenant backup schedule is created, you cannot create a backup schedule for the related cluster. Before you configure a cluster backup schedule, you must cancel the backup scheduling task of the related tenant and suspend the related incremental backup task.

Prerequisites

No running backup scheduling tasks or incremental backup tasks in the cluster to which the specified tenant belongs.

Procedure

1. Log on to OceanBase Cloud Platform (OCP).
2. In the upper-right corner of the page, click **Return to Old Version**.
3. In the left-side navigation pane, click **Tenants**.
4. Click **Cluster Backup** in the **Actions** column of the specified cluster.
5. Set the required parameters.

    i. Set the **Backup Mode** and **Backup Cycle** parameters.

    - The valid values of the **Backup Mode** parameter are **Backup By Week** and **Backup By Month**.
    - The backup cycle can be set to the specified day or day of the week for backup based on the specified backup mode.

    ii. Set the **Backup Configuration** parameter.

    - Only the backup configuration files of the related version are displayed in the drop-down list.
    - If no backup configuration files are available, create a backup configuration file before you configure a cluster backup schedule.

    iii. Set the **Back Start Time** parameter.

    iv. Set the **Initiate Incremental Backup** parameter. Incremental backup is log backup.

6. Click **Submit**.

Manage a tenant backup schedule

After you create a tenant backup schedule, the system automatically initiates backup tasks based on the preset cycle and time. You can modify the backup scheduling tasks based on your business requirements. The following operations are supported to manage your schedules:

- Suspend a backup scheduling task. Click **Suspend** in the Actions column of a specified backup scheduling task to suspend the task.
- Click **Rerun** in the Actions column of a specified backup scheduling task to rerun the task. Then, the system automatically initiates backup tasks based on the preset cycle and time.

9.11.5.6.3. Back up now

You can initiate an instant backup task for a cluster or tenant that has a backup schedule. If a backup schedule is available, you can manually perform a baseline backup task.

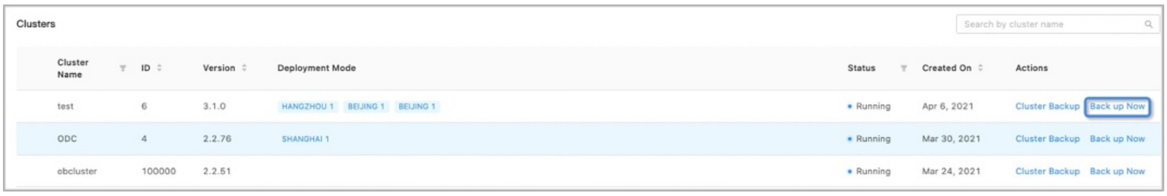
> **Note**
>
> A major freeze version of ApsaraDB for OceanBase can only have one baseline backup task. If multiple backup tasks are initiated based on the same version, errors are reported for subsequent backup tasks. However, the backup tasks of this version are available.

Prerequisites

A backup scheduling task is configured for a cluster or a tenant.

Procedure

1. Log on to OceanBase Cloud Platform (OCP).
2. In the upper-right corner of the page, click **Return to Old Version**.
3. In the left-side navigation pane, click **Tenants** or **Clusters**.
4. Click **Back Up Now** in the **Actions** column of the tenant or cluster.

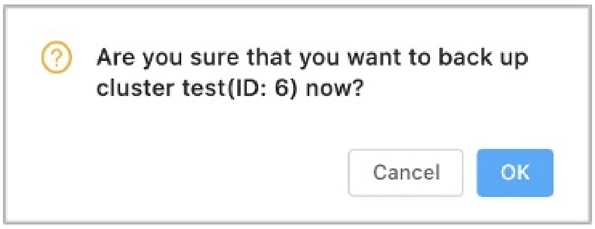


Clusters

Search by cluster name

Cluster Name	ID	Version	Deployment Mode	Status	Created On	Actions
test	6	3.1.0	HANGZHOU 1 BEIJING 1 BEIJING 1	Running	Apr 6, 2021	Cluster Backup Back up Now
ODC	4	2.2.76	SHANGHAI 1	Running	Mar 30, 2021	Cluster Backup Back up Now
obcluster	100000	2.2.51		Running	Mar 24, 2021	Cluster Backup Back up Now

5. In the dialog box that appears, click **OK**.



Are you sure that you want to back up cluster test(ID: 6) now?

9.11.5.7. Recover backup data

After the system performs a backup operation, it can initiate a recovery task based on the backup. The minimum granularity of recovery tasks is tenant-level data. Multiple tenants can be recovered in batches.

Prerequisites

A baseline backup task is performed on the cluster or tenant to be recovered.

Procedure

1. Log on to OceanBase Cloud Platform (OCP).
2. Go to the Backup and Recovery page.
3. On the **Backup Scheduling** tab, click the name of the specified cluster.
4. On the **Baseline Backup History** tab, find the baseline backup to be restored.

5. In the **Actions** column, click **Initiate Recovery**. The click position and the recovery version have no relations. The system automatically calculates and chooses a baseline version for recovery based on recovery time.
6. Specify **Cluster for Recovery** and **Restore to Point in Time**. The cluster to be recovered can be a source cluster or another cluster.
7. Enter the user password.
8. Select the tenant to be restored and confirm the settings of **Target Tenant Name, Restore Locality, Restore Pool List, and Restore Primary Zone**. The system automatically fills the related fields based on the backup information. You must confirm whether the filled content is correct.

- If you recover data to the source cluster, you must change the tenant name to a new name.
- Restore Pool List indicates the related resource configurations of the tenant. The resource pool name cannot exist in the destination cluster.

9. Click **OK**. After the recovery request is successfully initiated, a success message appears.

View the status of a recovery task

In the **Recovery History** column, you can view the status of the recovery task. You must refresh the page to view the updated information.

The recovery process consists of the following two phases. Only when both phases are successful, the tenant recovery is successful.

- Baseline recovery
- Incremental recovery

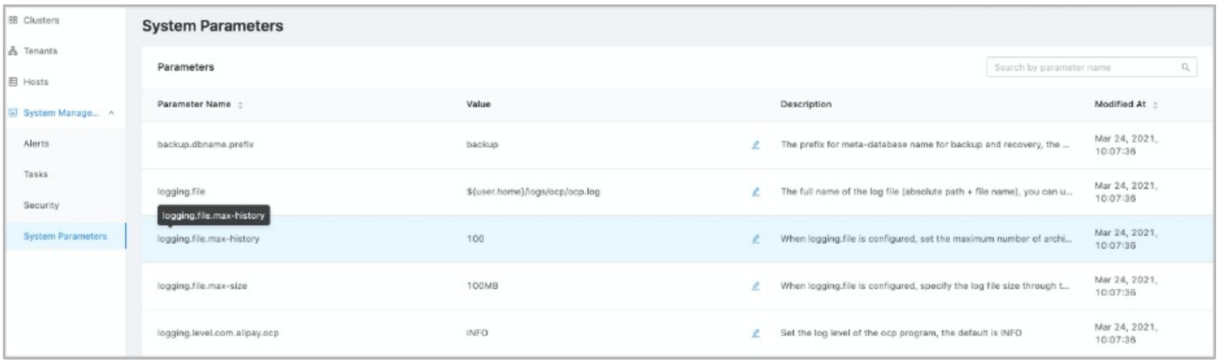
Use a recovery tenant

The connection password of the recovery tenant is empty. When the message is prompted, enter to confirm.

9.11.5.8. Monitoring and alert configurations

Backup and recovery settings are configured as system parameters in OceanBase Cloud Platform (OCP).

On the System Management>System Parameters page of the new version of OCP, enter backup in the search box to query and view the parameters of backup and recovery.



System Parameters

Parameters

Parameter Name	Value	Description	Modified At
backup.dbname.prefix	backup	The prefix for meta-database name for backup and recovery, the ...	Mar 24, 2021, 10:07:36
logging.file	${user.home}/logs/ocp/ocp.log	The full name of the log file (absolute path + file name), you can u...	Mar 24, 2021, 10:07:36
logging.file.max-history	100	When logging.file is configured, set the maximum number of archi...	Mar 24, 2021, 10:07:36
logging.file.max-size	100MB	When logging.file is configured, specify the log file size through t...	Mar 24, 2021, 10:07:36
logging.level.com.alipay.ocp	INFO	Set the log level of the ocp program, the default is INFO	Mar 24, 2021, 10:07:36

Monitoring configurations

In the current OCP version, you can manage and configure the following parameters of backup and recovery:

- Status monitoring of agents.
- Monitoring of failed baseline backup tasks.
- Monitoring of incremental backup task latency. For more information, see `ocp.backup.alarm.inc-backup-delay-threshold` .
- Monitoring of failed backup scheduling tasks.
- Monitoring of expired backup file cleaning. For more information, see `ocp.backup.alarm.backup-data-retention-days` .
- Monitoring for the log cleaning of backup agents. For more information, see `ocp.backup.alarm.backup-liboblog-expire-days` .

> ? Note
>
> The current version does not support the monitoring for the capacity of backup files.

Alert configurations

The following table describes the parameters of alerts.

Parameter	Default value	Description
ocp.backup.alarm.base-backup-last-finished-threshold	12960	The baseline has not been successfully backed up for 9 days, the initial threshold is 9 days (12960 minutes), the unit is minutes
ocp.backup.alarm.base-backup-timeout	10	Baseline backup scheduling timeout period (minutes)
ocp.backup.alarm.inc-backup-delay-threshold	3600	Incremental backup delay alarm threshold (seconds)
ocp.backup.alarm.last-data-backup-max-interval-minutes	1440	Check whether the baseline backup task failed in a certain time range recently, the default is 1 day, the unit is minute; that is, the maximum allowable interval between the last successful data backup and the current time

For more information about alert configurations, see related documentation to subscribe and configure.

9.11.6. Troubleshooting

9.11.6.1. Troubleshooting methods

After a system fault is detected during routine maintenance, you can log on to the Apsara Stack Operations console for ApsaraDB for OceanBase to check the fault details. Then, you can analyze the fault causes and rectify the fault based on detailed analysis.

If the fault cannot be rectified, you can collect related information such as system information and fault symptoms, and contact technical support.

After you rectify a fault, analyze its causes, review the troubleshooting process, and make improvements.

9.11.6.2. Troubleshoot common faults

9.11.6.2.1. Insufficient memory

Possible causes

Insufficient memory may occur due to three possible causes. One of the possible causes is that the service data is written to the memory of a tenant at a high rate. Another possible cause is that the tenant is allocated with only a small amount of memory space. The last possible cause is that the cluster processes high loads of service data.

The memory space that is occupied by the MemStore of one tenant or all the tenants may reach the upper limit for the memory space. If this occurs, data cannot be written to ApsaraDB for OceanBase nodes, or the "Over tenant memory limits" error is reported. In this scenario, errors occur if you perform operations in ApsaraDB for OceanBase.

Solutions

- Trigger major freeze operations or configure minor freeze operations to release some memory space.
- Allocate more memory resources to the tenant.
- Scale out the cluster.
- Implement rate limiting and throttling.

9.11.6.2.2. Insufficient disk space

Possible causes

A large number of system log files or commit log files are written into the disks.

Solutions

- If a large number of system log files are written to the disks, delete the earliest system log files in the oceanbase/log directory.
- If a large number of commit log files are written to the disks, delete the earliest files in the clog folder. Then, you can perform two major freeze operations.

9.11.6.2.3. High CPU utilization

Possible causes

High CPU utilization may be caused by high program workloads, slow SQL queries, or inappropriate resource allocation.

Solutions

- If high CPU utilization is detected on some servers, increase the value of the unit_number parameter to increase the CPU resources that are allocated to the tenants of the servers. This allows the servers to occupy more resources and helps you balance the server loads.
- If high CPU utilization is caused by slow SQL queries, contact the developers to check the issue and optimize the SQL statements that result in the issue.

9.11.6.2.4. High loads

Possible causes

One of the possible causes is that a large number of programs are concurrently running. Another possible cause is that SQL statements are executed at a low efficiency.

Solutions

- If the loads of some servers are high, increase the value of the unit_number parameter to increase the resources that are allocated to the tenants of the servers. This allows the servers to occupy more resources and helps you balance the server loads.
- If a large number of programs are concurrently running, contact the developers to reduce the number of concurrent programs.
- If high loads are caused by low efficiency of executing SQL statements, execute the EXPLAIN statement to check how the system processes the SQL statements and to find performance bottlenecks. If you cannot use indexes to improve the execution efficiency, contact the developers.

9.12. Log Service

9.12.1. O&M methods

This topic describes two O&M methods of Log Service.

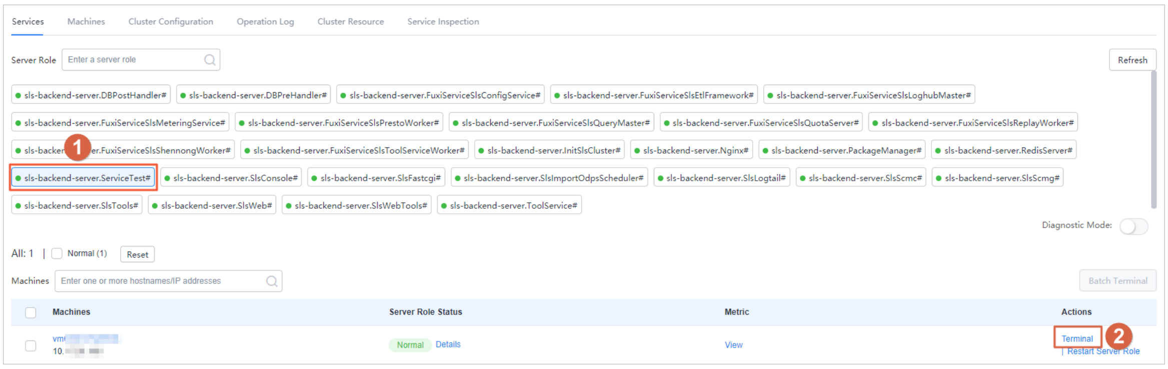
Log Service is deployed, operated, and maintained by using the Apsara Infrastructure Management Framework console. Log Service supports the following two O&M methods:

- Terminal: In the Apsara Infrastructure Management Framework console, you can use the terminal service to log on to the server where Log Service resides and view logs.
- Portal: The Portal provides a user interface to manage Log Service. The Portal complies with the standard Java applications of Alibaba Cloud.

Terminal

1. Log on to the Apsara Uni-manager Operations Console.For more information, see the **ASAPI Reference > Log on to the API Tool console** topic in *Log Service Operation Guide*.

2. In the left-side navigation pane, choose **Products > Product List**.
3. On the page that appears, click **Apsara Infrastructure Management Framework** to go to the Apsara Infrastructure Management Framework console.
4. In the left-side navigation pane, choose **Operations > Service Operations**.
5. On the page that appears, find `sls-backend-server` in the Services column, and then click **Operations** in the Actions column.
6. On the **Clusters** tab, find the destination cluster in the Clusters column, and then click **Operations** in the Actions column.
7. On the **Services** tab, select the destination server role, for example, sls-backend-server.ServiceTest#, and then click **Terminal** in the Actions column.



sls-backend-server.DBPostHandler#
sls-backend-server.DBPreHandler#
sls-backend-server.FuxiServiceSlsConfigService#
sls-backend-server.FuxiServiceSlsEtlFramework#
sls-backend-server.FuxiServiceSlsLoghubMaster#
sls-backend-server.FuxiServiceSlsMeteringService#
sls-backend-server.FuxiServiceSlsPrestoWorker#
sls-backend-server.FuxiServiceSlsQueryMaster#
sls-backend-server.FuxiServiceSlsQuotaServer#
sls-backend-server.FuxiServiceSlsReplayWorker#
sls-backend-server.FuxiServiceSlsShennongWorker#
sls-backend-server.FuxiServiceSlsToolServiceWorker#
sls-backend-server.InitSlsCluster#
sls-backend-server.Nginx#
sls-backend-server.PackageManager#
sls-backend-server.RedisServer#
sls-backend-server.ServiceTest#
sls-backend-server.SlsConsole#
sls-backend-server.SlsFastcgi#
sls-backend-server.SlsImportOdpsScheduler#
sls-backend-server.SlsLogtail#
sls-backend-server.SlsScmc#
sls-backend-server.SlsScmg#
sls-backend-server.SlsTools#
sls-backend-server.SlsWeb#
sls-backend-server.SlsWebTools#
sls-backend-server.ToolService#

All: 1 | □ Normal (1) Reset

Machines: Enter one or more hostnames/IP addresses

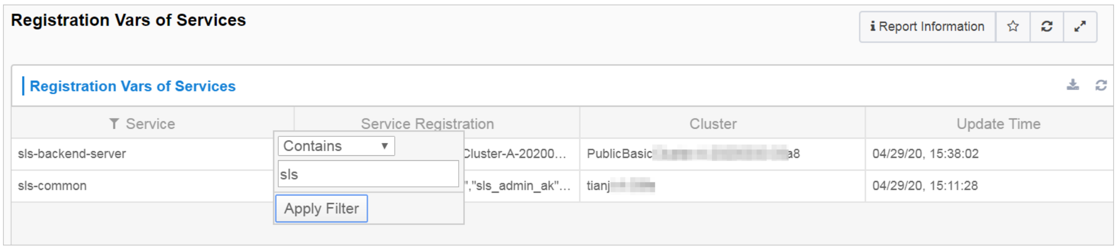
□	Machines	Server Role Status	Metric	Actions
□	vm[redacted] 10.[redacted]	Normal Details	View	Terminal | Restart Server Role

8. Log on to the server by using the terminal service and go to the related directory to view logs.

Portal

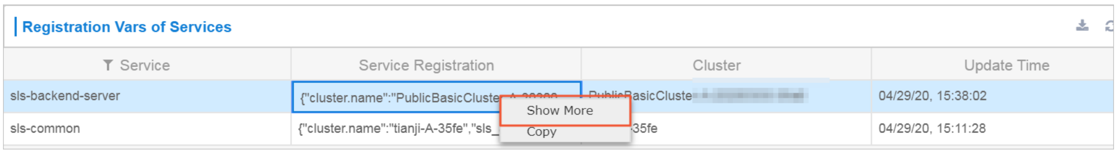
You can collect logs from your server and send the logs to the portal service. Then, you can query, retrieve, and analyze these logs by using the portal service.

1. Log on to the Apsara Infrastructure Management Framework console to obtain the endpoint of the portal service.
   i. For more information, see Terminal.
   ii. In the left-side navigation pane, click **Reports**. You are redirected to the **All Reports** page.
   iii. In the Report column, click **Registration Vars of Services**.
   iv. In the dialog box that appears, click the ☰ icon in the column, enter **sls** in the search box, and then click **Apply Filter**.



Service	Service Registration	Cluster	Update Time
sls-backend-server	Cluster-A-20200...	PublicBasic[redacted]a8	04/29/20, 15:38:02
sls-common	","sls_admin_ak"...	tianj[redacted]	04/29/20, 15:11:28

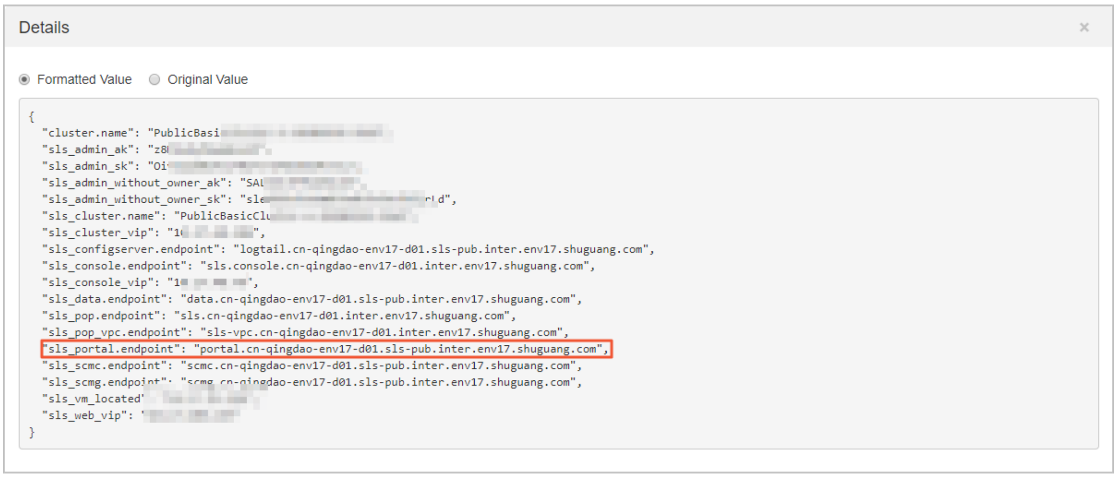
v. Right-click the **Service Registration** column of the **sls-backend-server** service, and then select **Show More**.



Registration Vars of Services

Service	Service Registration	Cluster	Update Time
sls-backend-server	{"cluster.name":"PublicBasicCluste	PublicBasicCluste[redacted]	04/29/20, 15:38:02
sls-common	{"cluster.name":"tianji-A-35fe","sls_	35fe	04/29/20, 15:11:28

vi. On the **Details** page, find the endpoint of the Portal.



Details

● Formatted Value ○ Original Value

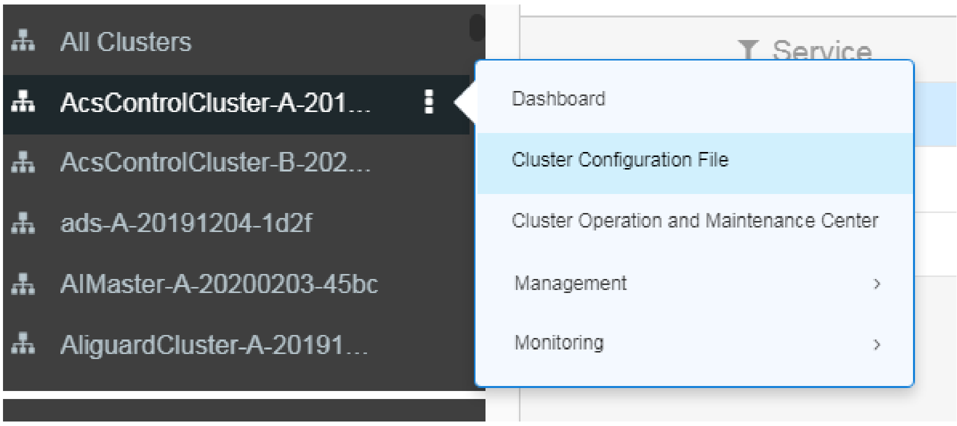
```
{
  "cluster.name": "PublicBasi[redacted]
  "sls_admin_ak": "z8[redacted]
  "sls_admin_sk": "Oi[redacted]
  "sls_admin_without_owner_ak": "SAL[redacted]
  "sls_admin_without_owner_sk": "sle[redacted]rld",
  "sls_cluster.name": "PublicBasicClu[redacted]
  "sls_cluster_vip": "1[redacted]",
  "sls_configserver.endpoint": "logtail.cn-qingdao-env17-d01.sls-pub.inter.env17.shuguang.com",
  "sls_console.endpoint": "sls.console.cn-qingdao-env17-d01.inter.env17.shuguang.com",
  "sls_console_vip": "1[redacted]",
  "sls_data.endpoint": "data.cn-qingdao-env17-d01.sls-pub.inter.env17.shuguang.com",
  "sls_pop.endpoint": "sls.cn-qingdao-env17-d01.inter.env17.shuguang.com",
  "sls_pop_vpc.endpoint": "sls-vpc.cn-qingdao-env17-d01.inter.env17.shuguang.com",
  "sls_portal.endpoint": "portal.cn-qingdao-env17-d01.sls-pub.inter.env17.shuguang.com",
  "sls_scmc.endpoint": "scmc.cn-qingdao-env17-d01.sls-pub.inter.env17.shuguang.com",
  "sls_scmg.endpoint": "scmg.cn-qingdao-env17-d01.sls-pub.inter.env17.shuguang.com",
  "sls_vm_located'[redacted]
  "sls_web_vip": '[redacted]
}
```

2. Log on to the Apsara Infrastructure Management Framework console to obtain the AccessKey pair of the portal service.

   i. Log on to the Apsara Infrastructure Management Framework console. For more information, see Terminal.

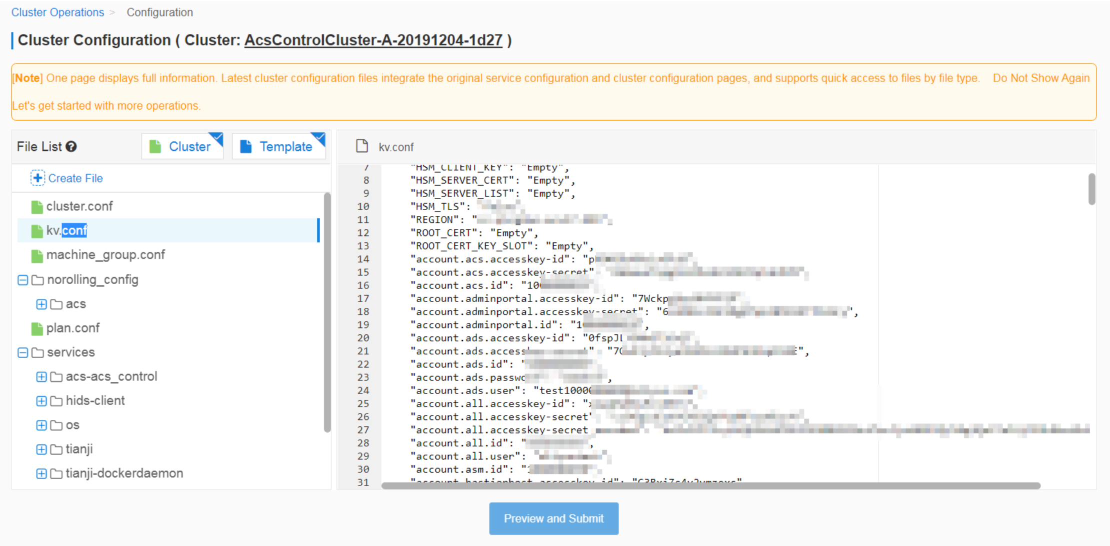
   ii. In the left-side navigation pane, click **Reports**. You are redirected to the **All Reports** page.

   iii. On the left side of the page, click the **Cluster** tab, find the destination cluster, and then choose ⋮ > **Cluster Configuration File**.



All Clusters
AcsControlCluster-A-201...
AcsControlCluster-B-202...
ads-A-20191204-1d2f
AIMaster-A-20200203-45bc
AliguardCluster-A-20191...
Service
Dashboard
Cluster Configuration File
Cluster Operation and Maintenance Center
Management
Monitoring

iv. Click **kv.conf** to obtain the AccessKey pair of the portal service.



Cluster Operations > Configuration

Cluster Configuration (Cluster: AcsControlCluster-A-20191204-1d27)

[Note] One page displays full information. Latest cluster configuration files integrate the original service configuration and cluster configuration pages, and supports quick access to files by file type. Do Not Show Again

Let's get started with more operations.

```
    "HSM_CLIENT_KEY": "Empty",
    "HSM_SERVER_CERT": "Empty",
    "HSM_SERVER_LIST": "Empty",
    "HSM_TLS": [redacted]
    "REGION": "[redacted]
    "ROOT_CERT": "Empty",
    "ROOT_CERT_KEY_SLOT": "Empty",
    "account.acs.accesskey-id": "p[redacted]
    "account.acs.accesskey-secret"[redacted]
    "account.acs.id": "10[redacted]
    "account.adminportal.accesskey-id": "7Wckp[redacted]
    "account.adminportal.accesskey-secret": "6[redacted]",
    "account.adminportal.id": "1[redacted],
    "account.ads.accesskey-id": "0fspJl[redacted]
    "account.ads.access[redacted]": "7C[redacted]",
    "account.ads.id": '[redacted]
    "account.ads.passwc[redacted],
    "account.ads.user": "test1000[redacted]
    "account.all.accesskey-id": "[redacted]
    "account.all.accesskey-secret'[redacted]
    "account.all.accesskey-secret [redacted]
    "account.all.id": "[redacted],
    "account.all.user": [redacted]
    "account.asm.id": "[redacted]
    "account.bastionhost.accesskey-id": "C3Bxi7c4v2vmzexc"
```

3. Log on to the Apsara Infrastructure Management Framework console.Log on to the portal service by using the endpoint obtained in Step 1 and the AccessKey pair obtained in Step 2.
4. Find the destination project and Logstore, and then query and analyze logs.

9.12.2. O&M

9.12.2.1. View logs on machines

InitSlsCluster#

- Startup log: /cloud/app/sls-backend-server/InitSlsCluster#/init_sls_cluster/current/log/start.log
- Service log: none

Nginx#

- Startup log: /cloud/app/sls-backend-server/Nginx#/nginx/current/log/start.log
- Service logs:
  - /apsara/nginx/logs/access.log
  - /apsara/nginx/logs/error.log
  - /apsara/nginx/logs/fastcgi_agent_access.log
  - /apsara/nginx/logs/offline_access.log
  - /apsara/nginx/logs/scmc_access.log
  - /apsara/nginx/logs/scmc_err_log
  - /apsara/nginx/logs/scmc_op_log
  - /apsara/nginx/logs/scmg_access.log
  - /apsara/nginx/logs/scmg_err_log
  - /apsara/nginx/logs/scmg_op_log
  - /apsara/nginx/logs/sls_console.log
  - /apsara/nginx/logs/web_access.log

PackageManager#

- Startup log: /cloud/app/sls-backend-server/PackageManager#/package_manager/current/log/start.log
- Service log: none

RedisServer#

- Startup log: /cloud/app/sls-backend-server/RedisServer#/sls_redis/current/log/start.log
- Service log: /var/log/redis/redis.log

SlsConsole#

- Startup log: /cloud/app/sls-backend-server/SlsConsole#/sls_console/current/log/start.log
- Service logs: /alidata/www/logs/
  - /alidata/www/logs/java/sls/
    - /alidata/www/logs/java/sls/dashboard.log
    - /alidata/www/logs/java/sls/debug.log
    - /alidata/www/logs/java/sls/error.log
    - /alidata/www/logs/java/sls/info.log
    - /alidata/www/logs/java/sls/reasons.log
    - /alidata/www/logs/java/sls/tairSave.log
  - /alidata/www/logs/java/sls-service/applog
    - /alidata/www/logs/java/sls-service/applog/error.log
    - /alidata/www/logs/java/sls-service/applog/info.log
    - /alidata/www/logs/java/sls-service/applog/warn.log
  - /usr/share/jetty/logs/
    - /usr/share/jetty/logs/request.log
    - /usr/share/jetty/logs/stderrout.log

SlsFastcgi#

- Startup log: /cloud/app/sls-backend-server/SlsFastcgi#/sls_fastcgi/current/log/start.log
- Service logs:
  - /apsara/fcgi_agent/FastcgiAgent.LOG
  - /apsara/fcgi_agent/metering.LOG
  - /apsara/fcgi_agent/monitor.LOG
  - /apsara/fcgi_agent/ols_operation.LOG

SlsLogtail#

- Startup log: /cloud/app/sls-backend-server/SlsLogtail#/sls_ilogtail/current/log/start.log
- Service logs
  - Service log on Apsara Stack: /usr/local/ilogtail_private/ilogtail.LOG
  - Service log on on-premises machines: /usr/local/ilogtail/ilogtail.LOG

SlsScmc#

- Startup log: /cloud/app/sls-backend-server/SlsScmc#/sls_scmc/current/log/start.log
- Service logs:
  - /var/www/html/SCMC/logs/scm_op_log
  - /var/www/html/SCMC/logs/scm_err_log

SlsScmg#

- Startup log: /cloud/app/sls-backend-server/SlsScmg#/sls_scmg/current/log/start.log
- Service logs:
  - /var/www/html/SCMG/logs/scm_err_log
  - /var/www/html/SCMG/logs/scm_op_log

SlsTools#

- Startup log: /cloud/app/sls-backend-server/SlsTools#/aliyun_log_cli/current/log/start.log
- Service log: none

SlsWeb#

- Startup log: /cloud/app/sls-backend-server/SlsWeb#/sls_web/current/log/start.log
- Service logs:
  - /apsara/sls/web/logs/access.log
  - /apsara/sls/web/logs/apidetail.log
  - /apsara/sls/web/logs/httpclient.log
  - /apsara/sls/web/logs/normal.log
  - /apsara/sls/web/logs/sysinfo.log
  - /apsara/sls/web/logs/worker.log

SlsWebTools#

- Startup log: /cloud/app/sls-backend-server/SlsWebTools#/sls_web_tools/current/log/start.log
- Service log: none

ToolService#

- Startup logs:
  - /cloud/app/sls-backend-server/ToolService#/init_db/current/log/start.log
  - /cloud/app/sls-backend-server/ToolService#/init_diamond/current/log/start.log
  - /cloud/app/sls-backend-server/ToolService#/init_odps/current/log/start.log
  - /cloud/app/sls-backend-server/ToolService#/init_pop/current/log/start.log
  - /cloud/app/sls-backend-server/ToolService#/jdk_uploader/current/log/start.log
- Service log: none

SlsImportOdpsScheduler#

- Startup log: /cloud/app/sls-backend-server/SlsImportOdpsScheduler#/sls_import_odps_scheduler/current/log/start.log

- Service Logs: Job Scheduler service

FuxiServiceSlsConfigService#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsConfigService#/sls_config_service/current/log/start.log
- Service log: none

FuxiServiceSlsEtlFramework#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsEtlFramework#/sls_etl_framework/current/log/start.log
- Service log: none

FuxiServiceSlsLoghubMaster#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsLoghubMaster#/sls_loghub_master/current/log/start.log
- Service log: none

FuxiServiceSlsMeteringService#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsMeteringService#/sls_metering_service/current/log/start.log
- Service log: none

FuxiServiceSlsPrestoWorker#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsPrestoWorker#/sls_presto_worker/current/log/start.log
- Service log: none

FuxiServiceSlsQueryMaster#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsQueryMaster#/sls_query_master/current/log/start.log
- Service log: none

FuxiServiceSlsQuotaServer#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsQuotaServer#/sls_quota_server/current/log/start.log
- Service log: none

FuxiServiceSlsReplayWorker#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsReplayWorker#/sls_replay_worker/current/log/start.log
- Service log: none

FuxiServiceSlsShennongWorker#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsShennongWorker#/sls_shennong_worker/current/log/start.log

- Service log: none

FuxiServiceSlsToolServiceWorker#

- Startup log: /cloud/app/sls-backend-server/FuxiServiceSlsToolServiceWorker#/sls_tool_service_worker/current/log/start.log
- Service log: none

NGINX

Error log: */apsara/nginx/log/error.log*

Error	Action
Bind Address Failed	Check the port listening information in */etc/init.d/nginx.conf*.
open() ... failed	Check whether the item that you want to open exists in the static resource file.

Console

Error log: */alidata/www/logs/java/sls/error.log*

Error	Action
SLS SDK Exception	No action is required.
Create Bean Failed	Check the dubbo settings in the console configurations of SlsConsole.

Service

Error log: */alidata/www/logs/java/sls-service/applog/error.log*

Error	Action
Create Bean Failed	Check the dubbo settings in the service configurations of SlsConsole.
Invoke failed	Check the scmg settings in the service configurations of SlsConsole.

Query Job Scheduler service logs

1. In the startup log, find the **rpc sql** command.

   For example, if the command is **/apsara/deploy/pc_wrapper/rpc.sh spl EtlFramework**, EtlFramework is the name of the Job Scheduler service.

```
[root@vm010025018250 /cloud/app/sls-backend-server/FuxiServiceSlsEtlFramework#/sls_etl_framew
ork/current]
#tail -n 10 /cloud/app/sls-backend-server/FuxiServiceSlsEtlFramework#/sls_etl_framework/current/log
/start.log
2020-01-07 15:06:55,213 - 83648 - root - tianji_starter.handle_check_alive:353 - INFO - Enter the check ali
ve phase, deploy_flag=True
2020-01-07 15:06:55,213 - 83648 - root - command_executor.exec_cmd:12 - INFO - Prepare to execute cm
d, cmd=[/apsara/deploy/rpc_wrapper/rpc.sh spl EtlFramework]
2020-01-07 15:06:55,414 - 83648 - root - tianji_proxy_client.report_status:23 - INFO - Prepare to report st
atus, monitor=sls_etl_framework_monitor_app, level=good, description=, hostname=vm01002501825
0, server_role=sls-backend-server.FuxiServiceSlsEtlFramework#
2020-01-07 15:06:55,854 - 83648 - root - tianji_starter.do_check_conf_notify:214 - INFO - Check conf_not
ify, last_check_time=1576942460.83, cur_check_time=1576942460.83
2020-01-07 15:07:05,357 - 83648 - root - tianji_starter.handle_check_alive:353 - INFO - Enter the check ali
ve phase, deploy_flag=True
2020-01-07 15:07:05,358 - 83648 - root - command_executor.exec_cmd:12 - INFO - Prepare to execute cm
d, cmd=[/apsara/deploy/rpc_wrapper/rpc.sh spl EtlFramework]
2020-01-07 15:07:05,426 - 83648 - root - tianji_starter.handle_check_alive:353 - INFO - Enter the check ali
ve phase, deploy_flag=True
2020-01-07 15:07:05,427 - 83648 - root - command_executor.exec_cmd:12 - INFO - Prepare to execute cm
d, cmd=[/apsara/deploy/rpc_wrapper/rpc.sh spl EtlFramework]
2020-01-07 15:07:05,580 - 83648 - root - tianji_proxy_client.report_status:23 - INFO - Prepare to report st
atus, monitor=sls_etl_framework_monitor_app, level=good, description=, hostname=vm01002501825
0, server_role=sls-backend-server.FuxiServiceSlsEtlFramework#
2020-01-07 15:07:05,856 - 83648 - root - tianji_starter.do_check_conf_notify:214 - INFO - Check conf_not
ify, last_check_time=1576942460.83, cur_check_time=1576942460.83
```

2. Find the Job Scheduler machine.

```
/apsara/deploy/rpc_wrapper/rpc.sh spl EtlFramework
Partition | WorkerName                                    | LastUpdateTime          | status
66       | EtlFrameworkPartitionRole@a34h11080.cloud.h11.amtest87 | Sun Jan  5 16:03:01 2020 | loaded
62       | EtlFrameworkPartitionRole@a34h11080.cloud.h11.amtest87 | Sun Jan  5 16:03:01 2020 | loaded
111      | EtlFrameworkPartitionRole@a34h11080.cloud.h11.amtest87 | Sun Jan  5 16:03:01 2020 | loaded
113      | EtlFrameworkPartitionRole@a34h11080.cloud.h11.amtest87 | Sun Jan  5 16:03:01 2020 | loaded
```

3. Log on to the Job Scheduler machine without using a password.

```
ssh a34h11080.cloud.h11.amtest87
```

4. View the logs.

```
[root@a34h11078.cloud.h11.amtest87 /root]
#ls /apsara/tubo/TempRoot/sys/EtlFramework/EtlFrameworkPartitionRole@a34h11078.cloud.h11.amt
est87/etl_worker.LOG
/apsara/tubo/TempRoot/sys/EtlFramework/EtlFrameworkPartitionRole@a34h11078.cloud.h11.amtest
87/etl_worker.LOG
```

- /apsara/tubo/TempRoot/sys/: fixed directory
- EtlFramework: the service name obtained in Step 1.
- EtlFrameworkPartitionRole@a34h11078.cloud.h11.amtest87: the Job Scheduler machine name obtained in Step 2.
- etl_worker.LOG: the log name.

9.12.2.2. Use Log Service Portal to view logs

Project admin

Logstore	Log directory
metering	/tmp/metering_*.LOG metering.log
sls_service_error_log	/alidata/www/logs/java/sls-service/applog/error.log
sls_service_info_log	/alidata/www/logs/java/sls-service/applog/info.log
sls_console_error_log	/alidata/www/logs/java/slserror.log
sls_console_info_log	/alidata/www/logs/java/slsinfo.log
scmc_access_log	/apsara/nginx/logsscmc_access.log
scmc_err_log	/apsara/nginx/logs/scmc_err_log
scmc_op_log	/apsara/nginx/logs/scmc_op_log
sls_operation_agg_log	/apsara/fcgi_agent/metering_*.LOG
sls_operation_log	/apsara/fcgi_agent/ols_operation*.LOG
offline_scheduler_log	/apsara/sls/import_odps/scheduler/*.[Ll][Oo][Gg]
sls_fastcgi_log	/apsara/fcgi_agent/FastcgiAgent*.LOG
trace_log	/apsara/shennong_agent/tracer/index_worker_trace.LOG
dispatch_worker_log	/apsara/tubo/TempRoot/sys/DispatchWorker/[[user@ip]]/log_dispatch_worker.LOG
etl_framework_log	/apsara/tubo/TempRoot/sys/EtlFramework/[[user@ip]]/etl_worker.LOG
etl_golang_worker_log	/apsara/tubo/TempRoot/sys/EtlFramework/[[user@ip]]/etl_golang_worker.LOG
fc_trigger_log	/apsara/tubo/TempRoot/sys/FcTriggerWorker/[[user@ip]]/fc_trigger.log
query_master_log	/apsara/tubo/TempRoot/sys/QueryMaster/[[user@ip]]/query_master.LOG
sls_configservice_log	/apsara/tubo/TempRoot/sys/ConfigService/[[user@ip]]/sls_config_service.LOG

Logstore	Log directory
sls_configservice_query_log	/apsara/tubo/TempRoot/sys/ConfigService/[[user@ip]]/config_service_query.LOG
sls_consumergroup_log	/apsara/tubo/TempRoot/sys/QuotaServer/[[user@ip]]/monitor.LOG
sls_index_status_log	/apsara/tubo/TempRoot/sys/ShennongWorker/[[user@ip]]/project_index_size.LOG
sls_indexworker_log	/apsara/tubo/TempRoot/sys/OlsIndexWorker/[[user@ip]]/ols_index_worker.LOG
sls_loghub_shard_status_log	/apsara/tubo/TempRoot/sys/LoghubMaster/[[user@ip]]/loghub_master_meta.LOG
sls_loghubmaster_log	/apsara/tubo/TempRoot/sys/LoghubMaster/[[user@ip]]/sls_loghub_master.LOG
sls_quotaserver_log	/apsara/tubo/TempRoot/sys/QuotaServer/[[user@ip]]/quota_server.LOG
sls_quotausage_log	/apsara/tubo/TempRoot/sys/QuotaServer/[[user@ip]]/charge.LOG
sls_replayworker_log	/apsara/tubo/TempRoot/sys/ShennongReplayWorker/[[user@ip]]/shennong_replay_worker.LOG
sls_shennongworker_log	/apsara/tubo/TempRoot/sys/ShennongWorker/[[user@ip]]/shennong_worker.LOG
worker_input_log	/apsara/tubo/TempRoot/sys/ShennongWorker/[[user@ip]]/shennong_worker_input.LOG

Project scmg

Logstore	Log directory
scmg_access_log	/apsara/nginx/logs/scmg_access.log
nginx_error_log	/apsara/nginx/logs/error.log
scmg_err_log	/apsara/nginx/logs/scmg_err_log
scmg_op_log	/apsara/nginx/logs/scmg_op_log
sls_portal_access_log	/apsara/sls/web/logsaccess.log
sls_portal_http_req	/apsara/sls/web/logshttpclient.log
sls_portal_sys_info	/apsara/sls/web/logssysinfo.log
sls_portal_normal	/apsara/sls/web/logsnormal.log

Logstore	Log directory
sls_portal_api_audit	/apsara/sls/web/logsapidetail.log

9.13. Apsara Stack Security

9.13.1. Log on to the Apsara Infrastructure Management Framework console

This topic describes how to log on to the Apsara Infrastructure Management Framework console.

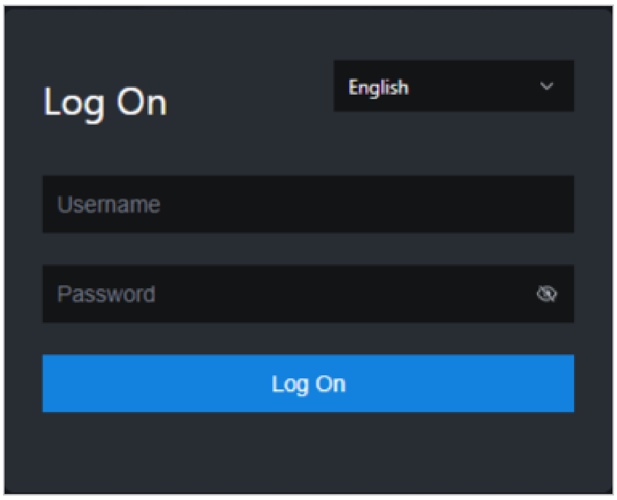
Prerequisites

- The URL, username, and password that are required to log on to the Apsara Uni-manager Operations Console are obtained from the deployment personnel or administrators.

  The URL of the Apsara Uni-manager Operations Console is in the format of *region-id*.ops.console.*intranet-domain-id*.
- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL. Then, press the Enter key.

   ⓘ **Note** You can select a language from the drop-down list in the upper-right corner of the page.
3. Enter your username and password.

   ⓘ **Note** To obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console, contact the deployment personnel or administrators.

If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username as prompted.

To enhance security, make sure that the password meets the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password is 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**. In the left-side navigation pane, choose **Product Management** > **Products**. In the **Apsara Stack O&M** section, click **Apsara Infrastructure Management Framework**.

9.13.2. Routine operations and maintenance of Server Guard

9.13.2.1. Check the service status

9.13.2.1.1. Check the client status

Check the following status information about the Server Guard client to verify that the client is running properly:

Client logs

Client logs are stored in the data directory under the directory of the Server Guard process file, for example, */usr/local/aegis/aegis_client/aegis_xx_xx/data*.

Client logs are saved by day, for example, *data.1 to data.7*

Client's online status

Run the following command to check the client's online status:

```
ps -aux | grep AliYunDun
```

Network connectivity

Run the following command to check whether the client has set up a TCP connection with the server:

```
netstat -tunpe |grep AliYunDun
```

Client UUID

Open the client log file data.x and check the character string following `Currentuid Ret`. This character string is the UUID of the current client.

Client processes

The Server Guard client has three resident processes: AliYunDun, AliYunDunUpdate, and AliHids.

When the client runs properly, all of the three processes run normally.

> **Note** On a Windows OS client, the AliYunDun and AliYunDunUpdate processes exist in the form of services. The service names are Server Guard Detect Service and Server Guard Update Service, respectively.

9.13.2.1.2. Check the status of Aegiserver

Context

To check the running status of Aegiserver, follow the following steps:

Procedure

1. Run the `ssh server IP address` command to log on to the server of Aegiserver.
2. Run the following command to find the Aegiserver image ID:

   ```
   docker ps -a |grep aegiserver
   ```

   The following message is displayed:

   ```
   b9e59994df41 reg.docker.alibaba-inc.com/aqs/aegiserverlite@sha256:f9d292f54c58646b672a8533a0d78fba534d26d376a194034e8840c70d9aa0b3 "/bin/bash /startApp." 2 hours ago Up 2 hours 80/tcp, 7001/tcp, 8005/tcp, 8009/tcp yundun-aegis.Aegiserverlite__.aegiserverlite. 1484712802
   ```

3. Run the following command to go to the Docker container:

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. Run the following command to check whether the Java process is normal:

   ```
   ps aux |grep aegiserver
   ```

   The following message is displayed:

   ```
   root 153 0.6 25.8 2983812 1084588 ? Sl 12:13 1:01 /opt/taobao/java/bin/java -Djava.util.logging.config.file=/home/admin/aegiserverlite/.default/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager -server -Xms2g -Xmx2g -XX:PermSize=96m -XX:MaxPermSize=384m -Xmn1g -XX:+UseConcMarkSweepGC -XX:+UseCMSCompactAtFullCollection -XX:CMSMaxAbortablePrecleanTime=5000 -XX:+CMSClassUnloadingEnabled -XX:+UseCMSInitiatingOccupancyOnly -XX:CMSInitiatingOccupancyFraction=80 -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/home/admin/logs/java.hprof -verbose:gc -Xloggc:/home/admin/logs/gc.log -XX:+PrintGCDetails -XX:+PrintGCDateStamps -Djava.awt.headless=true -Dsun.net.client.defaultConnectTimeout=10000 -Dsun.net.client.defaultReadTimeout=30000 -XX:+DisableExplicitGC -Dfile.encoding=UTF-8 -Ddruid.filters=mergeStat -Ddruid.useGloalDataSourceStat=true -Dproject.name=aegiserverlite -Dcatalina.vendor=alibaba -Djava.security.egd=file:/dev/./urandom -Dlog4j.defaultInitOverride=true -Dorg.apache.tomcat.util.http.ServerCookie.ALLOW_EQUALS_IN_VALUE=true -Dorg.apache.tomcat.util.http.ServerCookie.ALLOW_HTTP_SEPARATORS_IN_V0=true -Djava.endorsed.dirs=/opt/taobao/tomcat/endorsed -classpath /opt/taobao/tomcat/bin/bootstrap.jar:/opt/taobao/tomcat/bin/tomcat-juli.jar -Dcatalina.logs=/home/admin/aegiserverlite/.default/logs -Dcatalina.base=/home/admin/aegiserverlite/.default -Dcatalina.home=/opt/taobao/tomcat -Djava.io.tmpdir=/home/admin/aegiserverlite/.default/temp org.apache.catalina.startup.Bootstrap -Djboss.server.home.dir=/home/admin/aegiserverlite/.default -Djboss.server.home.url=file:/home/admin/aegiserverlite/.default start
   ```

5. Run the following command to perform the health check:

```
curl 127.0.0.1:7001/checkpreload.htm
```

If the response is "success", the service is normal.

6. View related logs.
   - **Protocol logs**: View logs about upstream and downstream protocol messages between the server and client in */home/admin/aegiserver/logs/AEGIS_MESSAGE.log*.
   - **Operation logs**: View abnormal stack information during operation in */home/admin/aegiserver/logs/aegis-default.log*.
   - **Offline logs**: View the logs about client disconnection caused by time-out in */home/admin/aegiserver/logs/AEGIS_OFFLINE_MESSAGE.log*.

9.13.2.1.3. Check the Server Guard Update Service status

Context

To check the status of Server Guard Update Service, follow the following steps:

Procedure

1. Run the `ssh host IP address` command to log on to the server of Aegiserver.
2. Run the following command to find the Aegiserver image ID:

   ```
   docker ps -a |grep aegiserver
   ```

3. Run the following command to go to the Docker container:

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. Run the following command to check whether the Java process is normal:

   ```
   ps aux |grep aegisupdate
   ```

5. Run the following command to perform the health check:

   ```
   curl 127.0.0.1:7001/checkpreload.htm
   ```

   If the response is "success", the service is normal.

9.13.2.1.4. Check the Defender module status

Context

To check the status of the Defender module of Server Guard, follow these steps:

Procedure

1. Run the `ssh server IP address` command to log on to the server that hosts the Defender module of Server Guard.
2. Run the following command to find the image ID of the Defender module of Server Guard:

   ```
   docker ps -a |grep defender
   ```

3. Run the following command to go to the Docker container:

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. Run the following command to check whether the Java process is normal:

```
ps aux |grep defender
```

5. Run the following command to perform health check:

   ```
   curl 127.0.0.1:7001/checkpreload.htm
   ```

   If the response is "success", the service is normal.

9.13.2.2. Restart Server Guard

Context

To restart Server Guard when a fault occurs, follow these steps:

Procedure

1. Run the `ssh server IP address` command to log on to the server that hosts Server Guard.
2. Run the following command to find the image ID of Server Guard:

   ```
   docker ps -a |grep application name
   ```

3. Run the following command to go to the Docker container:

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. Restart related services.
   - Restart the Server Guard client service.
     - For a server running a Windows OS, go to the service manager, locate *Server Guard Detect Service*, and restart this service.
     - For a server running a Linux OS, use either of the following methods to restart the Server Guard client service:
       - Run the `service aegis restart` command to restart the service.
       - Run the `killall AliYunDun` command as the root user to stop the current process, and then restart the */usr/local/aegis/aegis_client/aegis_xx_xx/AliYunDun* process.
   - Restart the Aegiserver service.
     a. Run the following command to view the Java process ID:

     ```
     ps aux |grep aegiserver
     ```

     b. Run the following command to stop the current process:

     ```
     kill -9 process
     ```

     c. Run the following command to restart the process:

     ```
     sudo -u admin /home/admin/aegiserever/bin/jbossctl restart
     ```

     d. Run the following command to check whether the process has been successfully restarted:

     ```
     curl 127.0.0.1:7001/checkpreload.htm
     ```

   - Restart Server Guard Update Service:
     a. Run the following command to view the Java process ID:

     ```
     ps aux |grep aegisupdate
     ```

   b. Run the following command to stop the current process:

      ```
      kill -9 process
      ```

   c. Run the following command to restart the process:

      ```
      sudo -u admin /home/admin/aegisupdate/bin/jbossctl restart
      ```

   d. Run the following command to check whether the process has been successfully restarted:

      ```
      curl 127.0.0.1:7001/checkpreload.htm
      ```

- Restart the Defender service of Server Guard.

   a. Run the following command to view the Java process ID:

      ```
      ps aux |grep secure-service
      ```

   b. Run the following command to stop the current process:

      ```
      kill -9 process
      ```

   c. Run the following command to restart the process:

      ```
      sudo -u admin /home/admin/secure-service/bin/jbossctl restart
      ```

   d. Run the following command to check whether the process has been successfully restarted:

      ```
      curl 127.0.0.1:7001/checkpreload.htm
      ```

9.13.3. Routine operations and maintenance of Network Traffic Monitoring System

9.13.3.1. Check the service status

9.13.3.1.1. Basic inspection

The basic inspection of Network Traffic Monitoring System checks whether the service status is normal.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
3. In the **Clusters** search box, enter **BeaverCluster**.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. On the **Services** tab, enter yundun-beaver-advance in the **Services** search box. Then, check whether the service status is normal.

9.13.3.1.2. Advanced inspection

The advanced inspection of Network Traffic Monitoring System checks the service status and features.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to the two physical machines of Network Traffic Monitoring System.

 i. In the left-side navigation pane, choose **Operations > Cluster Operations**.
 ii. In the **Clusters** search box, enter **BeaverCluster**. Then, click the cluster name. The **Cluster Details** page appears.
 iii. On the **Services** tab, enter **yundun-beaver-advance** in the **Services** search box. Then, click **Details**. The **Service Details** page appears.
 iv. In the **Service Role** search box, enter **BeaverAdvance#**.
 v. View the machine information, and click **Terminal** in the Actions column to log on to the two physical machines of Network Traffic Monitoring System.

3. Check the log status of Network Traffic Monitoring System. Run the `sudo cat /var/log/messages` command. If a record is returned, the log status is normal.
4. Check the status of mirrored traffic. Run the `sudo cat /proc/ixgbe_debug_info` command. If the value of **speed** in the second-to-last row is not 0, the mirrored traffic is normal.
5. Check the protected CIDR block in the log file. Run the `tail -f /dev/shm/banff-2018-xx.log` command. In the command, set *xx* to the month. For example, the log file for May in 2018 is named *banff-2018-05.log*. The CIDR block in the command output is an SLB or EIP CIDR block in the classic network. However, if the CIDR block is connected to Network Traffic Monitoring System through CSWs, a CIDR block in a VPC is returned.
6. Check the network connectivity between Network Traffic Monitoring System and a VM. Run the `ping VM IP address` command to check the network connectivity. In the command, set *VM IP address* to an IP address in the CIDR block returned in the previous step.
7. Check the tcp_decode process status. Run the `ps -ef | grep tcp_decode` command. If a record is returned, the tcp_decode process is normal.
8. Check configurations of the traffic scrubbing server. Run the `cat /home/admin/beaver-dj-schedule/conf/dj.conf` command. Check whether the value of the ip parameter in the aliguard_smart field that is not commented out is set to the DNS virtual IP address mapped to the aliguard.${global:internet-domain} domain name.
9. View the following logs:
    - DDoS alert logs

      Run the `grep -A 10 -B 10 LIDS /var/log/messages` command to view the DDoS alert logs.
    - TCP intercept command logs

      Run the `grep add_to_blacklist.htm /var/log/messages` command to view the TCP intercept command logs.
    - Outbound attack logs

      Run the `grep zombie_new /var/log/messages` command to view the outbound attack logs.

9.13.3.2. Common operations and maintenance

9.13.3.2.1. Restart the Network Traffic Monitoring System process

Context

To restart the Network Traffic Monitoring System process, follow the following steps:

Procedure

1. Log on to the physical machine of Network Traffic Monitoring System.
2. Switch to the root account.
3. Run the following command to restart the Network Traffic Monitoring System process: `rm -rf /dev/shm/drv_setup_path`

9.13.3.2.2. Uninstall Network Traffic Monitoring System

Context

To uninstall Network Traffic Monitoring System, follow the following steps:

Procedure

1. Log on to a physical machine of Network Traffic Monitoring System.
2. Switch to the root account.
3. Run the following command to uninstall Network Traffic Monitoring System:

   ```
   bash /opt/beaver/bin/uninstall.sh
   ```

9.13.3.2.3. Disable TCP blocking

Context

To disable TCP blocking for Network Traffic Monitoring System, follow the following steps:

Procedure

1. Log on to a physical machine of Network Traffic Monitoring System.
2. Switch to the root account.
3. Open the */beaver_client.sh* file on each server of Network Traffic Monitoring System, and add a number sign (`#`) to the start of the `./tcp_reset` line to comment out the line.
4. Run the following command on each server of Network Traffic Monitoring System to disable TCP blocking:

   ```
   killall tcp_reset
   ```

9.13.3.2.4. Enable TCPDump

Context

To enable TCPDump for Network Traffic Monitoring System, follow the following steps:

Procedure

1. Log on to a physical machine of Network Traffic Monitoring System.
2. Switch to the root account.
3. Run the following command to enable TCPDump:

   ```
   echo 1 > /proc/ixgbe_debug_dispatch
   ```

> Note
>
> When TCPDump is enabled, the performance of Network Traffic Monitoring System may be affected. We recommend that you run the following command to disable TCPDump after packet capture is complete.
>
> ```
> echo 0 > /proc/ixgbe_debug_dispatch
> ```

9.13.4. Routine operations and maintenance of Anti-DDoS Service

9.13.4.1. Check the service status

9.13.4.1.1. Basic inspection

The basic inspection of Traffic Scrubbing checks whether the service status is normal.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations > Cluster Operations**.
3. In the **Clusters** search box, enter **AliguardCluster**.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. On the **Services** tab, enter yundun-aliguard in the **Services** search box. Then, check whether the service status is normal.

9.13.4.1.2. Advanced inspection

The advanced inspection of Traffic Scrubbing checks the service status and features.

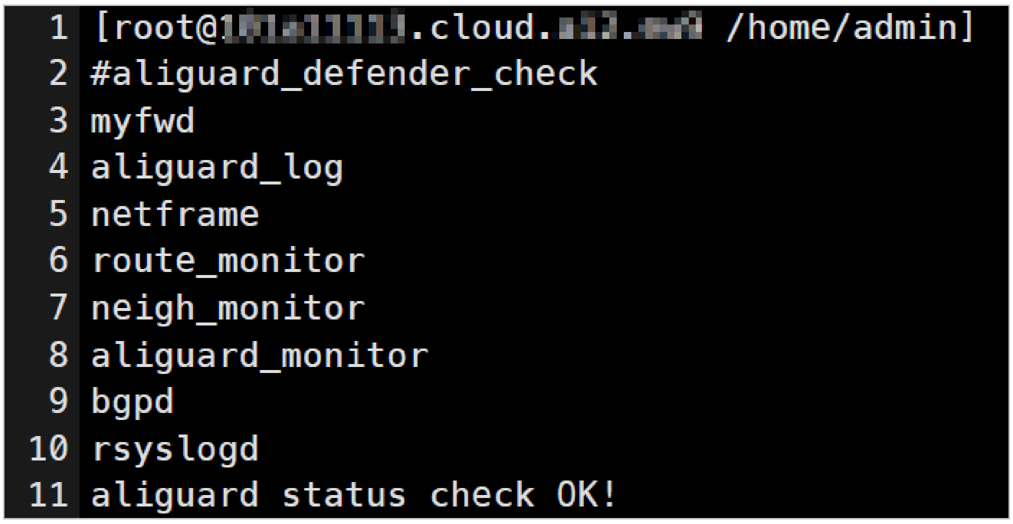
Procedure

1. Log on to the two physical machines of Traffic Scrubbing.
   i. Log on to the Apsara Infrastructure Management Framework console. In the left-side navigation pane, choose **Operations > Cluster Operations**.
   ii. In the **Clusters** search box, enter **AliguardCluster**. Then, click the cluster name. The **Cluster Details** page appears.
   iii. On the **Services** tab, enter **yundun-aliguard** in the **Services** search box. Then, click **Details**. The **Service Details** page appears.
   iv. In the **Service Role** search box, enter **AliguardConsole#**.
   v. View the machine information, and click **Terminal** in the Actions column to log on to the two physical machines of Traffic Scrubbing.
2. Check the deployment status of Traffic Scrubbing. Run the `/home/admin/aliguard/target/AliguardDefender/bin/aliguard_defender_check` command and check the command output.

> ⓘ **Note** If the host of Traffic Scrubbing has just restarted, wait for 3 to 5 minutes before you run the command to check the deployment status.

- If `aliguard status check OK!` is returned, Traffic Scrubbing is properly deployed, and its service status is normal, as shown in the Traffic Scrubbing status figure.

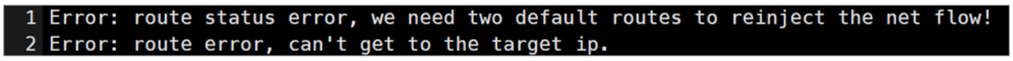
  Traffic Scrubbing status

  ```
  [root@1[redacted].cloud.[redacted] /home/admin]
  #aliguard_defender_check
  myfwd
  aliguard_log
  netframe
  route_monitor
  neigh_monitor
  aliguard_monitor
  bgpd
  rsyslogd
  aliguard status check OK!
  ```

- If the error message shown in Reinjection route error message is returned, the reinjection route is incorrect.

  Reinjection route error message

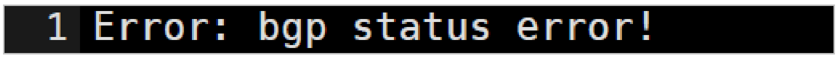
  

  ```
  Error: route status error, we need two default routes to reinject the net flow!
  Error: route error, can't get to the target ip.
  ```

  Troubleshooting: The reinjection route is a default route generated by Traffic Scrubbing. Its next hop is the ISW interface that is bound to the VPN. If an error occurs, check whether this route is generated by Traffic Scrubbing. If the route is generated, check ISW configurations to determine whether the route to downstream devices is available.

- If the error message shown in BGP route error message is returned, the BGP route is incorrect.

  BGP route error message

  ```
  Error: bgp status error!
  ```

  Troubleshooting: If the BGP route is incorrect, troubleshoot the error based on the following operations:

  a. Check whether the BGP neighbor is normal on the ISW.

  b. Check whether the destination of the BGP route is an attacked IP address with a 32-bit subnet mask and the next hop of the BGP route is the Traffic Scrubbing address.

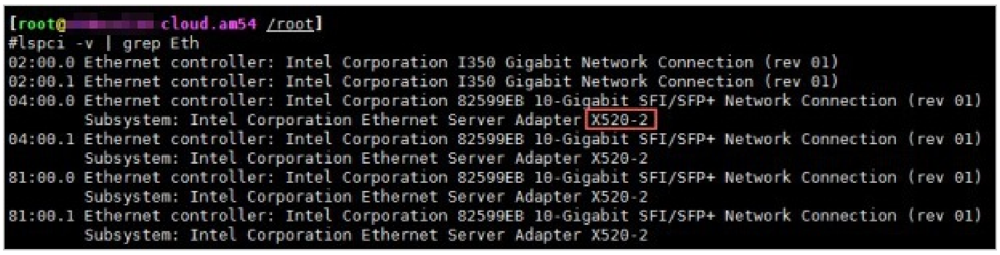
  c. Check whether the BGP routing policy on the ISW is correct.

- If other errors are reported, the core process is faulty. Contact Alibaba Cloud technical support.

3. Check the status of the NICs or optical modules of Traffic Scrubbing.

> ⓘ **Note** Traffic Scrubbing must use NICs or optical modules equipped with Intel X520 or Intel 82599.

Run the `lspci | grep Eth` command. Information containing Intel X520 or Intel 82599 is returned.



```
[root@[redacted] cloud.am54 /root]
#lspci -v | grep Eth
02:00.0 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
02:00.1 Ethernet controller: Intel Corporation I350 Gigabit Network Connection (rev 01)
04:00.0 Ethernet controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection (rev 01)
        Subsystem: Intel Corporation Ethernet Server Adapter X520-2
04:00.1 Ethernet controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection (rev 01)
        Subsystem: Intel Corporation Ethernet Server Adapter X520-2
81:00.0 Ethernet controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection (rev 01)
        Subsystem: Intel Corporation Ethernet Server Adapter X520-2
81:00.1 Ethernet controller: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection (rev 01)
        Subsystem: Intel Corporation Ethernet Server Adapter X520-2
```

9.13.4.2. Common operations and maintenance

9.13.4.2.1. Restart Anti-DDoS Service

Context

To restart Anti-DDoS Service when an error occurs, follow the following steps:

Procedure

1. Run the `ssh server IP address` command to log on to the server that hosts Anti-DDoS Service.
2. Run the following command to stop Anti-DDoS Service: `/home/admin/aliguard/target/AliguardDefender/bin/aliguard stop`

   > **Note** If the `ERROR: Module net_msg is in use` message is displayed, run the command again later. If Anti-DDoS Service cannot be stopped after several attempts, restart the server of Anti-DDoS Service.

3. Run the following command to restart Anti-DDoS Service: `/home/admin/aliguard/target/AliguardDefender/bin/aliguard start`
4. Run the service status check command five minutes after Anti-DDoS Service is restarted.

9.13.4.2.2. Troubleshoot common faults

Context

When an error occurs in Anti-DDoS Service, follow the following troubleshooting steps:

Procedure

1. Restart Anti-DDoS Service.
   - If Anti-DDoS Service is in the normal status after being restarted but an error message is returned during the health check performed later, non-standard NICs or optical modules are used. To check whether standard NICs or optical modules are used, see Check the status of the NICs or optical modules of Anti-DDoS Service. If non-standard NICs or optical modules are used, change the NICs or optical modules.
   - If Anti-DDoS Service is in an unusual status after being restarted, go to the next step.
2. View the `aliguard_dynamic_config` file. Carefully check whether each configuration item in the file

is exactly the same as that in the plan.

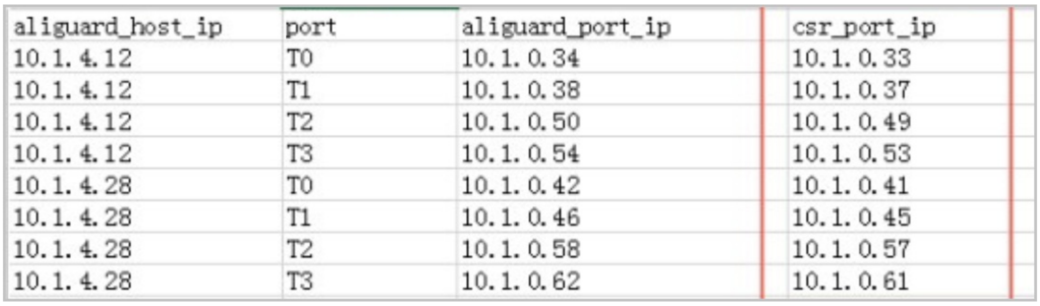
> Note Ensure that the AS number specified in `aliguard local` is 65515 and that the BGP password is correct.

3. Check the wiring and switch configuration.

> Note If any incorrect configuration is found, the current fault is caused by incorrect wiring or switch IP address configuration, rather than incorrect deployment of Anti-DDoS Service. In this case, contact the network engineer.

Assume that the Anti-DDoS Service configurations to be checked are listed in the following figure, among which the server IP address is 10.1.4.12. To check whether the four ports of Anti-DDoS Service can ping the ports of the switch, follow the following steps:

Anti-DDoS Service configuration example



aliguard_host_ip	port	aliguard_port_ip	csr_port_ip
10.1.4.12	T0	10.1.0.34	10.1.0.33
10.1.4.12	T1	10.1.0.38	10.1.0.37
10.1.4.12	T2	10.1.0.50	10.1.0.49
10.1.4.12	T3	10.1.0.54	10.1.0.53
10.1.4.28	T0	10.1.0.42	10.1.0.41
10.1.4.28	T1	10.1.0.46	10.1.0.45
10.1.4.28	T2	10.1.0.58	10.1.0.57
10.1.4.28	T3	10.1.0.62	10.1.0.61

i. Run the following commands to check the NIC PCI IDs of Anti-DDoS Service:

```
cd /sys/bus/pci/drivers/igb_uio
```

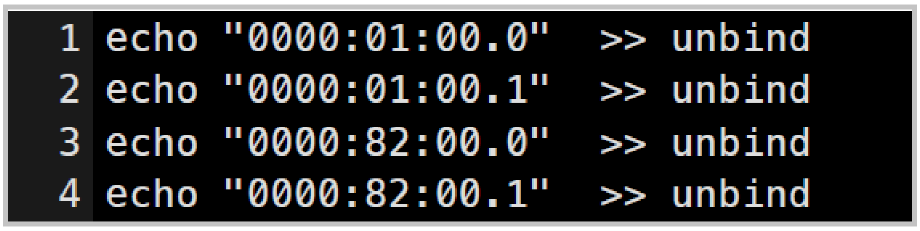
```
ls
```

Record the PCI IDs of the four NICs, for example, 0000:01:00.0, 0000:01:00.1, 0000:82:00.0, and 0000:82:00.1.

ii. Run the `/home/admin/aliguard/target/AliguardDefender/bin/aliguard stop` command to stop Anti-DDoS Service.

iii. In the /sys/bus/pci/drivers/igb_uio directory, unbind the four NICs recorded in the first step from the igb_uio driver, as shown in Unbind NICs.

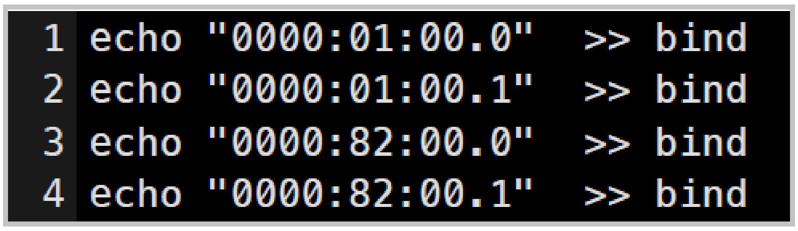
Unbind NICs



```
echo "0000:01:00.0"  >> unbind
echo "0000:01:00.1"  >> unbind
echo "0000:82:00.0"  >> unbind
echo "0000:82:00.1"  >> unbind
```

iv. In the /sys/bus/pci/drivers/ixgbe directory, bind the four NICs to the ixgbe driver for Linux, as shown in Bind NICs.

Bind NICs



```
echo "0000:01:00.0"  >> bind
echo "0000:01:00.1"  >> bind
echo "0000:82:00.0"  >> bind
echo "0000:82:00.1"  >> bind
```

v. Set Anti-DDoS Service IP addresses for the NICs.

The local server IP address is 10.1.4.12, and the NIC IP addresses are set to 10.1.0.34, 10.1.0.38, 10.1.0.50, and 10.1.0.54, as shown in Anti-DDoS Service configuration example.

a. Run the `ifconfig-a` command to display all NICs, and run the `ethtool -i` command to view the PCI ID of each NIC. Find the four NICs of which the IDs are the same as those recorded in the first step, for example, eth0, eth1, eth2, and eth3.

b. Run the following commands to move these NICs to the top of the queue:

```
ifconfig eth0 up
ifconfig eth1 up
ifconfig eth2 up
ifconfig eth3 up
```

c. Set Anti-DDoS Service IP addresses for the NICs. Run the following commands to set Anti-DDoS Service IP addresses for the NICs based on their PCI IDs in an ascending order:

```
ifconfig eth0 10.1.0.34 netmask 255.255.255.252
ifconfig eth1 10.1.0.38 netmask 255.255.255.252
ifconfig eth2 10.1.0.50 netmask 255.255.255.252
ifconfig eth3 10.1.0.54 netmask 255.255.255.252
```

vi. Try to ping the peer IP addresses configured. If the peer IP addresses cannot be pinged, the switch configuration or wiring is incorrect.

```
ping 10.1.0.33
ping 10.1.0.37
ping 10.1.0.49
ping 10.1.0.53
```

vii. If these four IP addresses can all be pinged, you can directly start Anti-DDoS Service without unbinding the NICs.

Run the `/home/admin/aliguard/target/AliguardDefender/bin/aliguard start` command to start Anti-DDoS Service.

After Anti-DDoS Service has been started for a while, run the `/home/admin/aliguard/target/AliguardDefender/bin/aliguard_rule -v 0.0.0.0 -d drop_icmp` command to disable the drop_icmp policy.

viii. Ping the peer IP addresses again.

```
ping 10.1.0.33
ping 10.1.0.37
ping 10.1.0.49
ping 10.1.0.53
```

If the peer IP addresses cannot be pinged, non-standard NICs or optical modules are used or the configuration is incorrect.

4. If these four peer IP addresses can be pinged after Anti-DDoS Service is started but an error is reported during a status check of Anti-DDoS Service, contact Alibaba Cloud technical support.

9.13.5. Routine operations and maintenance of Threat Detection Service

9.13.5.1. Check the service status

9.13.5.1.1. Basic inspection

The basic inspection of Threat Detection Service (TDS) checks whether the service status is normal.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
3. In the **Clusters** search box, enter **BasicThinCluster**.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. On the **Services** tab, enter yundun-sas in the **Services** search box. Then, check whether the service status is normal.

9.13.5.1.2. Advanced inspection

The advanced inspection of Threat Detection Service (TDS) checks the service status and features.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to the two physical machines of TDS.
   i. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
   ii. In the **Clusters** search box, enter **BasicThinCluster**. Then, click the cluster name. The **Cluster Details** page appears.
   iii. On the **Services** tab, enter **yundun-sas** in the **Services** search box. Then, click **Details**. The **Service Details** page appears.
   iv. In the **Service Role** search box, enter **SasApp#**.
   v. View the machine information, and click **Terminal** in the Actions column to log on to the two physical machines of TDS.

3. Log on to the two Docker containers of TDS. Run the `sudo docker exec -it $(sudo docker ps | grep sas | awk '{print $1}') bash` command.
4. Check the service process status. Run the `ps aux |grep sas` command. If a record is returned, the process is normal.
5. Check the health status. Run the `curl 127.0.0.1:3008/check.htm` command. If ok is returned, the service is normal.
6. View logs.
   - View all logs in the */home/admin/sas/logs/sas-default.log* file, including metaq message logs, execution logs of scheduled tasks, and error logs. You can locate TDS faults based on these logs.
   - View info logs generated when TDS is running in the */home/admin/sas/logs/common-default.log* file.
   - View TDS error logs in the */home/admin/sas/logs/common-error.log* file.
   - View logs about metaq messages received by TDS in the */home/admin/sas/logs/SAS_LOG.log* file.

     > **Note** Asset verification is performed on messages in this log file. Therefore, the number of messages in this log file is less than that in the sas-default.log file.

   - View logs generated when the alert contact sends alert notifications in the */home/admin/sas/logs/notify.log* file.

9.13.5.2. Restart Threat Detection Service

Context

When a fault occurs, you can restart Threat Detection Service (TDS).

Procedure

1. Run the `ssh Host IP address` command to log on to the host of TDS.
2. Run the following command to find the image ID of TDS:

   ```
   docker ps -a |grep sas
   ```

3. Run the following command to enter the Docker container:

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. Run the following command to find the Java process:

   ```
   ps aux |grep sas
   ```

5. Run the following command to stop the process:

   ```
   kill -9 Process ID
   ```

6. Run the following command to restart the process:

   ```
   sudo -u admin /home/admin/sas/bin/jbossctl restart
   ```

7. Run the following command to check whether the process is restarted:

   ```
   curl 127.0.0.1:7001/check.htm
   ```

9.13.6. Routine operations and maintenance of Cloud Firewall

9.13.6.1. Check the service status

To check the running status of the Cloud Firewall server, follow the following steps:

Procedure

1. Run the **ssh server IP address** command to log on to the server that hosts Cloud Firewall.
2. Run the following command to find the image ID of the Cloud Firewall server: `sudo docker ps | grep cloudfirewall`

   The following message is displayed:

   ```
   af8a1a182a17    reg.docker.aliyun-inc.com/yundun-advance/cloudfirewall:696dcf568512deceb7199dc4c
   9aa70855e66aca71244296cf13bfaf4a0897ebe    "/bin/bash /home/admi"    23 hours ago    Up 23 hours    yu
   ndun-cloudfirewall.CloudFirewallApp__.cloudfirewall-app. 1523453835
   ```

3. Run the following command to go to the Docker container: `docker exec –it [imageId] /bin/bash`
4. Run the following command to check whether the Java process is normal: `ps aux |grep cloudfirewall`

   The following message is displayed:

   ```
   admin 118 0.5 28.2 6261808 2368828 ? Sl Apr11 8:06 /opt/taobao/java/bin/java -Djava.util.logging.config.
   file=/home/admin/cloud-fi
   rewall/.default/conf/logging.properties -Djava.util.logging.manager=org.apache.juli.ClassLoaderLogMa
   nager -server -Xms4g -Xmx4g -XX:PermSize=96m -XX:MaxPermSize=384m -Xmn2g -XX:+UseConcMarkSwe
   epGC -XX:+UseCMSCompactAtFullCollection -XX:CMSMaxAbortablePrecleanTime=5000 -XX:+CMSClassU
   nloadingEnabled -XX:+UseCMSInitiatingOccupancyOnly -XX:CMSInitiatingOccupancyFraction=80 -XX:+H
   eapDumpOnOutOfMemoryError -XX:HeapDumpPath=/home/admin/logs/java.hprof -verbose:gc -Xloggc:
   /home/admin/logs/gc.log -XX:+PrintGCDetails -XX:+PrintGCDateStamps -Djava.awt.headless=true -Dsun
   .net.client.defaultConnectTimeout=10000 -Dsun.net.client.defaultReadTimeout=30000 -XX:+DisableExp
   licitGC -Dfile.encoding=UTF-8 -Ddruid.filters=mergeStat -Ddruid.useGloalDataSourceStat=true -Dproje
   ct.name=cloud-firewall -Dhsf.server.port=21015 -Djdk.tls.ephemeralDHKeySize=2048 -Dcatalina.vendor
   =alibaba -Djava.security.egd=file:/dev/./urandom -Dlog4j.defaultInitOverride=true -Dorg.apache.tomca
   t.util.http.ServerCookie.ALLOW_EQUALS_IN_VALUE=true -Dorg.apache.tomcat.util.http.ServerCookie.
   ALLOW_HTTP_SEPARATORS_IN_V0=true -Dcatalina.logs=/home/admin/cloud-firewall/.default/logs -Dig
   nore.endorsed.dirs= -classpath /opt/taobao/tomcat/bin/bootstrap.jar:/opt/taobao/tomcat/bin/tomcat
   -juli.jar -Dcatalina.base=/home/admin/cloud-firewall/.default -Dcatalina.home=/opt/taobao/tomcat -Dj
   ava.io.tmpdir=/home/admin/cloud-firewall/.default/temp org.apache.catalina.startup.Bootstrap -Djbo
   ss.server.home.dir=/home/admin/cloud-firewall/.default -Djboss.server.home.url=file:/home/admin/clo
   ud-firewall/.default startroot 4931 0.0 0.0 61208 764 ? S+ 21:32 0:00 grep cloud-firewall
   ```

5. Run the following command to perform the health check: `curl 127.0.0.1:2015/cloud-firewall/check_health`

   If OK is returned, the service is normal.

6. View related logs.
   - View the routine printing logs of the Cloud Firewall server in */home/admin/cloud-firewall/logs/cl*

oud-firewall-info.log.

- View the error printing logs of the Cloud Firewall server in */home/admin/cloud-firewall/logs/cloud-firewall-error.log*.
- View the logs returned after Cloud Firewall calls OpenAPI in */home/admin/cloud-firewall/logs/cloud-firewall-openApi.log*.

9.13.6.2. Restart Cloud Firewall

To restart Cloud Firewall when an error occurs, follow the following steps:

Procedure

1. Run the **ssh server IP address** command to log on to the server that hosts Cloud Firewall.
2. Run the following command to find the image ID of Cloud Firewall: `sudo docker ps | grep cloudfirewall`
3. Run the following command to go to the Docker container: `docker exec –it [imageId] /bin/bash`
4. Restart Cloud Firewall.
   1. Run the following command to view the Java process ID: `ps -aux | grep cloud-firewall`
   2. Run the following command to stop the current process: `kill -9 process`
   3. Run the following command to restart the process: `sudo –u admin /home/admin/cloud-firewall/bin/jbossctl restart`
   4. Run the following command to check whether the process has been successfully restarted: `curl 127.0.0.1:2015/cloud-firewall/check_health`

      If OK is returned, the service is normal.

9.13.7. Routine operations and maintenance of WAF

9.13.7.1. Check the service status

9.13.7.1.1. Basic inspection

The basic inspection of Web Application Firewall (WAF) checks whether the service status is normal.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations > Cluster Operations**.
3. In the **Clusters** search box, enter **SemaWafCluster**.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. On the **Services** tab, enter yundun-semawaf in the **Services**. Then, check whether the service status is normal.

9.13.7.1.2. Advanced inspection

The advanced inspection of Web Application Firewall (WAF) checks the system status and service status.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to the two physical machines of WAF.
    i. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
    ii. In the **Clusters** search box, enter **SemaWafCluster**. Then, click the cluster name. The **Cluster Details** page appears.
    iii. On the **Services** tab, enter **yundun-semawaf** in the **Services** search box. Then, click **Details**. The **Service Details** page appears.
    iv. In the **Service Role** search box, enter **YundunSemawafApp#**.
    v. View the machine information, and click **Terminal** in the Actions column to log on to the two physical machines of WAF.
3. Check the system status.
    i. View system logs. Run the `dmesg -T |tail -30` command to check for exception logs.
    ii. Check the system loads.
        - Run the `free -h` command to check whether the memory usage is normal.
        - Run the `df -h` command to check whether the disk usage is normal.
        - Run the `uptime` command to check whether the average system load is normal.
        - Run the `top` command to check whether the CPU utilization is normal.
4. Check the service status.

> **Note** Perform the following operations in the WAF installation directory, which is */home/safeline* by default.

    i. Run the `cd /home/safeline` command to open the installation directory.
    ii. Check the minion service.
        a. Run the `systemctl status minion` command to check the execution time and status of the Minion service.
        b. Run the `tail -100 logs/minion/minion.log` command to check for exception logs.
    iii. Check the mgt-api service.
        a. Run the `docker logs --tail 50 mgt-api` command to check for exception logs.
        b. Run the `docker exec -it mgt-api supervisorctl status` command to check whether the service properly runs and whether uptime is normal.
        c. Run the `tail -50 logs/management/gunicorn.log` command to check for exception logs.
        d. Run the `tail -50 logs/management/daphne.log` command to check for exception logs.
        e. Run the `tail -50 logs/management/scheduler.log` command to check for exception logs.
        f. Run the `tail -50 logs/management/dramatiq.log` command to check for exception logs.

iv. Check the redis service. Run the `docker logs --tail 50 mgt-redis` command to check for exception logs.

v. Check the detector service.

   a. Run the `docker logs --tail 50 detector-srv` command to check for exception logs.

   b. Run the `tail -50 logs/detector/snserver.log` command to check for exception logs.

   c. Run the `curl 127.0.0.1:8001/stat | grep num` command to check whether the service responds and whether the real-time request processing data is normal. For example, check the req_num_total parameter, which indicates the number of requests that were processed within the last 5 seconds.

vi. Check the tengine service.

   a. Run the `docker logs --tail 50 tengine` command to check for exception logs.

   b. Run the `tail -50 logs/nginx/error.log` command to check for exception logs.

vii. Check the mario service.

   a. Run the `docker logs --tail 50 mario` command to check for exception logs.

   b. Run the `tail -50 logs/mario/mario.log` command to check for exception logs.

   c. Run the `curl 127.0.0.1:3335/api/v1/state` command to check whether the service responds and whether the real-time request processing data is normal. For example, check whether the num_pending parameter remains at a high value of nearly 10,000 or whether the num_processed_last_10s parameter, which indicates the number of requests that were processed within the last 10 seconds, is normal.

9.13.8. Routine operations and maintenance of Sensitive Data Discovery and Protection

9.13.8.1. Check the service status

9.13.8.1.1. Basic inspection

During the basic inspection of Sensitive Data Discovery and Protection (SDDP), check whether the service has reached the final status.

Procedure

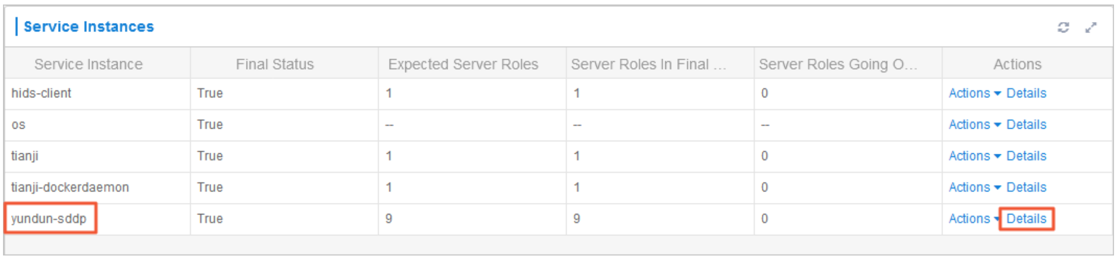
1. Log on to the Apsara Infrastructure Management Framework console.
2. Choose **Operations > Project Operations**.
3. In the **Fuzzy Search** field, enter *yundun-sddp*.
4. Click **Details** in the **Actions** column of the yundun-sddp project to go to the **Cluster Operations** page.
5. In the cluster list, click the cluster name that starts with **SddpCluster**.
6. In the **Service Instances** section of the **Cluster Dashboard** page, check whether the **yundun-sddp** service instance is in the final status.

9.13.8.1.2. Advanced inspection: Check the status of the SddpService service

This topic describes how to check the running status of the SddpService service.

Procedure

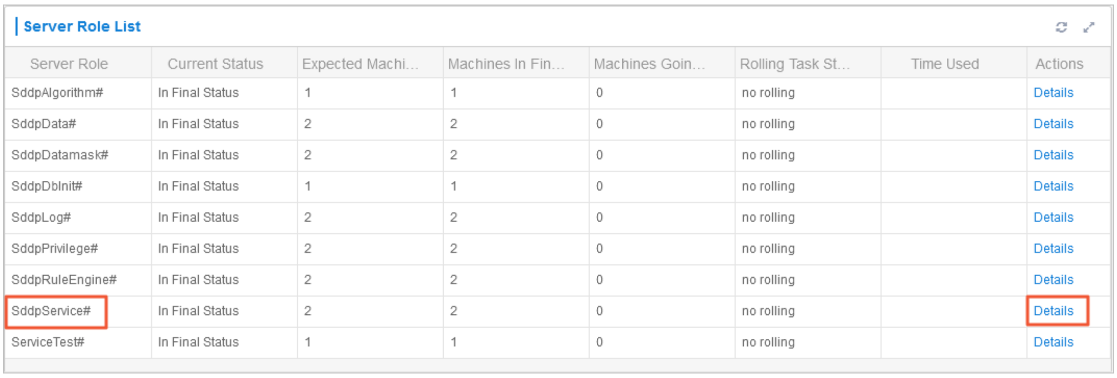
1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to the two physical servers of Sensitive Data Discovery and Protection (SDDP), respectively.
   i. Choose **Operations > Project Operations**.
   ii. In the **Fuzzy Search** field, enter *yundun-sddp*. Click **Details** in the **Actions** column of the yundun-sddp project to go to the **Cluster Operations** page.
   iii. In the cluster list, click the cluster name that starts with **SddpCluster**.
   iv. In the Service Instances section, find **yundun-sddp** and click **Details** in the **Actions** column to go to the **Service Instance Information Dashboard** page.



Service Instances

Service Instance	Final Status	Expected Server Roles	Server Roles In Final ...	Server Roles Going O...	Actions
hids-client	True	1	1	0	Actions ▾ Details
os	True	--	--	--	Actions ▾ Details
tianji	True	1	1	0	Actions ▾ Details
tianji-dockerdaemon	True	1	1	0	Actions ▾ Details
yundun-sddp	True	9	9	0	Actions ▾ Details

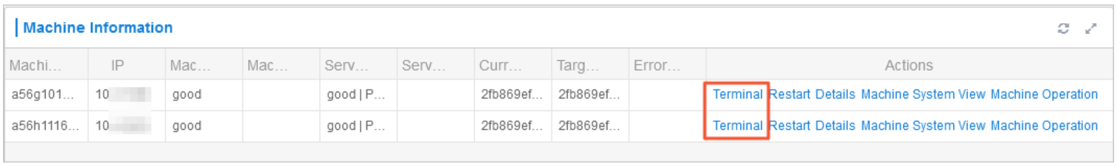
   v. In the **Server Role List** section, find **SddpService#** and click **Details** in the **Actions** column to go to the **Server Role Dashboard** page.



Server Role List

Server Role	Current Status	Expected Machi...	Machines In Fin...	Machines Goin...	Rolling Task St...	Time Used	Actions
SddpAlgorithm#	In Final Status	1	1	0	no rolling		Details
SddpData#	In Final Status	2	2	0	no rolling		Details
SddpDatamask#	In Final Status	2	2	0	no rolling		Details
SddpDbInit#	In Final Status	1	1	0	no rolling		Details
SddpLog#	In Final Status	2	2	0	no rolling		Details
SddpPrivilege#	In Final Status	2	2	0	no rolling		Details
SddpRuleEngine#	In Final Status	2	2	0	no rolling		Details
SddpService#	In Final Status	2	2	0	no rolling		Details
ServiceTest#	In Final Status	1	1	0	no rolling		Details

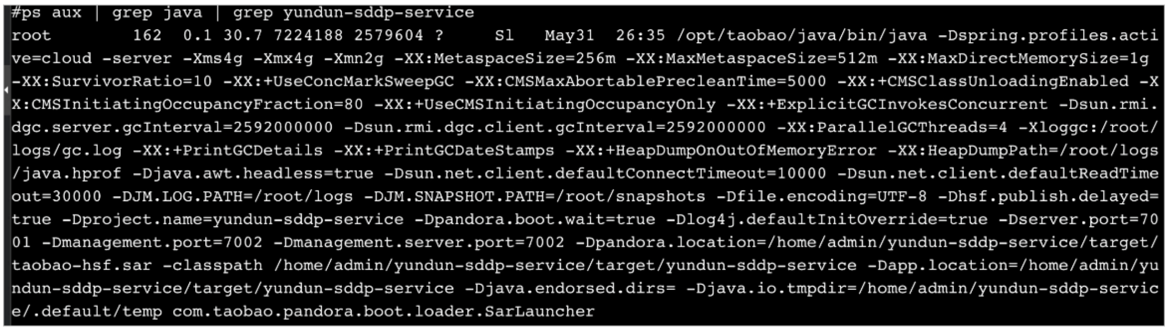
   vi. In the **Machine Information** section, click **Terminal** in the **Actions** column to log on to the two physical servers of SDDP, respectively.



Machine Information

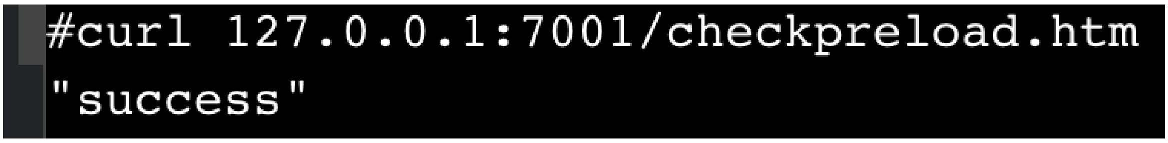
Machi...	IP	Mac...	Mac...	Serv...	Serv...	Curr...	Targ...	Error...	Actions
a56g101...	10[redacted]	good		good | P...		2fb869ef...	2fb869ef...		Terminal Restart Details Machine System View Machine Operation
a56h1116...	10[redacted]	good		good | P...		2fb869ef...	2fb869ef...		Terminal Restart Details Machine System View Machine Operation

3. Log on to two Docker containers of the SddpService service, respectively. Run the `sudo docker exec -it $(sudo docker ps | grep SddpService | awk '{print $1}') bash` command.
4. Check the process status of the SddpService service. Run the `ps aux | grep java | grep yundun-sddp-service` command. If any record is returned, the service is normal.



```
#ps aux | grep java | grep yundun-sddp-service
root        162  0.1 30.7 7224188 2579604 ?     Sl   May31  26:35 /opt/taobao/java/bin/java -Dspring.profiles.acti
ve=cloud -server -Xms4g -Xmx4g -Xmn2g -XX:MetaspaceSize=256m -XX:MaxMetaspaceSize=512m -XX:MaxDirectMemorySize=1g
-XX:SurvivorRatio=10 -XX:+UseConcMarkSweepGC -XX:CMSMaxAbortablePrecleanTime=5000 -XX:+CMSClassUnloadingEnabled -X
X:CMSInitiatingOccupancyFraction=80 -XX:+UseCMSInitiatingOccupancyOnly -XX:+ExplicitGCInvokesConcurrent -Dsun.rmi.
dgc.server.gcInterval=2592000000 -Dsun.rmi.dgc.client.gcInterval=2592000000 -XX:ParallelGCThreads=4 -Xloggc:/root/
logs/gc.log -XX:+PrintGCDetails -XX:+PrintGCDateStamps -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/root/logs
/java.hprof -Djava.awt.headless=true -Dsun.net.client.defaultConnectTimeout=10000 -Dsun.net.client.defaultReadTime
out=30000 -DJM.LOG.PATH=/root/logs -DJM.SNAPSHOT.PATH=/root/snapshots -Dfile.encoding=UTF-8 -Dhsf.publish.delayed=
true -Dproject.name=yundun-sddp-service -Dpandora.boot.wait=true -Dlog4j.defaultInitOverride=true -Dserver.port=70
01 -Dmanagement.port=7002 -Dmanagement.server.port=7002 -Dpandora.location=/home/admin/yundun-sddp-service/target/
taobao-hsf.sar -classpath /home/admin/yundun-sddp-service/target/yundun-sddp-service -Dapp.location=/home/admin/yu
ndun-sddp-service/target/yundun-sddp-service -Djava.endorsed.dirs= -Djava.io.tmpdir=/home/admin/yundun-sddp-servic
e/.default/temp com.taobao.pandora.boot.loader.SarLauncher
```

5. Check the health status. Run the `curl 127.0.0.1:7001/checkpreload.htm` command. If the response is **success**, the service is normal.



```
#curl 127.0.0.1:7001/checkpreload.htm
"success"
```

6. View related logs.
   - View common logs in the */home/admin/yundun-sddp-service/logs/common-log.log* file.
   - View application logs in the */home/admin/yundun-sddp-service/logs/application.log* file.
   - View front-end request logs in the */home/admin/yundun-sddp-service/logs/common-request.log* file.
   - View system logs in the */home/admin/yundun-sddp-service/logs/service-stdout.log* file.

9.13.8.1.3. Advanced inspection: Check the status of the SddpData service

This topic describes how to check the running status of the SddpData service.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to the two physical servers of Sensitive Data Discovery and Protection (SDDP), respectively.
   i. Choose **Operations** > **Project Operations**.
   ii. In the **Fuzzy Search** field, enter *yundun-sddp*. Click **Details** in the **Actions** column of the yundun-sddp project to go to the **Cluster Operations** page.
   iii. In the cluster list, click the cluster name that starts with **SddpCluster**.
   iv. In the **Service Instances** section, find **yundun-sddp** and click **Details** in the **Actions** column to go to the **Service Instance Information Dashboard** page.
   v. In the **Server Role List** section, find **SddpData#** and click **Details** in the **Actions** column to go to the **Server Role Dashboard** page.
   vi. In the **Machine Information** section, click **Terminal** in the **Actions** column to log on to the two physical servers of SDDP, respectively.
3. Log on to two Docker containers of the SddpData service, respectively. Run the `sudo docker exec -it $(sudo docker ps | grep SddpData | awk '{print $1}') bash` command.
4. Check the process status of the SddpData service. Run the `ps aux | grep yundun-sddp-data`

command. If any record is returned, the service is normal.

5. View related logs. View logs in the */home/admin/yundun-sddp-data/logs/sddp.log* file.

9.13.8.1.4. Advanced inspection: Check the status of the SddpPrivilege service

This topic describes how to check the running status of the SddpPrivilege service.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to the two physical servers of Sensitive Data Discovery and Protection (SDDP), respectively.
   i. Choose **Operations** > **Project Operations**.
   ii. In the **Fuzzy Search** field, enter *yundun-sddp*. Click **Details** in the **Actions** column of the yundun-sddp project to go to the **Cluster Operations** page.
   iii. In the cluster list, click the cluster name that starts with **SddpCluster**.
   iv. In the **Service Instances** section, find **yundun-sddp** and click **Details** in the **Actions** column to go to the **Service Instance Information Dashboard** page.
   v. In the **Server Role List** section, find **SddpPrivilege#** and click **Details** in the **Actions** column to go to the **Server Role Dashboard** page.
   vi. In the **Machine Information** section, click **Terminal** in the **Actions** column to log on to the two physical servers of SDDP, respectively.
3. Log on to two Docker containers of the SddpPrivilege service, respectively. Run the `sudo docker exec -it $(sudo docker ps | grep SddpPrivilege | awk '{print $1}') bash` command.
4. Check the process status of the SddpPrivilege service. Run the `ps aux | grep java | grep yundun-sddp-privilege` command. If any record is returned, the service is normal.
5. Check the health status. Run the `curl 127.0.0.1:7001/checkpreload.htm` command. If the response is **success**, the service is normal.
6. View related logs.
   - View exception logs in the */home/admin/yundun-sddp-privilege/logs/exception.log* file.
   - View application logs in the */home/admin/yundun-sddp-privilege/logs/application.log* file.
   - View task logs in the */home/admin/yundun-sddp-privilege/logs/task.log* file.
   - View system logs in the */home/admin/yundun-sddp-privilege/logs/service-stdout.log* file.

9.13.8.1.5. Advanced inspection: Check the status of the SddpLog service

This topic describes how to check the running status of the SddpLog service.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to the two physical servers of Sensitive Data Discovery and Protection (SDDP), respectively.

   i. Choose **Operations** > **Project Operations**.
   ii. In the **Fuzzy Search** field, enter *yundun-sddp*. Click **Details** in the **Actions** column of the yundun-sddp project to go to the **Cluster Operations** page.
   iii. In the cluster list, click the cluster name that starts with **SddpCluster**.
   iv. In the **Service Instances** section, find **yundun-sddp** and click **Details** in the **Actions** column to go to the **Service Instance Information Dashboard** page.
   v. In the **Server Role List** section, find **SddpLog#** and click **Details** in the **Actions** column to go to the **Server Role Dashboard** page.
   vi. In the **Machine Information** section, click **Terminal** in the **Actions** column to log on to the two physical servers of SDDP, respectively.

3. Log on to two Docker containers of the SddpLog service, respectively. Run the `sudo docker exec -it $(sudo docker ps | grep SddpLog | awk '{print $1}') bash` command.
4. Check the process status of the SddpLog service. Run the `ps aux | grep java | grep yundun-sddp-log`. If any record is returned, the service is normal.
5. Check the health status. Run the `curl 127.0.0.1:7001/checkpreload.htm` command. If the response is **success**, the service is normal.
6. View related logs.
   - View exception logs in the */home/admin/yundun-sddp-log/logs/exception.log* file.
   - View application logs in the */home/admin/yundun-sddp-log/logs/application.log* file.
   - View debug logs in the */home/admin/yundun-sddp-log/logs/debug.log* file.
   - View system logs in the */home/admin/yundun-sddp-log/logs/service-stdout.log* file.

9.13.8.2. Restart SDDP

This topic describes how to restart Sensitive Data Discovery and Protection (SDDP) when a fault occurs.

Procedure

1. Run the `ssh Server IP address` command to log on to the server that hosts SDDP.
2. Run the following command to find the image ID of the service:

```
docker ps -a |grep service name
```

3. Run the following command to log on to the Docker container:

```
docker exec -it [imageId] /bin/bash
```

4. Restart related services.
   - Restart the yundun-sddp-service service.
     a. Run the following command to stop the current process:

```
kill -9 $(ps -ef | grep java | grep yundun-sddp-service | grep -v grep | awk '{print$2}')
```

     b. Run the following command to restart the process:

```
/bin/bash /home/admin/start.sh
```

c. Run the following command to check whether the process is restarted:

```
curl 127.0.0.1:7001/check.htm
```

If the response is **success**, the service is normal.

- Restart the yundun-sddp-log service.

a. Run the following command to stop the current process:

```
kill -9 $(ps -ef | grep java | grep yundun-sddp-log | grep -v grep | awk '{print $2}')
```

b. Run the following command to restart the process:

```
/bin/bash /home/admin/start.sh
```

c. Run the following command to check whether the process is restarted:

```
curl 127.0.0.1:7001/check.htm
```

If the response is **success**, the service is normal.

- Restart the yundun-sddp-privilege service.

a. Run the following command to stop the current process:

```
kill -9 $(ps -ef | grep java | grep yundun-sddp-privilege | grep -v grep | awk '{print $2}')
```

b. Run the following command to restart the process:

```
/bin/bash /home/admin/start.sh
```

c. Run the following command to check whether the process is restarted:

```
curl 127.0.0.1:7001/check.htm
```

If the response is **success**, the service is normal.

- Restart the yundun-sddp-data service.

a. Run the following command to stop the current process:

```
kill -9 $(ps -ef | grep yundun-sddp-data | grep -v grep | awk '{print $2}')
```

b. Run the following command to restart the process:

```
/bin/bash /home/admin/yundun-sddp-data/start.sh
```

c. Check whether the process is restarted.

Run the `ps aux | grep yundun-sddp-data` command. If any record is returned, the service is normal.

9.13.9. Routine operations and maintenance of Apsara Stack Security Center

9.13.9.1. Check service status

9.13.9.1.1. Basic inspection

During the basic inspection of Apsara Stack Security Center, check whether the service has reached the final status.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Choose **Operations > Project Operations**. Enter *yundun-advance*, and click Details to go to the Cluster Operations page.
3. Select **BasicCluster**.
4. Check whether yundun-secureconsole has reached the final status in **Service Instances List**.

9.13.9.1.2. Advanced inspection

Check the running status of Apsara Stack Security Center.

Context

To check the running status of Apsara Stack Security Center, follow the following steps:

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to two physical machines, respectively.
   i. Choose **Operations > Project Operations**.
   ii. Enter *yundun-advance*, and click **Details** to go to the Cluster Operations page.
   iii. Select **BasicCluster**.
   iv. Select **yundun-secureconsole** from Service Instances List, and click **Details** to go to the **Service Instance Dashboard** page.
   v. Select **SecureConsoleApp#** from Service Role List, and click **Details** to go to the **Service Role Dashboard** page.
   vi. View Server Information, and use TerminalService to log on to two physical machines, respectively.
3. Log on to two secure-console Docker containers, respectively. Run `sudo docker exec -it $(sudo docker ps | grep secureconsole | awk '{print $1}') bash` .
4. Check the console progress status. Run `ps aux |grep console` . If any record is returned, the console progress is normal.
5. Check the health status. Run `curl 127.0.0.1:3014/check.htm` . If `OK` is returned, the service is normal.
6. View related logs.
   - View the Tomcat logs in */home/admin/console/logs/jboss_stdout.log*.

9.13.9.2. Restart the secure-console service

Context

To restart the secure-console service when an error occurs, follow the following steps:

Procedure

1. Run the `ssh server IP address` command to log on to the server that hosts the secure-console service.

2. Run the following command to find the image ID of the secure-console service:

   ```
   sudo docker ps -a |grep console
   ```

3. Run the following command to go to the Docker container:

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. Run the following command to locate the Java process:

   ```
   ps aux |grep console
   ```

5. Run the following command to stop the current process:

   ```
   kill -9 process
   ```

6. Run the following command to restart the process:

   ```
   sudo -u admin /home/admin/console/bin/jbossctl restart
   ```

7. Run the following command to check whether the process has been successfully restarted:

   ```
   curl 127.0.0.1:7001/check.htm
   ```

9.13.10. Routine operations and maintenance of secure-service

9.13.10.1. Check the service status

9.13.10.1.1. Basic inspection

During the basic inspection of secure-service, check whether the service has reached the final status.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Choose **Operations** > **Project Operations**. On the page that appears, enter *yundun-advance*, and click Details to go to the Cluster Operations page.
3. Select **BasicCluster**.
4. Check whether yundun-secureservice has reached the final status in **Service Instances List**.

9.13.10.1.2. Advanced inspection: Check the secure-service status

This topic describes how to check the secure-service running status.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to two physical machines, respectively.
   1. Choose **Operations** > **Project Operations**.
   2. Enter *yundun-advance*, and click **Details** to go to the Cluster Operations page.
   3. Select **BasicCluster**.

   iv. Select **yundun-secureservice** from Service Instances List, and click **Details** to go to the **Service Instance Dashboard** page.

   v. Select **SecureServiceApp#** from Service Role List, and click **Details** to go to the **Service Role Dashboard** page.

   vi. View Server Information, and click Terminal to log on to two physical machines, respectively.

3. Log on to two secure-service Docker containers, respectively. Run `sudo docker exec -it $(sudo docker ps | grep secureservice | awk '{print $1}') bash` .
4. Check the secure-service process status. Run `ps aux |grep secure-service` . If any record is returned, the secure-service process is normal.
5. Check the health status. Run `curl 127.0.0.1:3010` . If `OK` is returned, the service is normal.
6. Run the following command to go to the Docker container:

   ```
   sudo docker exec -it [imageId] /bin/bash
   ```

7. View related logs.
   - View the Server Guard logs in */home/admin/secure-service/logs/aegis-info.log*.
   - View the error logs in */home/admin/secure-service/logs/Error*.
   - View the vulnerability analysis and scanning logs in */home/admin/secure-service/logs/leakage-info.log*.
   - View the cloud intelligence logs in */home/admin/secure-service/logs/threat-info.log*.
   - View the web attack logs in */home/admin/secure-service/logs/web-info.log*.

9.13.10.1.3. Check the Dolphin service status

Context

To check the running status of the Dolphin service, follow the following steps:

Procedure

1. Run the `ssh server IP address` command to log on to the server that hosts the Dolphin service.
2. Run the following command to find the image ID of the Dolphin service:

   ```
   sudo docker ps -a |grep dolphin
   ```

3. Run the following command to go to the Docker container:

   ```
   sudo docker exec -it [imageId] /bin/bash
   ```

4. Run the following command to check whether the Java process is normal:

   ```
   ps aux |grep dolphin
   ```

5. Run the following command to perform the health check:

   ```
   curl 127.0.0.1:7001/checkpreload.htm
   ```

   If the response is "success", the service is normal.

6. View related logs.
   - View the info logs generated when the Dolphin service is running in */home/admin/dolphin/logs/common-default.log*.
   - View the Dolphin service error logs in */home/admin/dolphin/logs/common-error.log*.

  - View the metaq messages received by the Dolphin service in */home/admin/dolphin/logs/dolphin-message-consumer.log*.

    > **Note** Currently, only Threat Detection Service (TDS) sends messages to the Dolphin service.

  - View the metaq messages sent by the Dolphin service in */home/admin/dolphin/logs/dolphin-message-producer.log*.

    > **Note** Currently, the Dolphin service sends messages only to TDS.

9.13.10.1.4. Check the data-sync service status

Context

To check the running status of the data-sync service, follow these steps:

Procedure

1. Run the `ssh server IP address` command to log on to the server that hosts the data-sync service.
2. Run the following command to find the image ID of the data-sync service:

   ```
   sudo docker ps -a |grep data-sync
   ```

3. Run the following command to go to the Docker container:

   ```
   sudo docker exec -it [imageId] /bin/bash
   ```

4. Run the following command to check whether the Java process is normal:

   ```
   ps aux |grep data-sync
   ```

5. Run the following command to perform health check:

   ```
   curl 127.0.0.1:7001/check_health
   ```

   If OK is returned, the service is normal.

6. View related logs.

   View the data-sync service logs in *data-sync.log*.

9.13.10.2. Restart secure-service

Context

To restart secure-service when a fault occurs, follow the following steps:

Procedure

1. Run the `ssh server IP address` command to log on to the server of the service.
2. Run the following command to find the image ID of the service:

   ```
   docker ps -a |grep application name
   ```

3. Run the following command to go to the Docker container:

   ```
   docker exec -it [imageId] /bin/bash
   ```

4. Restart related services.
   - Restart secure-service.
     a. Run the following command to view the Java process ID:
        ```
        ps aux |grep secure-service
        ```
     b. Run the following command to stop the current process:
        ```
        kill -9 process
        ```
     c. Run the following command to restart the process:
        ```
        sudo -u admin /home/admin/secure-service/bin/jbossctl restart
        ```
     d. Run the following command to check whether the process has been successfully restarted:
        ```
        curl 127.0.0.1:7001
        ```
   - Restart the Dolphin service.
     a. Run the following command to view the Java process ID:
        ```
        ps aux |grep dolphin
        ```
     b. Run the following command to stop the current process:
        ```
        kill -9 process
        ```
     c. Run the following command to restart the process:
        ```
        sudo -u admin /home/admin/dolphin/bin/jbossctl restart
        ```
     d. Run the following command to check whether the process has been successfully restarted:
        ```
        curl 127.0.0.1:7001/checkpreload.htm
        ```
   - Restart the data-sync service.
     a. Run the following command to view the Java process ID:
        ```
        ps aux |grep data-sync
        ```
     b. Run the following command to stop the current process:
        ```
        kill -9 process
        ```
     c. Run the following command to restart the process:
        ```
        sudo -u admin /home/admin/data-sync/bin/jbossctl restart
        ```
     d. Run the following command to check whether the process has been successfully restarted:
        ```
        curl 127.0.0.1:7001/check_health
        ```

9.14. Key Management Service (KMS)

9.14.1. O&M of KMS components

9.14.1.1. Overview

You can deploy KMS and perform O&M on KMS components in the Apsara Infrastructure Management Framework console.

You can log on to the machine where KMS resides from **Machine Operations** in the Apsara Infrastructure Management Framework console.

9.14.1.2. Log on to the Apsara Infrastructure Management Framework console

This topic describes how to log on to the Apsara Infrastructure Management Framework console.

Prerequisites

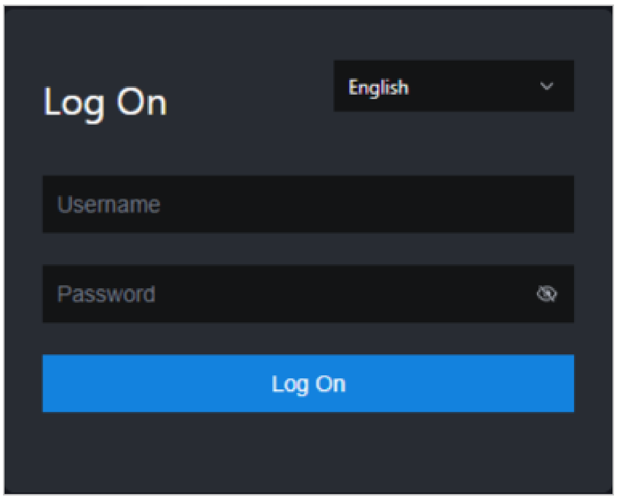
- The URL of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from a deployment engineer or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the format of *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL. Then, press the Enter key.



> **Note** You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

> **Note** Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from a deployment engineer or an administrator.

When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

To ensure security, your password must meet the complexity requirements. The password must be 10 to 20 characters in length. It must contain the following character types: uppercase letters, lowercase letters, digits, and special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).

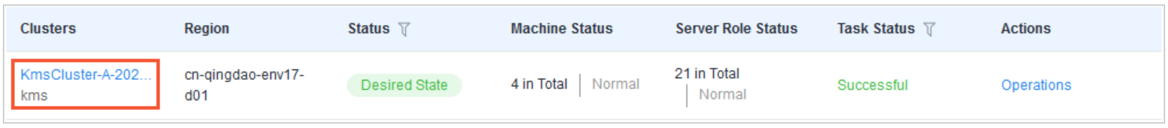
4. Click **Log On** to log on to the Apsara Uni-manager Operations Console.
5. In the top navigation bar, click **O&M**.
6. In the left-side navigation pane, choose **Product Management > Products**.
7. In the **Apsara Stack O&M** section, click **Apsara Infrastructure Management Framework**.

9.14.1.3. KMS_HOST

This topic describes how to check the status of the KMS_HOST service.

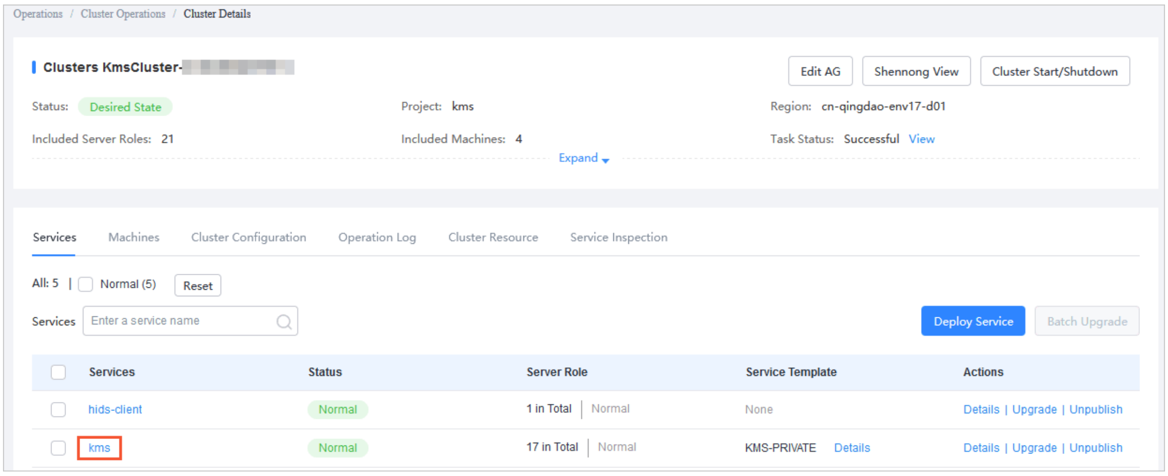
Check whether the server role is normal

1. Log on to the Apsara Infrastructure Management Framework console. For more information, see Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations > Cluster Operations**.
3. On the **Cluster Operations** page, search for the Key Management Service (KMS) cluster.



Clusters	Region	Status	Machine Status	Server Role Status	Task Status	Actions
KmsCluster-A-202... kms	cn-qingdao-env17-d01	Desired State	4 in Total | Normal	21 in Total | Normal	Successful	Operations

4. Click the link in the Clusters column to go to the **Cluster Details** page.
5. On the **Services** tab, click **kms** in the Service column to go to the **Service Details** page.



Operations / Cluster Operations / Cluster Details

Clusters KmsCluster-[redacted]

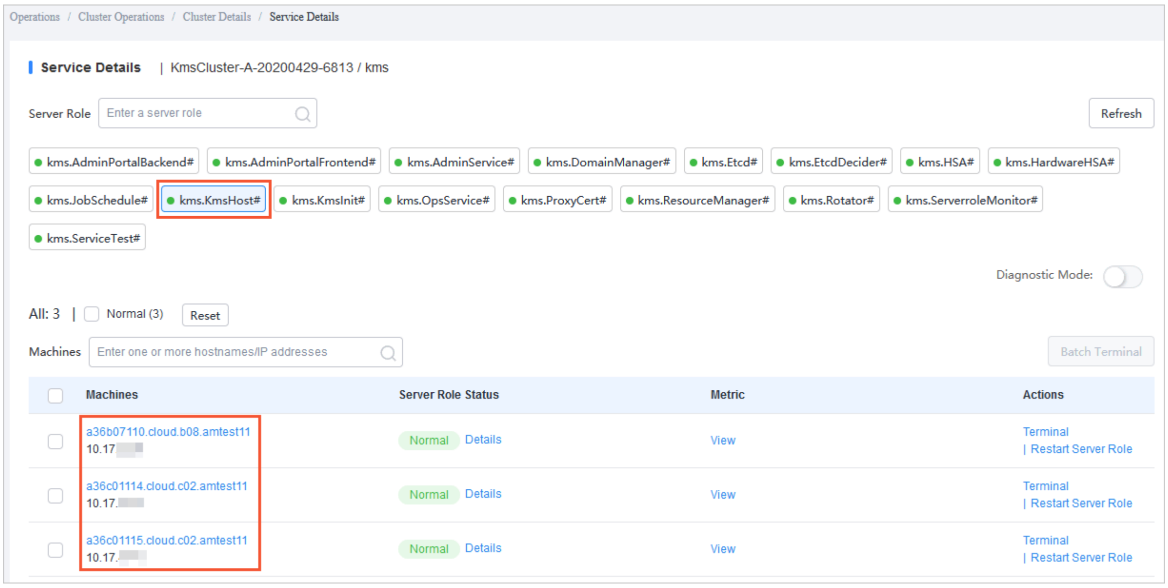
Status: Desired State
Project: kms
Region: cn-qingdao-env17-d01
Included Server Roles: 21
Included Machines: 4
Task Status: Successful View

All: 5 | □ Normal (5) Reset

Services: Enter a service name

□	Services	Status	Server Role	Service Template	Actions
□	hids-client	Normal	1 in Total | Normal	None	Details | Upgrade | Unpublish
□	kms	Normal	17 in Total | Normal	KMS-PRIVATE Details	Details | Upgrade | Unpublish

6. On the **Service Details** page, check whether the KMS_HOST server role is at desired state. If the indicator for the kms.KmsHost# server role is green, the server role is at desired state.
7. On the **Service Details** page, click **kms.KmsHost#**. The information of the machines on which the KMS_HOST service is deployed is displayed in the lower part of the page. The IP addresses of the machines are required in subsequent steps.



Operations / Cluster Operations / Cluster Details / Service Details

Service Details | KmsCluster-A-20200429-6813 / kms

Server Role: Enter a server role

● kms.AdminPortalBackend# ● kms.AdminPortalFrontend# ● kms.AdminService# ● kms.DomainManager# ● kms.Etcd# ● kms.EtcdDecider# ● kms.HSA# ● kms.HardwareHSA# ● kms.JobSchedule# ● kms.KmsHost# ● kms.KmsInit# ● kms.OpsService# ● kms.ProxyCert# ● kms.ResourceManager# ● kms.Rotator# ● kms.ServerroleMonitor# ● kms.ServiceTest#

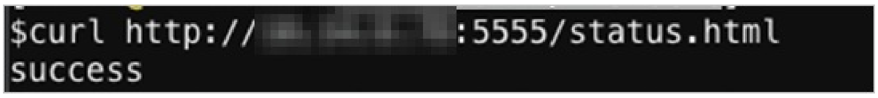
Diagnostic Mode: ○

All: 3 | □ Normal (3) Reset

Machines: Enter one or more hostnames/IP addresses

□	Machines	Server Role Status	Metric	Actions
□	a36b07110.cloud.b08.amtest11 10.17[redacted]	Normal Details	View	Terminal | Restart Server Role
□	a36c01114.cloud.c02.amtest11 10.17.[redacted]	Normal Details	View	Terminal | Restart Server Role
□	a36c01115.cloud.c02.amtest11 10.17.[redacted]	Normal Details	View	Terminal | Restart Server Role

8. Click **Terminal** in the Actions column for a machine to log on to this machine.
9. Run the `curl http://ip:5555/status.html` command and check whether the success message is returned.



```
$curl http://[redacted]:5555/status.html
success
```

> Note
> - Replace ip in the command with the IP address of this machine you obtained in Step 7.
> - Use this method to verify all machines on which the KMS_HOST service is deployed.

Troubleshooting

1. View logs in the */cloud/log/kms/KmsHost#/kms_host* directory.
2. Check whether the KMS_HOST service is running normally.
   - If KMS_HOST abnormally exits after it starts, view debug logs in the *debug.log* file to troubleshoot the specific error.
   - If KMS_HOST is running but does not function normally, view status logs in the *status.log* file to troubleshoot the specific error.

Possible errors

Error	Troubleshooting
`xxx selfCheck error` Note *xxx* indicates a dependency service.	• Check whether the dependency configuration is valid. You can view debug logs in the *debug.log* file to troubleshoot the specific error. • Check whether the xxx service runs normally.

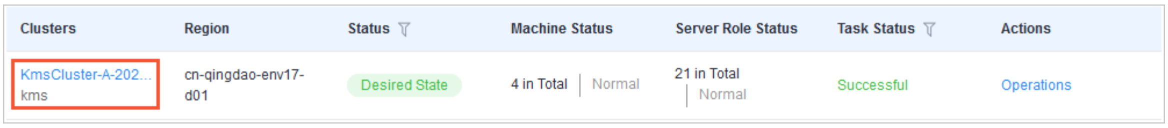
Error	Troubleshooting
exit code 1	View debug logs in the *debug.log* file to identify the cause of the abnormal exit.

9.14.1.4. HSA

This topic describes how to check the status of the HSA service.

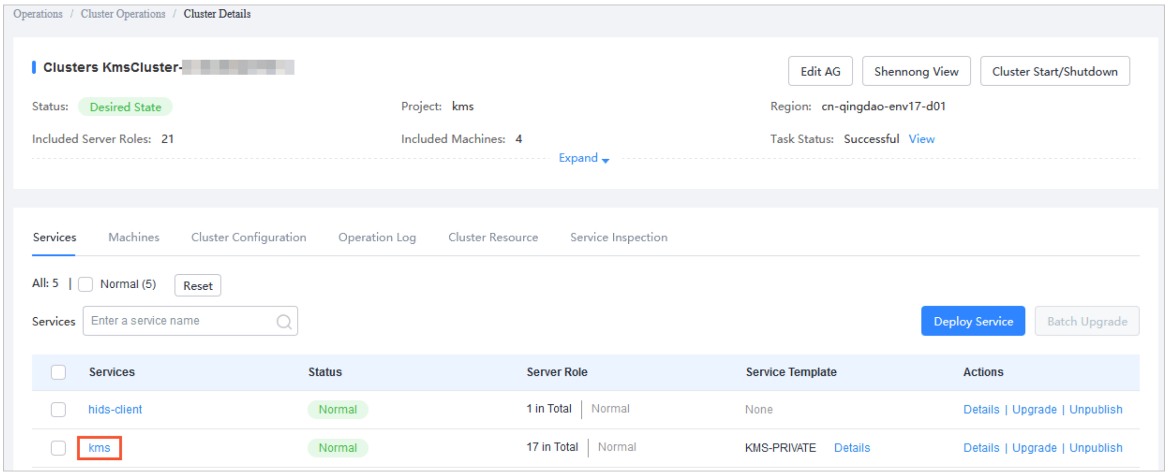
Check whether the server role is normal

1. Log on to the Apsara Infrastructure Management Framework console. For more information, see Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations > Cluster Operations**.
3. On the **Cluster Operations** page, search for the Key Management Service (KMS) cluster.



Clusters	Region	Status	Machine Status	Server Role Status	Task Status	Actions
KmsCluster-A-202... kms	cn-qingdao-env17-d01	Desired State	4 in Total | Normal	21 in Total | Normal	Successful	Operations

4. Click the link in the Clusters column to go to the **Cluster Details** page.
5. On the **Services** tab, click **kms** in the Service column to go to the **Service Details** page.



Operations / Cluster Operations / Cluster Details

Clusters KmsCluster-[redacted]

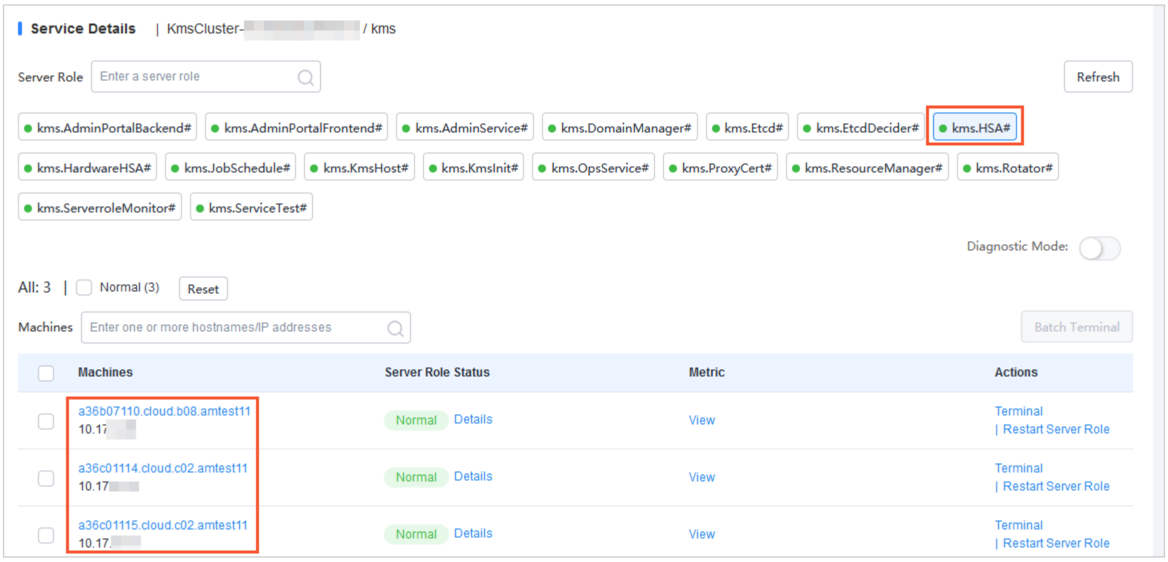
Status: Desired State
Project: kms
Region: cn-qingdao-env17-d01
Included Server Roles: 21
Included Machines: 4
Task Status: Successful View

All: 5 | □ Normal (5) Reset

Services: Enter a service name

□	Services	Status	Server Role	Service Template	Actions
□	hids-client	Normal	1 in Total | Normal	None	Details | Upgrade | Unpublish
□	kms	Normal	17 in Total | Normal	KMS-PRIVATE Details	Details | Upgrade | Unpublish

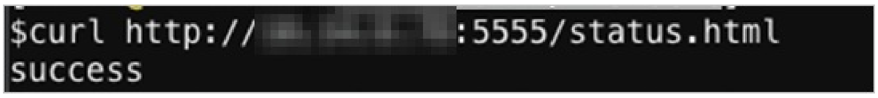
6. On the **Service Details** page, check whether the HSA server role is at desired state. If the indicator for the kms.HSA# server role is green, the server role is at desired state.
7. On the **Service Details** page, click **kms.HSA#**. The information of the machines on which the HSA service is deployed is displayed in the lower part of the page. The IP addresses of the machines are required in subsequent steps.



Machines	Server Role Status	Metric	Actions
a36b07110.cloud.b08.amtest11 10.17[redacted]	Normal Details	View	Terminal | Restart Server Role
a36c01114.cloud.c02.amtest11 10.17[redacted]	Normal Details	View	Terminal | Restart Server Role
a36c01115.cloud.c02.amtest11 10.17[redacted]	Normal Details	View	Terminal | Restart Server Role

8. Click **Terminal** in the Actions column for a machine to log on to this machine.

9. Run the `curl http://ip:5555/status.html` command and check whether the success message is returned.



```
$curl http://[redacted]:5555/status.html
success
```

> **Note**
>
> - Replace ip in the command with the IP address of this machine you obtained in Step 7.
> - Use this method to verify all machines on which the HSA service is deployed.

Troubleshooting

1. View logs in the */cloud/log/kms/HSA#/hsa* directory.
2. Check whether the HSA service is running normally.
   - If the HSA service abnormally exits after it starts, view debug logs in the *debug.log* file to troubleshoot the specific error.
   - If the HSA service is running but does not function normally, view status logs in the *status.log* file to troubleshoot the specific error.

Possible errors

Error: `exit code 1`

Troubleshooting: View debug logs in the debug.log file to identify the cause of the abnormal exit. This error can be caused by one of the following reasons:

- The etcd service does not start normally.
- The etcd service starts normally, but its data is invalid.

> **Note** During disaster recovery, synchronization errors in the secondary cluster may cause this error.

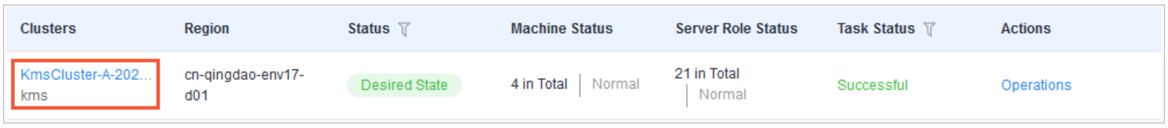
9.14.1.5. ETCD

This topic describes how to check the status of the etcd service.

Check whether the server roles are normal

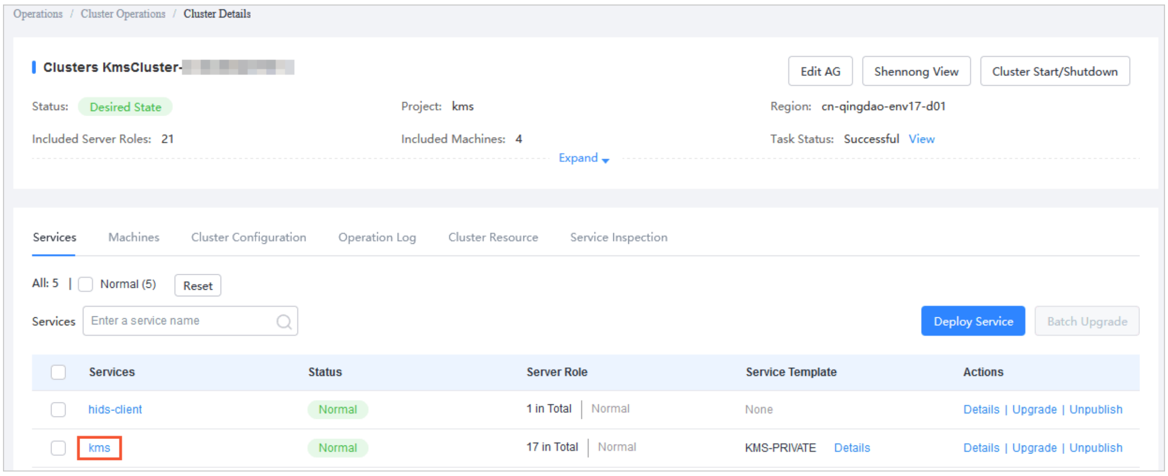
In the Apsara Infrastructure Management Framework console, check whether the Etcd and EtcdDecider server roles are at desired state.

1. Log on to the Apsara Infrastructure Management Framework console. For more information, see Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
3. On the **Cluster Operations** page, search for the Key Management Service (KMS) cluster.



Clusters	Region	Status	Machine Status	Server Role Status	Task Status	Actions
KmsCluster-A-202... kms	cn-qingdao-env17-d01	Desired State	4 in Total | Normal	21 in Total | Normal	Successful	Operations

4. Click the link in the Clusters column to go to the **Cluster Details** page.
5. On the **Services** tab, click **kms** in the Service column to go to the **Service Details** page.



Operations / Cluster Operations / Cluster Details

Clusters KmsCluster-[redacted]

Edit AG | Shennong View | Cluster Start/Shutdown

Status: Desired State
Project: kms
Region: cn-qingdao-env17-d01
Included Server Roles: 21
Included Machines: 4
Task Status: Successful View

Expand

Services | Machines | Cluster Configuration | Operation Log | Cluster Resource | Service Inspection

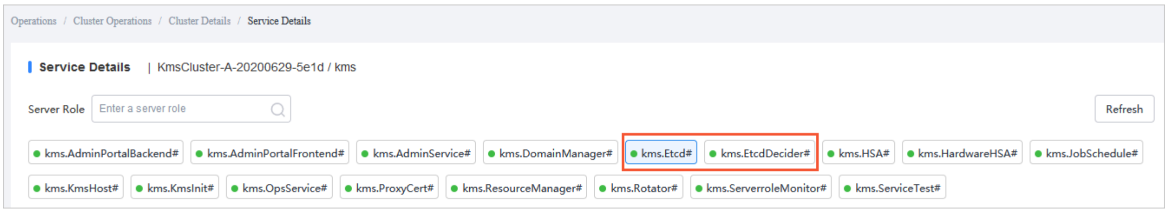
All: 5 | □ Normal (5) Reset

Services: Enter a service name

Deploy Service | Batch Upgrade

Services	Status	Server Role	Service Template	Actions
hids-client	Normal	1 in Total | Normal	None	Details | Upgrade | Unpublish
kms	Normal	17 in Total | Normal	KMS-PRIVATE Details	Details | Upgrade | Unpublish

6. On the **Service Details** page, check whether the Etcd and EtcdDecider server roles are at desired state. If the indicators for the kms.Etcd# and kms.EtcdDecider# server roles are green, the server roles are at desired state.



Operations / Cluster Operations / Cluster Details / Service Details

Service Details | KmsCluster-A-20200629-5e1d / kms

Server Role: Enter a server role

Refresh

● kms.AdminPortalBackend#
● kms.AdminPortalFrontend#
● kms.AdminService#
● kms.DomainManager#
● kms.Etcd#
● kms.EtcdDecider#
● kms.HSA#
● kms.HardwareHSA#
● kms.JobSchedule#
● kms.KmsHost#
● kms.KmsInit#
● kms.OpsService#
● kms.ProxyCert#
● kms.ResourceManager#
● kms.Rotator#
● kms.ServerroleMonitor#
● kms.ServiceTest#

Troubleshooting

View logs in the */cloud/log/kms/Etcd#/etcd* and */cloud/log/kms/EtcdDecider#/decider* directories to troubleshoot errors of the etcd service.

Possible errors

Error	Troubleshooting
The startup parameters of the etcd service are invalid.	Find the correct settings of the startup parameters in the historical records of the *debug.log* file. Then, manually start the etcd service. **Note** Retain the error logs and request the technical support team to identify the cause.
Errors in the EtcdDecider server role during service updates cause errors in the etcd service.	In most scenarios, this issue occurs when a rolling task exists. You can analyze the issue and identify the cause based on the *debug.log* file of the EtcdDecider server role.
The data directory of the etcd service is missing and the etcd service cannot start normally.	Solution: Use the Apsara Infrastructure Management Framework console to remove the abnormal etcd node from its server role group, and then add it back.

9.14.1.6. Rotator

9.14.1.6.1. Primary data center

This topic describes how to check the status of the rotator of the primary data center.

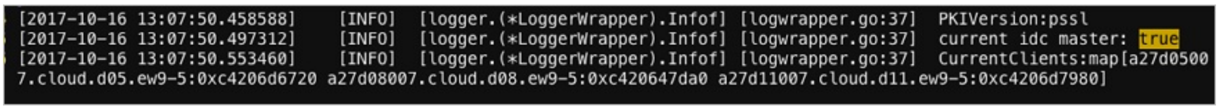
The rotator is a special component. Even if the server role of the rotator is at desired state in the Apsara Infrastructure Management Framework console, the rotator is not necessarily working normally.

Rotator exceptions do not have an impact on the API logic of Key Management Service (KMS).

In most scenarios, you must identify the cause of a rotator exception only when unexpected results are found, for example, when the data in ApsaraDB RDS does not meet expectations.

Check whether the rotator starts in primary data center mode

View the value of `current idc master` in the */cloud/log/kms/Rotator#/rotator/debug.log* file to check whether the rotator of the primary data center starts in primary data center mode, as shown in the following figure.



```
[2017-10-16 13:07:50.458588]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  PKIVersion:pssl
[2017-10-16 13:07:50.497312]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  current idc master: true
[2017-10-16 13:07:50.553460]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  CurrentClients:map[a27d0500
7.cloud.d05.ew9-5:0xc4206d6720 a27d08007.cloud.d08.ew9-5:0xc420647da0 a27d11007.cloud.d11.ew9-5:0xc4206d7980]
```

If the value of `current idc master` is true, the rotator starts in primary data center mode. If the value of `current idc master` is false, the rotator starts in secondary data center mode.

Check whether the rotator is in the working state

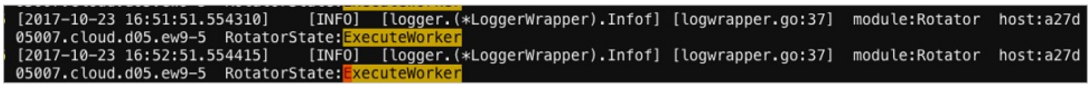
The rotator of the primary data center is deployed on all nodes. The nodes work in distributed lock mode to ensure that only one node can work at a time. All the other nodes remain in the standby state.

View status logs in the */cloud/log/kms/Rotator#/rotator/status.log* file and check the status of each node.

Check the value of the RotatorState parameter in the status logs. Valid values: ExecuteWorker and TryLock.

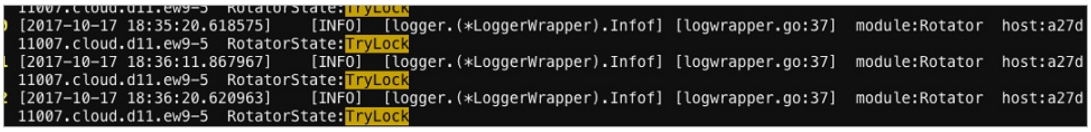
- ExecuteWorker: The node is in the working state.
- TryLock: The node is in the standby state.

  Working state



```
[2017-10-23 16:51:51.554310]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  module:Rotator  host:a27d
05007.cloud.d05.ew9-5  RotatorState:ExecuteWorker
[2017-10-23 16:52:51.554415]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  module:Rotator  host:a27d
05007.cloud.d05.ew9-5  RotatorState:ExecuteWorker
```

  Standby state



```
[2017-10-17 18:35:20.618575]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  module:Rotator  host:a27d
11007.cloud.d11.ew9-5  RotatorState:TryLock
[2017-10-17 18:36:11.867967]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  module:Rotator  host:a27d
11007.cloud.d11.ew9-5  RotatorState:TryLock
[2017-10-17 18:36:20.620963]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  module:Rotator  host:a27d
11007.cloud.d11.ew9-5  RotatorState:TryLock
```

Possible errors

- Abnormal ApsaraDB RDS database access. Statistics collection and key deletion tasks cannot be executed.
- Abnormal HSA service. Key rotation tasks cannot be executed.
- Abnormal Log Service. Metering tasks cannot be executed.
- Abnormal etcd service. Distributed locks are unavailable and tasks cannot be executed.
- If one of the tasks on the rotator is abnormal, the rotator may be unable to be at desired state. However, when this occurs, the rotator may still appear to be at desired state in the Apsara Infrastructure Management Framework console.

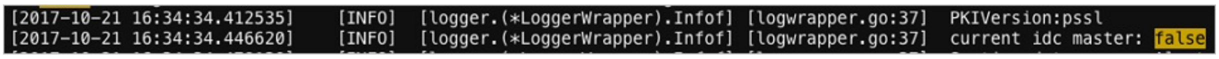
9.14.1.6.2. Secondary data center

This topic describes how to check the running status of the rotator of the secondary data center.

The rotator of the secondary data center is deployed on all nodes, which are all in the working state. The work scopes of the nodes are idempotent in a certain time range.

Check whether the rotator starts in secondary data center mode

Check the value of `current idc master` in */cloud/log/kms/Rotator#/rotator/debug.log*, as shown in the following figure.



```
[2017-10-21 16:34:34.412535]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  PKIVersion:pssl
[2017-10-21 16:34:34.446620]    [INFO]  [logger.(*LoggerWrapper).Infof] [logwrapper.go:37]  current idc master: false
```

If the value of `current idc master` is false, the rotator starts in secondary data center mode. If the value of `current idc master` is true, the rotator starts in primary data center mode.

Possible errors

- Abnormal network of the primary data center. The etcd of the primary data center is inaccessible.
- Abnormal etcd of the primary data center. The etcd of the primary data center is inaccessible.
- Abnormal etcd of the secondary data center. Data cannot be written into etcd.
- Incorrect etcd information of the primary data center. Data synchronization errors occur.

Notice Rotator exceptions of the secondary data center has a severe impact on KMS in the secondary data center. You must fix the exceptions in a timely manner.

9.14.2. Log analysis

9.14.2.1. Overview

Logtail is a log collection client provided by Log Service to facilitate your access to logs. After installing Logtail on a host that has KMS deployed, you can monitor a specified log. The newly written log entries are automatically uploaded to a specified log library.

Logtail is used to transmit the logs of KMS to Log Service. Then the portal or API of Log Service analyzes the logs. If Log Service has no portals, you have to log on to the hosts that have KMS deployed individually and check the hosts one by one.

9.14.2.2. View logs by using request IDs

After you send a request to Key Management Service (KMS), KMS sends you a message that contains a request ID. This topic describes how to view logs by using request IDs.

Request IDs can be used in the following scenarios:

- You can view the KMS audit logs in the */cloud/log/kms/KmsHost#/kms_host/audit.log* file.

  You can view the audit log information of the current access based on the value of request_id.

- For log entries whose expected_code values are not 200, you can view error information in the debug logs based on the value of request_id.

  Path to the on-premises logs: */cloud/log/kms/KmsHost#/kms_host/debug.log*

  Note The */cloud/log/kms/KmsHost#/kms_host/debug.log* and *audit.log* files are stored on the same machine.

- If you need all details of a request, you can view detailed information in the trace logs.

  Path to the on-premises logs: */cloud/log/kms/KmsHost#/kms_host/debug.log*

  Note The */cloud/log/kms/KmsHost#/kms_host/debug.log* and *audit.log* files are stored on the same machine.

- You can associate a cryptographic API operation with the trace logs of HSA by using the value of request_id.

  Path to the on-premises logs: */cloud/log/kms/HSA#/hsa/trace.log*

  Note The */cloud/log/kms/KmsHost#/kms_host/trace.log* and *audit.log* files may be stored on different machines.

- You can retrieve log information based on other information.

  You can retrieve the information in the audit logs of KMS by using information other than request_id. If you need to associate the audit logs with other logs, you must use request_id.

9.14.2.3. Common KMS errors

9.14.2.3.1. Overview

KMS has two HTTP status codes in audit.log: expected_code and status_code.

Typically, the expected code and status code of an error are the same. (`expected_code = status_code`). However, there are exceptions.

status_code is the HTTP status code that is actually returned to a user.

9.14.2.3.2. Errors with HTTP status code 4XX

Most errors with HTTP status code 4XX are included in the business logic of KMS. For example, HTTP status code 403 indicates a user request authentication failure, and HTTP status code 400 indicates that an input parameter is invalid.

You can view the details of an error in the debug log by using the value of request_id.

9.14.2.3.3. Errors with HTTP status code 500

This type of error is not included in the business logic of KMS. They are severe errors and must be fixed immediately.

In most scenarios, if the status code of an error is 500, the expected code of this error is also 500.

Such an error may be caused by an unexpected exception in a dependency service. We recommend that you contact the technical support personnel of the dependency service for further assistance.

You can view the details of an error in the debug log by using the value of request_id.

9.14.2.3.4. Errors with HTTP status code 503

An error with HTTP status code 503 occurs when the user interrupts the connection or a dependency service of Key Management Service (KMS) is abnormal. We recommend that you handle the exception at the earliest opportunity.

The status code and expected code of such an error may be different or consistent.

- The status code is 503 but the expected code is not 503.

  Possible causes:

  - The client of a user interrupts the connection in advance.
  - The client times out because KMS that functions as the server does not respond within the timeout period.

  You can check the trace logs by using the value of request_id to determine whether the error is caused by a slow response of the server and identify the specific module.

- Both the status code and expected code are 503.

  Such an error is an expected error in a dependency service of KMS. It may occur when the performance of the dependency service is unstable.

  You can view the details of the error in the debug logs by using the value of request_id. We recommend that you contact the technical support of the dependency service for further assistance.

9.14.2.3.5. Degradation of dependency on a service

KMS stores the data of its dependency services in the local cache. If a dependency service is unavailable, KMS uses the obsolete data stored in the cache.

In this scenario, the status code in the audit log of KMS is 200, but an additional debug log will be generated.

When this situation occurs, users with cached data can access KMS. However, users without cached data encounter a 503 error when they try to access KMS.

9.15. Apsara Stack DNS

9.15.1. Introduction to Apsara Stack DNS

This topic describes Apsara Stack DNS and the features of its modules.

Database management system

The database management system compares the versions in the baseline configuration with those in the database to better manage databases. This allows you to validate the database version in each update.

API system

The API system determines the business logic of all calls and manages all data and tasks. This system is written in Java.

DNS

The DNS system consists of BIND and Agent. Agent receives and processes task information passed from the API system. Agent parses the tasks into commands, and then delivers the commands to the BIND system.

9.15.2. Maintenance

9.15.2.1. View operational logs

During operations and maintenance, you can query and view logs that are stored at specific locations in different systems to troubleshoot errors.

The operational logs of the API service are stored in the */home/admin/gdns/logs/* directory. You can query logs as needed.

The operational logs of the Agent service are stored in the */var/log/dns/* directory of the DNS server. Each log contains log entries of a specific day.

The operational logs of the BIND service are stored in the */var/named/chroot/var/log/* directory of the DNS server.

9.15.2.2. Enable and disable a service

You can log on to the API server as an administrator and run the `/home/admin/gdns/bin/appctl.sh restart` command to restart the API service. We recommend that you run the command on one server at a time to ensure that another server can provide services. You can specify the start, stop, and restart parameters in the preceding command.

Apsara Stack DNS provides services by using anycast IP addresses. You must run the `service ospfd stop` command to disable the OSPF service before you run the `service named stop` command to disable the DNS service.

You must run the `service named start` command to enable the DNS service before you run the `service ospfd start` command to enable the OSPF service.

You can run the `/usr/local/AgentService/agent -s start` command to enable the Agent service. If you receive a message that indicates the PID file already exists, delete the `/var/dns/dns.pid` file and run the command again.

You can run the `/usr/local/AgentService/agent -s stop` command to disable the Agent service.

9.15.2.3. Data backup

If you need to back up data before updating the service, copy the */var/named/* and */etc/named/* directories to a backup location. When you need to restore your data, copy the backup data to the original directories. Do not trigger automatic update during a data restoration process. Otherwise, data inconsistency may occur.

9.15.3. DNS API

9.15.3.1. Manage the API system

You can manage the API system in the Apsara Infrastructure Management Framework console. To log on to the server in which the API system resides, choose **Operations > Machine Operations** in the Apsara Infrastructure Management Framework console.

Context

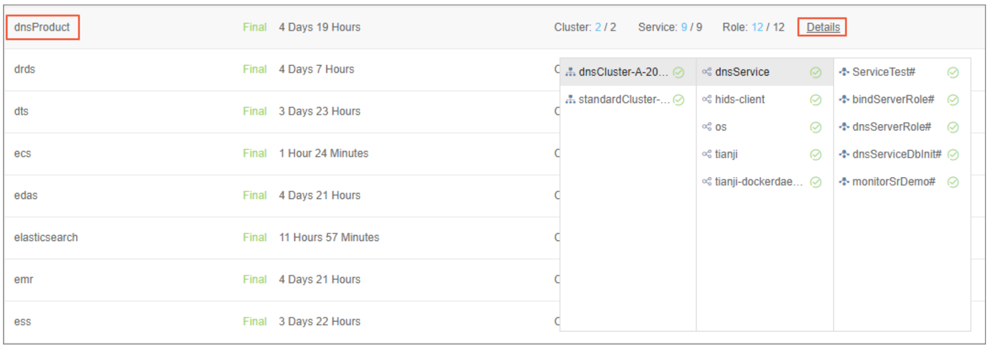
To determine whether a service role is running as expected, follow these steps:

Procedure

1. In the Apsara Infrastructure Management Framework console, check whether the API is at desired state.
   i. Log on to the Apsara Infrastructure Management Framework console.
   ii. In the top navigation bar, choose **Tasks > Deployment Summary** to open the **Deployment Summary** page.
   iii. Click **Deployment Details**.
   iv. On the **Deployment Details** page, find the dnsProduct project.

v. Find the dnsServerRole# service role, and click **Details** in the Deployment Progress column to check whether the service role is at desired state. If a green check mark is displayed after dnsServerRole#, then dnsServerRole# is at desired state.

View API status



dnsProduct	Final	4 Days 19 Hours	Cluster: 2 / 2 Service: 9 / 9 Role: 12 / 12 Details
drds	Final	4 Days 7 Hours	
dts	Final	3 Days 23 Hours	
ecs	Final	1 Hour 24 Minutes	
edas	Final	4 Days 21 Hours	
elasticsearch	Final	11 Hours 57 Minutes	
emr	Final	4 Days 21 Hours	
ess	Final	3 Days 22 Hours	

2. Obtain the IP addresses of servers where the API services are deployed.

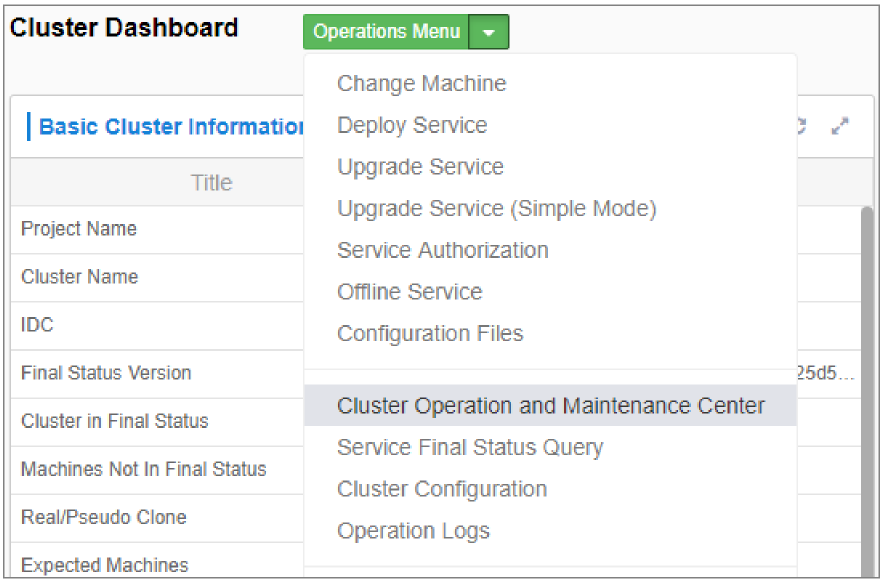
   i. Log on to the Apsara Infrastructure Management Framework console.

   ii. In the top navigation bar, choose **Operations > Cluster Operations**.

   iii. Click a cluster URL to open the **Cluster Dashboard** page.

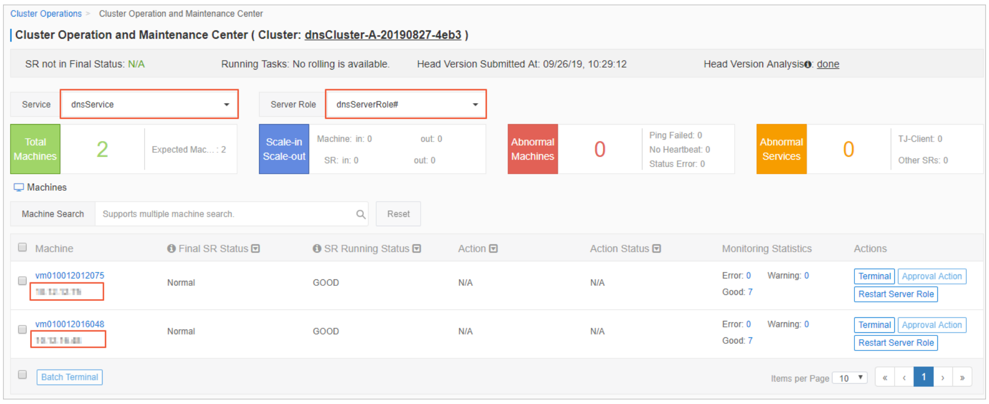
   iv. On the **Cluster Dashboard** page, choose **Operations Menu > Cluster Operation and Maintenance Center**.

Cluster Operation and Maintenance Center



v. On the **Cluster Operation and Maintenance Center** page, view and obtain the IP addresses of servers that are deployed with the API service.

View the IP addresses of servers



Cluster Operations > Cluster Operation and Maintenance Center

Cluster Operation and Maintenance Center (Cluster: dnsCluster-A-20190827-4eb3)

SR not in Final Status: N/A   Running Tasks: No rolling is available.   Head Version Submitted At: 09/26/19, 10:29:12   Head Version Analysis: done

Service: dnsService   Server Role: dnsServerRole#

Total Machines 2   Expected Mac... : 2
Scale-in Scale-out   Machine: in: 0   out: 0   SR: in: 0   out: 0
Abnormal Machines 0   Ping Failed: 0   No Heartbeat: 0   Status Error: 0
Abnormal Services 0   TJ-Client: 0   Other SRs: 0

Machines

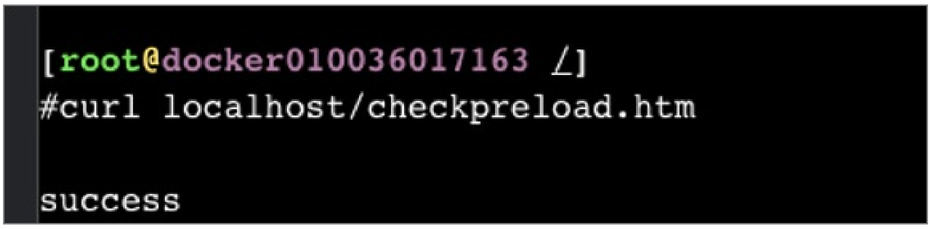
Machine Search: Supports multiple machine search.   Reset

□	Machine	Final SR Status	SR Running Status	Action	Action Status	Monitoring Statistics	Actions
□	vm010012012075 [redacted]	Normal	GOOD	N/A	N/A	Error: 0 Warning: 0 Good: 7	Terminal Approval Action Restart Server Role
□	vm010012016048 [redacted]	Normal	GOOD	N/A	N/A	Error: 0 Warning: 0 Good: 7	Terminal Approval Action Restart Server Role

□ Batch Terminal   Items per Page 10   « ‹ 1 › »

3. Log on to the DNS API server. Run the `curl http://localhost/checkpreload.htm` command, and check whether the command output is "success".
   i. Log on to the Apsara Infrastructure Management Framework console.
   ii. In the top navigation bar, choose **Operations > Machine Operations**.
   iii. Click **Terminal** in the Actions column of a server to log on to the server.
   iv. Run the `curl http://localhost/checkpreload.htm` command on the server where the API service is deployed and check whether the command output is "success".

   Verify the server



```
[root@docker010036017163 /]
#curl localhost/checkpreload.htm

success
```

9.15.3.2. Troubleshooting

Procedure

1. View logs stored in */home/admin/gdns/logs/*.
2. Check whether the API service is running. If an error occurs when you call an API operation, check the log to troubleshoot the error.
3. If the API service is running, but its features do not function as expected, check the application.log file.

9.15.4. DNS system

9.15.4.1. Check whether a server role is normal

Procedure

1. In the Apsara Infrastructure Management Framework console, check whether the Apsara Stack DNS

system is in its final state.

  i. Log on to the Apsara Infrastructure Management Framework console.

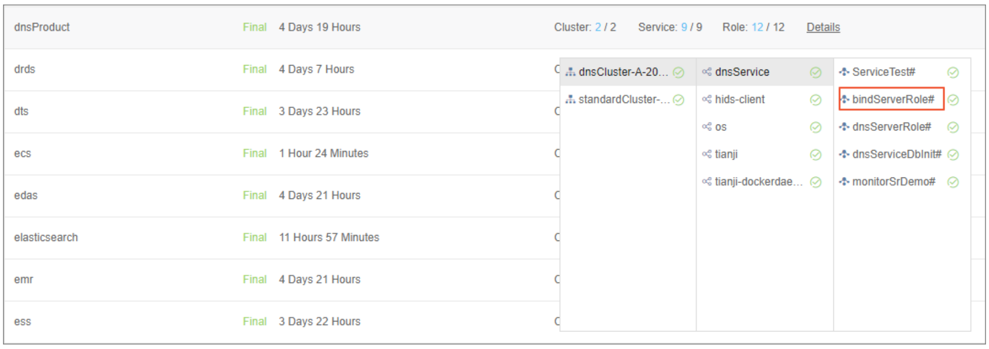
  ii. In the top navigation bar, choose **Tasks > Deployment Summary**.

  iii. On the **Deployment Summary** page, click **Deployment Details**.

  iv. On the **Deployment Details** page, find dnsProduct.

  v. Click **Details** in the **Deployment Progress** column to check whether the bindServerRole# role is in its final state.

Checking whether the bindServerRole# server role is in its final state



dnsProduct	Final	4 Days 19 Hours	Cluster: 2 / 2 Service: 9 / 9 Role: 12 / 12 Details
drds	Final	4 Days 7 Hours	
dts	Final	3 Days 23 Hours	
ecs	Final	1 Hour 24 Minutes	
edas	Final	4 Days 21 Hours	
elasticsearch	Final	11 Hours 57 Minutes	
emr	Final	4 Days 21 Hours	
ess	Final	3 Days 22 Hours	

2. Obtain the IP addresses of the servers where DNS services are deployed.

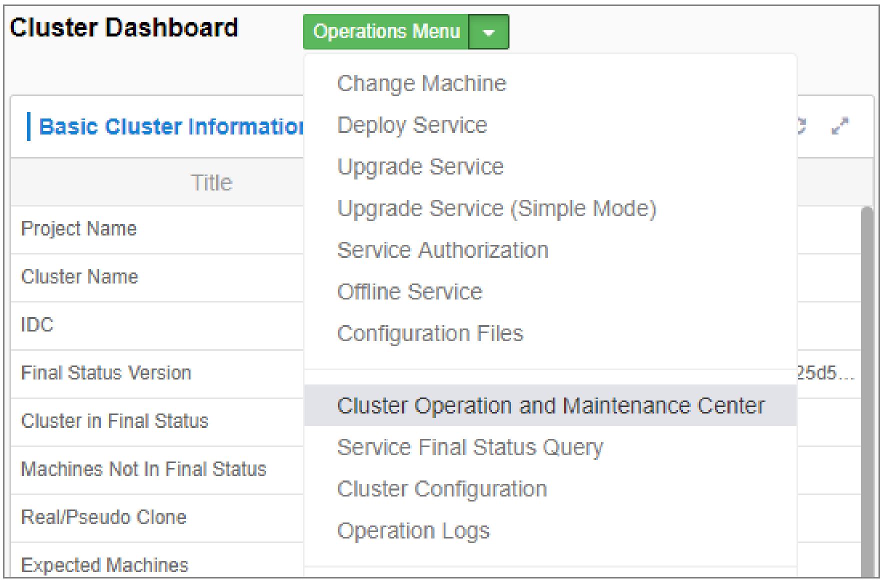
  i. Log on to the Apsara Infrastructure Management Framework console.

  ii. In the top navigation bar, choose **Operations > Cluster Operations**.

  iii. Click a cluster URL to go to the Cluster Dashboard page.

  iv. On the Cluster Dashboard page, choose **Operations Menu > Cluster Operation and Maintenance Center**.

Cluster Operation and Maintenance Center



  v. On the Cluster Operation and Maintenance Center page, view and obtain IP addresses of all the servers that are assigned with the bindServerRole# role.

3. Log on to the DNS server, run the **python /bind/hello/check_health.py|echo $?** command, and check whether the command output is 0.

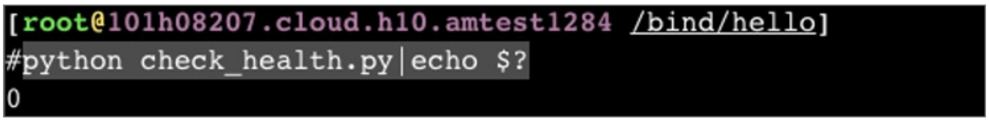
i. Log on to the Apsara Infrastructure Management Framework console.

ii. Choose **Operations** > **Machine Operations**.

iii. Select a server and click **Terminal** to log on to the server.

iv. Run the **python /bind/hello/check_health.py|echo $?** command on each server that is assigned with the bindServerRole# role and check whether the command output is 0.

Verifying the server



```
[root@101h08207.cloud.h10.amtest1284 /bind/hello]
#python check_health.py|echo $?
0
```

9.15.4.2. Troubleshooting

Procedure

1. Check the operational logs of the BIND service that are stored in the */var/named/chroot/var/log/* directory, and determine whether errors have occurred.
2. Check the operational logs of the Agent service that are stored in the */var/log/dns/* directory, and determine whether errors have occurred.
3. Run the **named-checkconf** command to check whether errors have occurred in the configuration file.

9.15.4.3. Errors and exceptions

Error: exit code 1

Run the health check script to view the cause of this error.

Common causes include:

- The DNS service is not running.
- The Agent service is not running.
- The OSPF service is not running, or anycast and public IP addresses cannot be advertised because of a network information retrieval error.
- Failed to run the task.

9.15.5. Log analysis

Query log entries by request ID

After you send a request, you will receive a response that contains the request ID. The request ID can be used in the following scenarios:

1. Query the tasks that are associated with the current request from the database.
2. Retrieve the execution results and error messages of the current request from the API system log.
3. Retrieve the results of the current request from the log of `bindServerRole#` , and verify the results with information that is retrieved from multiple other systems.

9.15.6. View and process data

Context

You can view task records and execution results.

Procedure

1. Log on to the API server to view database connection details.
2. Run the **use genesisdns** command of MySQL to log on to the database and then run the **select * from task** command to retrieve the progress and status of each task.

9.16. API Gateway

9.16.1. API Gateway introduction

This topic describes Apsara Stack API Gateway and the features of its modules.

API Gateway console

The API Gateway console is used to configure and manage your APIs and related policies. With the API management system, you can query, update, edit, and delete APIs. You can also create, associate, disassociate, and delete API management policies. API Gateway also provides a full range of API lifecycle management functions, including creating, testing, publishing, and unpublishing APIs. It improves API management and iteration efficiency. All your data will eventually be used as the API metadata for API Gateway.

API Gateway

API Gateway is a complete API hosting service. It helps you use APIs to provide capabilities, services, and data to your partners. API Gateway is initialized based on the API metadata generated by the API management system, and ultimately acts as the agent to send API requests. API Gateway provides a range of mechanisms to enhance security and reduce risks arising from APIs. These mechanisms include attack prevention, replay prevention, request encryption, identity authentication, permission management, and throttling.

9.16.2. Routine maintenance

9.16.2.1. View operational logs

During O&M, you can query and view logs that are stored in specific directories of different systems to troubleshoot issues.

API Gateway pop logs: The operational log files are stored in the */apsara/alidata/www/logs/java/cloudapi-openapi/* directory. You can query the files as required.

API Gateway logs: The operational log files are stored in the */apsara/alidata/logs/* directory. Each log file contains log entries that are generated over a single day. You can query the files as required.

9.16.2.2. Enable and disable a service

Perform the following operations to enable a service: Log on to the Apsara Infrastructure Management Framework console. Find the apigateway service instance in the Service Instances section of the Cluster Dashboard page and click Details in the Actions column.

On the Service Instance Information Dashboard page, find the target SR in the Server Role List section and click Details in the Actions column.

On the Server Role Dashboard page, find the target machine in the Machine Information section and click `Restart` in the Actions column.

In the message that appears, click OK. To disable a service, click Terminal in the Actions column and run the docker stop [containerId] command.

9.16.3. API Gateway O&M

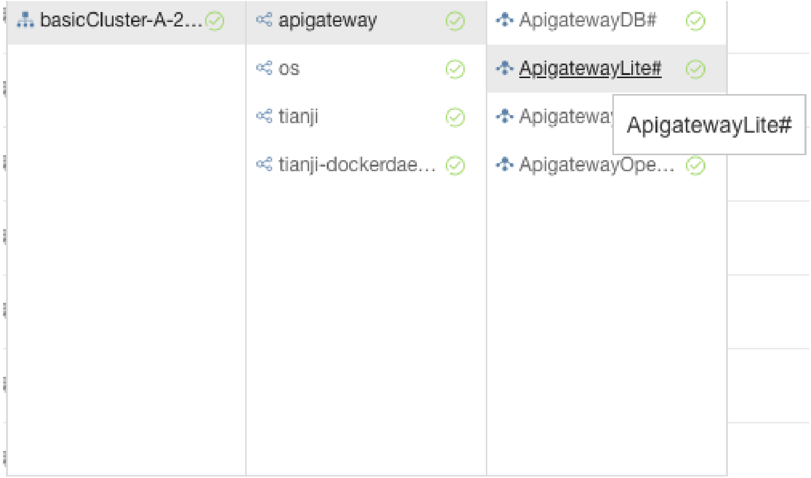
9.16.3.1. System O&M

9.16.3.1.1. Check the desired state of API Gateway

You can use Apsara Infrastructure Management Framework to operate and maintain API Gateway. To log on to the machines in which the API Gateway console resides, choose Operations > Server Operations in the Apsara Infrastructure Management Framework console.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the top navigation bar, choose **Tasks > Deployment Summary**.
3. On the Deployment Summary page that appears, click **Deployment Details**.
4. On the **Deployment Details** page, find the apigateway project.
5. Click **Details** in the **Deployment Progress** column corresponding to the apigateway project. Check whether the ApigatwayLite# server role is in the desired state.If a green tick appears for the server role item, the server role has reached the desired state.



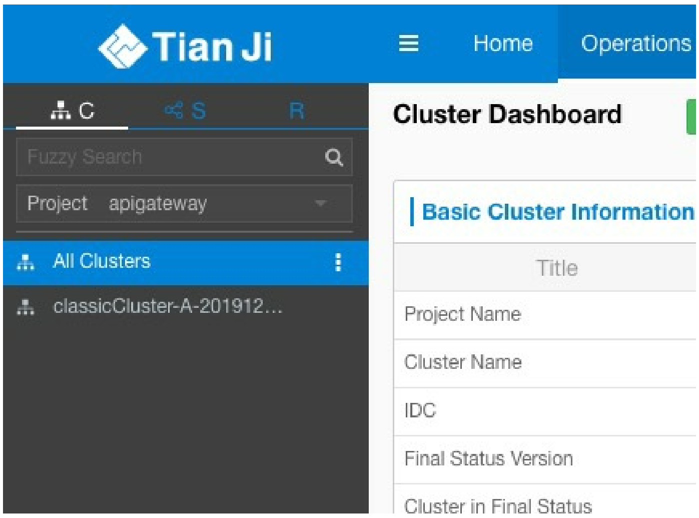
9.16.3.1.2. Check the service status of OpenAPI

Procedure

1. Find machines in the ApigatewayOpenAPI# server role.
   1. Log on to the Apsara Infrastructure Management Framework console.

ii. Click the **C** tab in the left-side navigation pane.

iii. Select apigateway from the Project drop-down list.

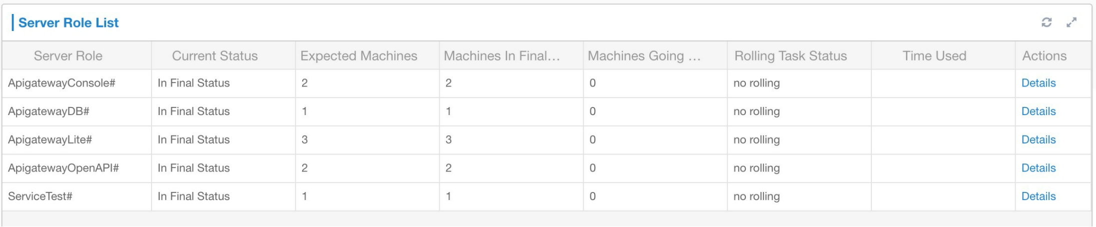


Project apigateway

iv. Place the pointer over the ⋮ icon next to one of the filtered clusters and choose **Dashboard** from the shortcut menu.

v. In the **Service Instance List** section, click Details in the Actions column corresponding to the apigateway service instance.

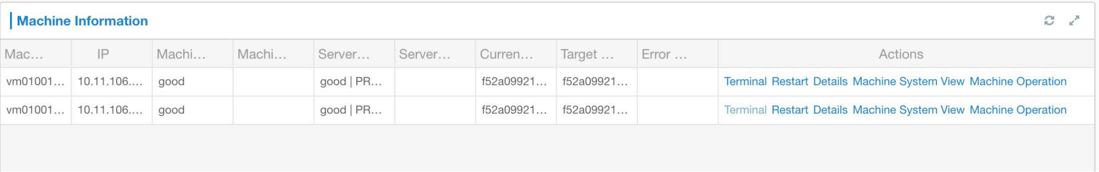
vi. In the **Server Role List** section, you can view the deployment status of each role.



Server Role List

Server Role	Current Status	Expected Machines	Machines In Final...	Machines Going ...	Rolling Task Status	Time Used	Actions
ApigatewayConsole#	In Final Status	2	2	0	no rolling		Details
ApigatewayDB#	In Final Status	1	1	0	no rolling		Details
ApigatewayLite#	In Final Status	3	3	0	no rolling		Details
ApigatewayOpenAPI#	In Final Status	2	2	0	no rolling		Details
ServiceTest#	In Final Status	1	1	0	no rolling		Details

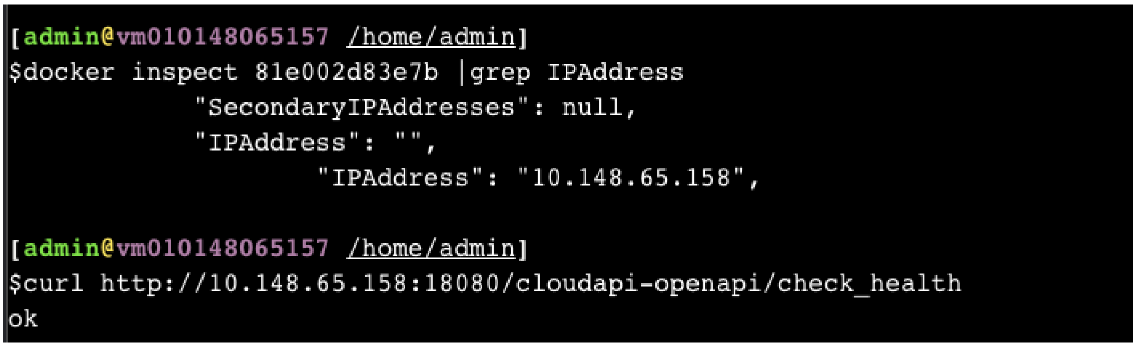
vii. Click Details in the Actions column corresponding to the ApigatewayOpenAPI# role and view machine information of the role in the **Machine Information** section.



Machine Information

Mac...	IP	Machi...	Machi...	Server...	Server...	Curren...	Target ...	Error ...	Actions
vm01001...	10.11.106....	good		good | PR...		f52a09921...	f52a09921...		Terminal Restart Details Machine System View Machine Operation
vm01001...	10.11.106....	good		good | PR...		f52a09921...	f52a09921...		Terminal Restart Details Machine System View Machine Operation

2. Click **Terminal** in the Actions column corresponding to a machine to log on to the machine.
3. Run the following command to find the container: **docker ps|grep cloudapi-openapi**
4. Run the following command to find the container IP address: **docker inspect [container ID] | grep IPAddress**
5. Run the following command to check whether OK is returned: **curl -i http://localhost:18080/cloudapi-openapi/check_health**



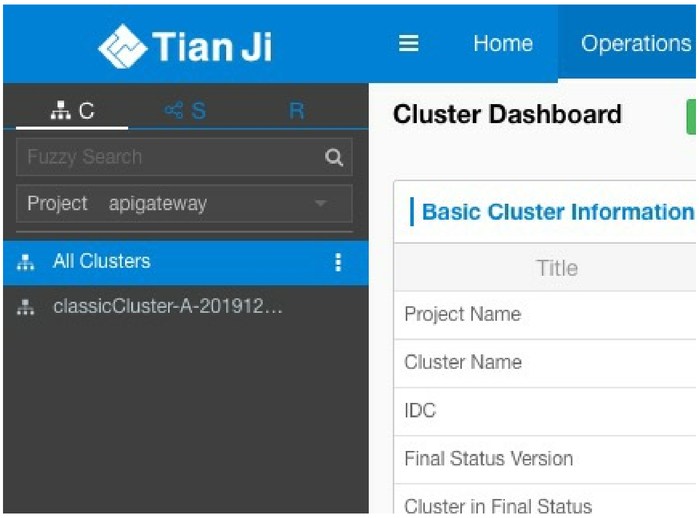
```
[admin@vm010148065157 /home/admin]
$docker inspect 81e002d83e7b |grep IPAddress
            "SecondaryIPAddresses": null,
            "IPAddress": "",
                    "IPAddress": "10.148.65.158",

[admin@vm010148065157 /home/admin]
$curl http://10.148.65.158:18080/cloudapi-openapi/check_health
ok
```

If OK is returned, the service status of the OpenAPI component is normal.

9.16.3.1.3. Check the service status of the API Gateway console

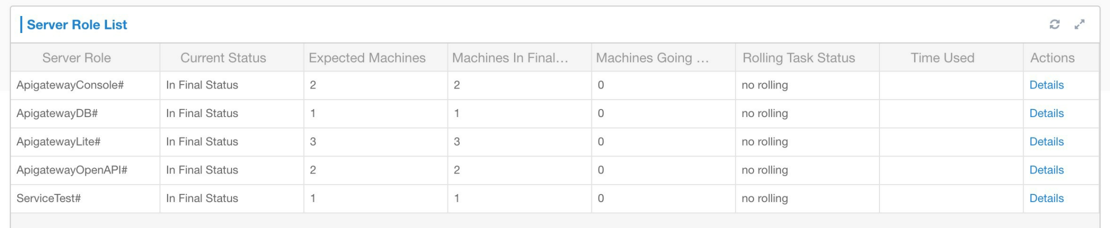
Procedure

1. Find machines in the ApigatewayConsole# server role.
   i. Log on to the Apsara Infrastructure Management Framework console.
   ii. Click the **C** tab in the left-side navigation pane.
   iii. Select apigateway from the Project drop-down list.



   iv. Place the pointer over the ⋮ icon next to one of the filtered clusters and choose **Dashboard** from the shortcut menu.
   v. In the **Service Instance List** section, click Details in the Actions column corresponding to the apigateway service instance.

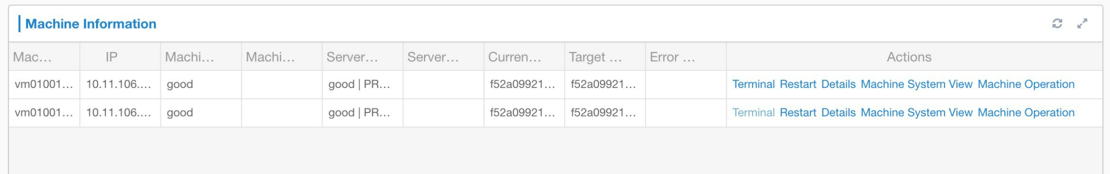
vi. In the **Server Role List** section, you can view the deployment status of each role.



Server Role List

Server Role	Current Status	Expected Machines	Machines In Final...	Machines Going ...	Rolling Task Status	Time Used	Actions
ApigatewayConsole#	In Final Status	2	2	0	no rolling		Details
ApigatewayDB#	In Final Status	1	1	0	no rolling		Details
ApigatewayLite#	In Final Status	3	3	0	no rolling		Details
ApigatewayOpenAPI#	In Final Status	2	2	0	no rolling		Details
ServiceTest#	In Final Status	1	1	0	no rolling		Details

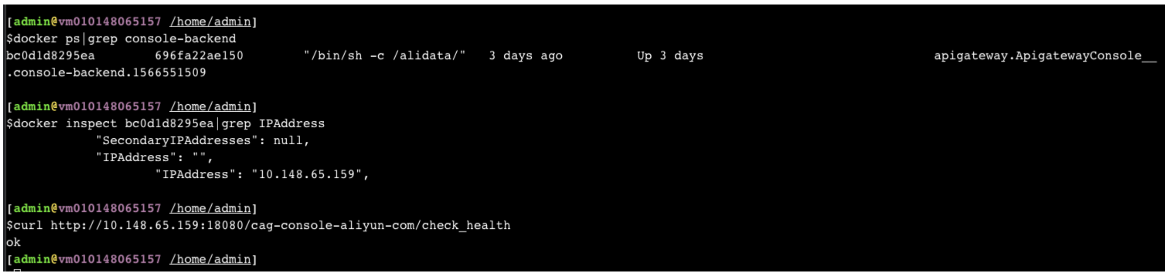
vii. Click Details in the Actions column corresponding to the ApigatewayConsole# role and view machine information of the role in the **Machine Information** section.



Machine Information

Mac...	IP	Machi...	Machi...	Server...	Server...	Curren...	Target ...	Error ...	Actions
vm01001...	10.11.106....	good		good | PR...		f52a09921...	f52a09921...		Terminal Restart Details Machine System View Machine Operation
vm01001...	10.11.106....	good		good | PR...		f52a09921...	f52a09921...		Terminal Restart Details Machine System View Machine Operation

2. Click **Terminal** in the Actions column corresponding to a machine to log on to the machine.
3. Run the following command to find the container: **docker ps|grep cloudapi-openapi**
4. Run the following command to find the container IP address: **docker inspect [container ID] | grep IPAddress**
5. Run the following command to check whether OK is returned: **curl -i http://localhost:18080/cag-console-aliyun-com/check_health**



```
[admin@vm010148065157 /home/admin]
$docker ps|grep console-backend
bc0d1d8295ea        696fa22ae150        "/bin/sh -c /alidata/"   3 days ago          Up 3 days                               apigateway.ApigatewayConsole__
.console-backend.1566551509

[admin@vm010148065157 /home/admin]
$docker inspect bc0d1d8295ea|grep IPAddress
            "SecondaryIPAddresses": null,
            "IPAddress": "",
                    "IPAddress": "10.148.65.159",

[admin@vm010148065157 /home/admin]
$curl http://10.148.65.159:18080/cag-console-aliyun-com/check_health
ok
[admin@vm010148065157 /home/admin]
```

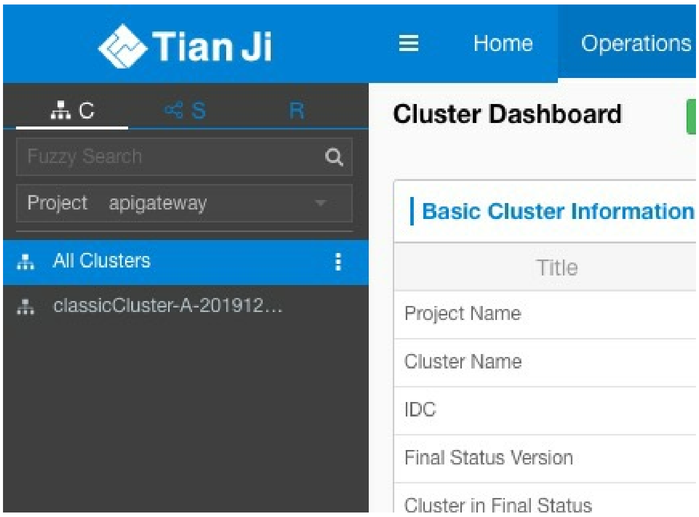
If OK is returned, the service status of the API Gateway console is normal.

9.16.3.1.4. Check the service status of API Gateway

Procedure

1. Find machines in the ApigatewayLite# server role.
    i. Log on to the Apsara Infrastructure Management Framework console.
    ii. Click the **C** tab in the left-side navigation pane.

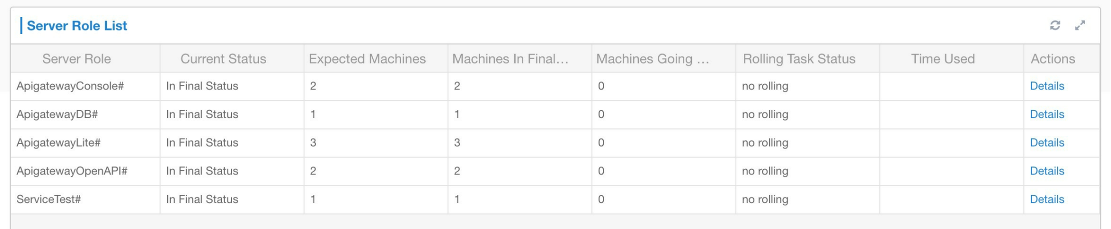
iii. Select apigateway from the Project drop-down list.



iv. Place the pointer over the ⋮ icon next to one of the filtered clusters and choose **Dashboard** from the shortcut menu.

v. In the **Service Instance List** section, click Details in the Actions column corresponding to the apigateway service instance.

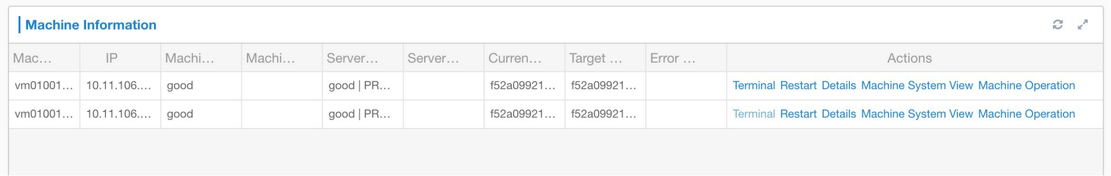
vi. In the **Server Role List** section, you can view the deployment status of each role.



Server Role List

Server Role	Current Status	Expected Machines	Machines In Final...	Machines Going ...	Rolling Task Status	Time Used	Actions
ApigatewayConsole#	In Final Status	2	2	0	no rolling		Details
ApigatewayDB#	In Final Status	1	1	0	no rolling		Details
ApigatewayLite#	In Final Status	3	3	0	no rolling		Details
ApigatewayOpenAPI#	In Final Status	2	2	0	no rolling		Details
ServiceTest#	In Final Status	1	1	0	no rolling		Details

vii. Click Details in the Actions column corresponding to the ApigatewayLite# role and view machine information of the role in the **Machine Information** section.



Machine Information

Mac...	IP	Machi...	Machi...	Server...	Server...	Curren...	Target ...	Error ...	Actions
vm01001...	10.11.106....	good		good | PR...		f52a09921...	f52a09921...		Terminal Restart Details Machine System View Machine Operation
vm01001...	10.11.106....	good		good | PR...		f52a09921...	f52a09921...		Terminal Restart Details Machine System View Machine Operation

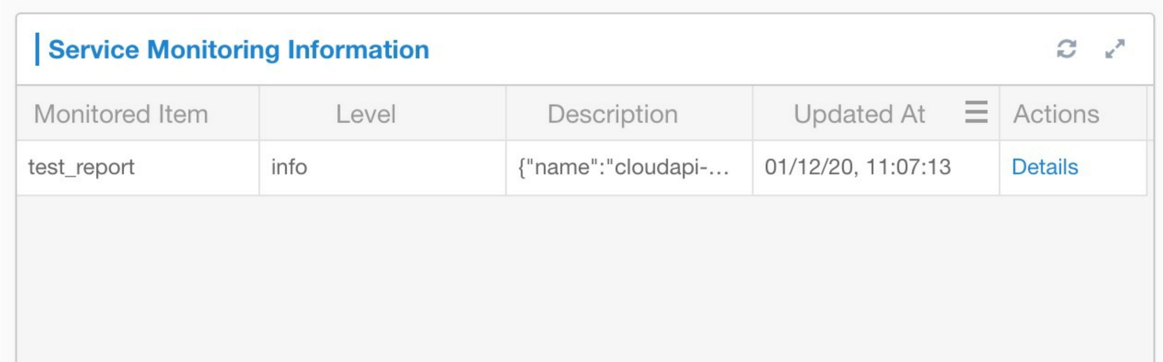
2. Click **Terminal** in the Actions column corresponding to a machine to log on to the machine.
3. Run the following command to check whether the `I'm fine, thank you, and you?` message is returned: **curl -i http://localhost/status -H Host:status.taobao.com**

9.16.3.1.5. View results of automated test cases

Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. Click the **C** tab in the left-side navigation pane.
3. Select **apigateway** from the **Project** drop-down list.

4. Place the pointer over the ⋮ icon next to one of the filtered clusters and choose **Dashboard** from the shortcut menu.
5. In the **Service Instance List** section, click **Details** in the Actions column corresponding to the apigateway service instance.
6. In the **Service Monitoring Information** section, click **Details** in the Actions column to view the automated test case report.



Service Monitoring Information

Monitored Item	Level	Description	Updated At	Actions
test_report	info	{"name":"cloudapi-...	01/12/20, 11:07:13	Details

9.16.3.2. Troubleshooting

Context

Note

- /alidata/logs/system.log: API Gateway logs.
- /usr/share/jetty/logs/stderrout.log: API Gateway console and OpenAPI logs.

Procedure

1. Start the application and check whether any errors have occurred. Check whether the system is operating normally.
   - If the system is operating but does not function properly, check the logs to troubleshoot errors.
   - If the system quits shortly after being started up, check the logs to troubleshoot errors.

9.16.4. Log analysis

You can perform log analysis based on the ID of an individual API request.

After you send a request, you will receive a response that contains the request ID from API Gateway.

You can use the request ID to perform the following operations:

- All API Gateway logs are uploaded to Log Service, where you can view the request ID.
- You can use the request ID to query the response to or error message for the current request in the API system logs.

10.Operations of middleware products

10.1. Enterprise Distributed Application Service (EDAS)

10.1.1. O&M overview

This topic describes the system architecture, component architecture, and O&M architecture of EDAS.

10.1.1.1. Architecture

This topic describes the system architecture and component architecture of Enterprise Distributed Application Service (EDAS), which helps you familiarize yourself with this knowledge when you perform O&M for EDAS.

System architecture

The system architecture of EDAS includes the console, data collection system, configuration registry, authentication center, and file system. System architecture of EDAS shows the overall architecture of EDAS.

- EDAS console

  The EDAS console is the only EDAS system component that you can use directly. You can implement resource management, application lifecycle management, maintenance control and service governance, three-dimensional monitoring, and digital operation in the console.

- Data collection system

  This system component allows you to collect, compute, and store the runtime status, trace query logs, and other information about clusters and instances where applications are deployed in EDAS in real time.

- Configuration registry

  This is a central server that is used to publish and subscribe to High-speed Service Framework (HSF) services (remote procedure call (RPC) framework) and to push distributed configurations.

- Authentication center

  This system component controls permissions for user data to ensure data security.

- File system

  This system component stores WAR packages and required components, such as JDK and Ali-Tomcat, which are uploaded by users.

Component architecture

Each system component of EDAS consists of one or more components. The following figure shows the component architecture of EDAS.

Component	Node type	Node quantity	Description
EDAS console	Control node	2	The console of EDAS. It provides the core features of the PaaS platform, including resource management, application lifecycle management, service governance, and auto scaling.
EDAS admin	Control node	2	A background task service. It provides the instance synchronization and application health check features.
EDAS server	Control node	2	It synchronizes status information with EDAS Agent.
Cai-fs	Control node	2	A file server. It stores the EDAS Agent installation package and EDAS application packages.
EagleEye console	Control node	2	It is used to query and view service traces.
Cai address	Control node	3	An address discovery service. It provides the address lists for DiamondServer and ConfigServer.
Diamond	Control node	3	A configuration management service. It provides configuration storage, query, and notification features, and mainly stores database metadata and EDAS feature switch configurations in EDAS.

Component	Node type	Node quantity	Description
ConfigServer	Control node	3	An RPC service registry. It is used to query and store the publishing and subscription data of services.

For information about other external components, such as DAuth and TLog, see the corresponding O&M documents.

10.1.1.2. O&M architecture

This topic describes the O&M architecture of Enterprise Distributed Application Service (EDAS). Before you use this topic, familiarize yourself with the system architecture of EDAS.

You can perform O&M for EDAS by mainly using the command-line interface (CLI).

O&M category	Description	O&M tool
Routine maintenance	Perform inspection and monitoring.	CLI: You can use the CLI to manually inspect the containers and components of EDAS.
Power-off maintenance	• Check and determine the statuses of containers and components. • Stop and start containers and components.	CLI
Troubleshooting	Handle component availability and service continuity faults of EDAS.	CLI

10.1.2. Overview of critical operations

Routine O&M for EDAS must be performed in strict accordance with the O&M guide. Failure to follow the O&M guide may cause risks to components and services.

O&M operations are classified into three levels: G1, G2, and G3. Operations vary by level. See the following table.

Definitions of operation levels

Level	Description
G1	L1|L2: Operations can be performed safely based on documented instructions, without having to apply for changes. Such operations will not affect the service.

Level	Description
G2	L1|L2: The onsite personnel must obtain confirmation from the product personnel before performing operations, which require applying for changes and following the documented instructions. Such operations will not affect the service.
G3	L1|L2: The onsite personnel must obtain confirmation from the product personnel and the customer before performing operations, which require applying for changes and following the documented instructions. Such operations may affect the service.

G3 is the highest level, which involves critical operations. See the following table.

A list of critical operations

Operation	Operation or Command
Check the AccessKeyId and AccessKeySecret	**cat /home/admin/.spas_key/default**
Clear logs	• For EagleEye: **find /home/admin/eagleeye/logs/ -name "*log.*" -exec rm {}** • For EDAS: **find /home/admin/edas/logs/ -name "*log.*" -exec rm {}**
Restart containers	**docker start {containerId}**

10.1.3. O&M preparation

This topic describes the logon portal, account, permissions, and tools required for O&M.

O&M preparation

Item	Purpose	Description
Remote Secure Shell (SSH) logon tool (such as *MobaXterm* or *PuTTY*)	Log on to the instances where components are located.	The logon account must be assigned the corresponding permissions. We recommend that you do not use the **root** or **admin** account for logon.

Item	Purpose	Description
Account	Log on to the console or an instance.	- Obtain the account and password for console logon from EDAS Customer Services. - The account used to log on to the instances where EDAS components are located must be assigned the corresponding permissions. We recommend that you do not use the **root** or **admin** account for logon.

10.1.4. Routine maintenance

EDAS routine maintenance includes inspection and monitoring.

- Inspection is the process where a periodic dialing test is performed on URLs or ports to determine whether EDAS services are normal. Currently, inspections in HTTP, TCP, ping, and JDBC modes are supported.
- Monitoring is the process where logs are collected from clients through TLog to summarize key metrics for measuring the system runtime status. Monitoring includes infrastructure monitoring and JVM monitoring.

10.1.4.1. Log on to the Apsara Infrastructure Management Framework console

This topic describes how to log on to the Apsara Infrastructure Management Framework console.

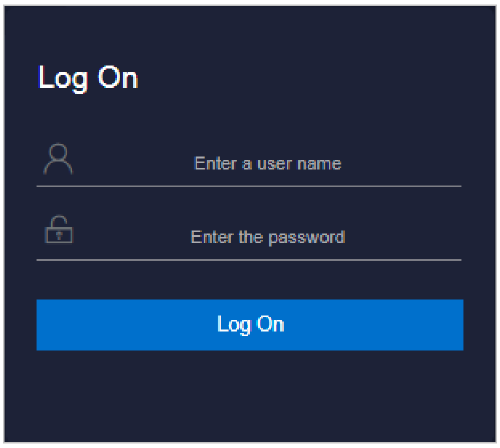
Prerequisites

- The URL, username, and password that are used to log on to the Apsara Uni-manager Operations Console are obtained from the deployment engineer or administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *region-id*.aso.*intranet-domain-id*.com.
- A browser is available. We recommend that you use the Google Chrome browser.

Procedure

1. Open your browser.
2. In the address bar, enter the *region-id*.aso.*intranet-domain-id*.com. URL and press the Enter key.



Log On

Enter a user name

Enter the password

Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   Note To obtain the username and password that are used to log on to the Apsara Uni-manager Operations Console, contact the deployment engineer or administrator.

   If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   To enhance security, make sure that the password meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password is 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Products > Product List**. On the **Product List** page, choose **Apsara Stack O&M > Apsara Infrastructure Management Framework**.

10.1.4.2. Inspection

You can configure the inspection rules of the HTTP, TCP, ping, and database types to inspect the components and services of Enterprise Distributed Application Service (EDAS). An inspection rule provides a response code that is used to check the configured alert rule. The alert content is configured in Alert Description. You can also log on to the instances where components and services are deployed and run commands for inspection.

EDAS inspection items lists the default inspection items of EDAS.

EDAS inspection items

Inspected object	Description	Inspection method
ConfigServer	Request /configserver/serverlist to check whether ConfigServer is normal.	Check /configserver/serverlist.
Diamond	Check whether the API operation for querying the DiamondServer status is normal.	Check /diamond-server/diamond.
	Check whether the DiamondServer database is connected.	Check the database connection.
TLog	Check whether the TLog service is normal.	Check /api/StageHealthCheck.
	Check whether the TLog listening port is normal.	Check port 8080.
	Check whether the TLog database is connected.	Check the database connection.
edas-console	Check whether the edas-console service is normal.	Check /checkpreload.htm.
	Check whether the edas-console port is normal.	Check port 8080.
	Check whether the EDAS database is connected.	Check the database connection.
HiStore	Check whether the HiStore listening port is normal.	Check port 5029.
	Check whether HiStore is connected.	Check the database connection.
Redis	Check whether the Redis listening port is normal.	Check port 6379.
edas-admin	Check whether the edas-admin service is running properly.	Check /index.
	Check whether the edas-admin listening port is normal.	Check port 8080.

10.1.4.2.1. Component inspection

You can inspect Enterprise Distributed Application Service (EDAS) components by using the CLI.

10.1.4.2.1.1. Manual inspection

Enterprise Distributed Application Service (EDAS) allows you to manually perform complex logic inspection by using the CLI.

Manual inspection uses commands typical of Linux operating systems. Set specific parameters based on the actual environment.

10.1.4.3. Monitoring

You can monitor the containers, system components, and services of Enterprise Distributed Application Service (EDAS) by using monitoring metrics.

Container monitoring

By default, the container status of each EDAS component is checked based on the monitoring script that is configured in an environment variable.

System monitoring

System monitoring includes infrastructure monitoring and Java Virtual Machine (JVM) monitoring.

System metrics

Monitoring type	Metric	Threshold
Infrastructure monitoring	CPU utilization	70%
	Memory usage	70%
	Disk usage	90%
JVM monitoring	Young garbage collection (GC) times	60
	FullGC	5
	Old generation usage	90%
	Permanent generation usage	90%

Service monitoring

Service monitoring is configured by EDAS and reported by API operations for monitoring and alerts. The following table lists the service metrics.

Monitored object	Monitoring type	Monitoring description
HTTP service	QPS	Monitors the QPS of the HTTP service.
	Time consumption	Monitors the input/output (I/O) time consumed by the HTTP service.
	Service provisioning QPS	Monitors the QPS of HSF service provisioning.

Monitored object	Monitoring type	Monitoring description
HSF service	Response time (RT) of service provisioning	Monitors the RT of HSF service provisioning.
	Service consumption QPS	Monitors the QPS of HSF service consumption.
	RT of service consumption	Monitors the RT of HSF service consumption.
Container	Heap memory usage	Measures how much heap memory is used by services.
	Off-heap memory usage	Measures how much off-heap memory is used by services.

10.1.4.3.1. Monitoring logs

Logs are critical for O&M of Enterprise Distributed Application Service (EDAS). You can monitor logs to promptly locate runtime faults.

The following table lists the EDAS logs that can be monitored.

Component	Log	Path
edas-console	console.log	/home/admin/edas/logs
edas-admin	admin.log	/home/admin/edas/logs
edas-server	agent-server.log	/home/admin/edas/logs

EDAS also provides other component logs, including the infrastructure monitoring log, service monitoring log, container monitoring log, and JVM monitoring log. For more information, see Log reference.

10.1.5. Troubleshooting

Faults may occur during EDAS usage. This topic describes the typical faults that may occur during O&M as well as their handling methods.

Fault classification

Currently, EDAS-related faults are classified into two categories:

- Component unavailability
- Service discontinuity

Fault locating

You can locate faults through inspection, monitoring, logs, and alarms.

10.1.5.1. Alert handling

During O&M of Enterprise Distributed Application Service (EDAS), you can inspect and monitor the status and metrics of each EDAS component. Alerts are triggered when inspection and monitoring are abnormal. This topic describes how to handle inspection and monitoring alerts.

10.1.5.1.1. CPU utilization alerts

The CPU utilization threshold is 70%. The CPU utilization is abnormal and an alert is triggered if it exceeds the threshold.

Possible causes

- High access concurrency
- Insufficient application instances

Impact on the system

Service performance is compromised.

Procedure

1. Open the Secure Sockets Layer (SSL) tool (MobaXterm Personal Edition).
2. Run **ssh <Username>@<IP address of your Ark client>** and enter your *password* to log on to the client.
3. Go to the target container and run **top** to check the CPU utilization of components.
   - If the CPU utilization is normal, no further action is required.
   - If the CPU utilization is abnormal, check the number of calls.
4. Run **netstat -tnlp | grep -E "80|8080" | wc -l** to check the call status of components.
   - If the number of calls is relatively large and meets the service status, scale out instances.
   - If the number of calls is not large, identify the cause of high CPU utilization by completing the following steps.

     > **Note** You can use the open-source script to locate and print the processes with high CPU utilization.

     a. Run **top -Hp <Component process ID>** to locate the processes with high CPU utilization or memory usage and convert them into the hexadecimal format.

     b. Go to the *jstack process id* path, open **ps.txt**, and identify the specific process class based on the hexadecimal thread ID.

     c. If Full GC occurs, check **gc.log** or run **jstat -gcutil [pid]** to check the corresponding GC log. Record *top/jstack file/full GC* and send the record to EDAS Customer Services.

10.1.5.1.2. Memory usage alerts

The memory usage threshold is 90%. Memory usage is abnormal if it exceeds the threshold.

Possible causes

- High access concurrency
- Insufficient application instances

Impact on the system

Service performance is compromised.

Procedure

1. Open the SSL tool (MobaXterm Personal Edition).
2. Run **ssh <Username>@<IP address of your Ark client>** and enter your *password* to log on to the client.
3. Go to the target container and run **top** to check the memory usage of components.
    - If the memory usage is normal, check the disk usage and JVM metrics.
    - If the memory usage is abnormal, check whether this is caused by JVM.
4. Run **jmap** to check memory usage.
5. Run **jstat -gcutil [pid]** to check memory usage.
6. Run **vmstat** to analyze and collect statistics on virtual memory.

Result

Log on to the target container by using the SSH tool and run **top** to check whether the memory usage is normal (less than 90%).

10.1.5.1.3. Disk usage alerts

The disk usage threshold is 90%. The disk usage is abnormal if it exceeds the threshold.

Possible causes

- High access concurrency
- Insufficient application instances
- Insufficient disk space or no periodic disk cleanup

Impact on the system

Service performance is compromised.

Procedure

1. Open the SSL tool (MobaXterm Personal Edition).
2. Run **ssh <Username>@<IP address of your Ark client>** and enter your *password* to log on to the client.
3. Go to the target container and run **df -lh** to check the disk usage of each directory and identify the directories with excessive and fast disk usage.
4. Run **iostat** to check the data write status. Perform disk cleanup if the *logs* directory occupies excessive disk space.
5. Run **netstat** to check the number of calls, view logs for call errors, and take relevant measures such as scale-out.

Result

Go to the target container by using the SSH tool and run **df -lh** to check whether the disk usage is normal (less than 90%).

10.1.5.1.4. Inspection alerts

The monitoring component periodically inspects EDAS over HTTP, TCP, PING, or DB based on the default inspection rule to monitor the condition of each component. An alert is triggered if a component is abnormal.

Possible causes

1. The check script is missing.
2. The component process breaks down.
3. The container breaks down.

Impact on the system

- If a single container is down, the business is not affected due to the high availability of the component cluster.
- If all containers are down, you cannot log on to the console and tasks cannot be implemented in the console. However, the business is not affected.

Solutions

1. Log on to the Apsara Infrastructure Management Framework console.
2. Log on to TerminalService of the component.
3. In the command line section next to **TerminalService**, run the `docker ps | grep <Component name>` command to check whether the component process exists.
   - If the process does not exist, run the `docker restart ${container_id}` command to restart the container, and then run the dial test again.
   - For information about how to troubleshoot the issue if the process exists, see .
4. Check the components such as OVS and VLAN based on the *Basic Component O&M Guide* to troubleshoot network faults.

10.1.5.2. Service continuity exceptions

10.1.5.2.1. EDAS monitoring exceptions

This topic describes how to troubleshoot Enterprise Distributed Application Service (EDAS) monitoring exceptions.

Problem description

- No application data can be monitored in the EDAS console.
- Data monitoring in the EDAS console has a significant lag.
- The monitoring and alerts features are ineffective.
- Traces cannot be queried.

Possible causes

The EDAS components and dependent components are abnormal.

Impact on the system

EDAS cannot monitor applications or services, or monitoring is inefficient.

Procedure

1. Check whether related components, such as Tlog, JStorm, and HBase, are normal.
   - If TLog is abnormal, log on to the instance where TLog is located, go to */home/admin/logs/*, and check the *tlogconsole.log* file. Then, troubleshoot the problem and restart TLog.
   - If JStorm is abnormal, log on to the instance where JStorm is located and check the log for the data collection task, such as */home/admin/logs/tlog_eagleeye-worker-6801.log*. Troubleshoot the problem and restart JStorm.

     > ? **Note** You need to restart each JStorm process. Otherwise, data cannot be written to HBase due to a connection error.

   - If HBase is abnormal, log on to the instance where HBase is located and check the related error log. Troubleshoot the problem and restart HBase.

Result

Check whether EDAS monitoring becomes normal.

10.1.5.2.2. Excessive node logs

This topic describes how to troubleshoot the problem of excessive node logs for EDAS.

Problem description

- Trace queries and system responses slow down, and disk usage alerts are reported.
- The service instance generates excessive log files.

Possible causes

A large amount of log files are not cleared from the disk in a timely manner, which affects system performance.

Impact on the system

Service nodes become less responsive.

Procedure

1. Log on to the EDAS component node to check logs.
   - Path to EagleEye logs: /home/admin/logs/eagleeye
   - Path to EDAS logs: /home/admin/edas/logs
2. Ensure that service logs are not printed on the preceding paths or that service logs have been backed up.

3. Clear backup logs by running **find /home/admin/logs/ -name "*log.*" -exec rm {};** or **find /home/admin/edas/logs/ -name "*log.*" -exec rm {};**.

Result

Check whether the service nodes become normal.

10.1.5.2.3. Console access failure

This topic describes how to troubleshoot EDAS console access failures.

Symptoms

The EDAS console cannot be accessed.

Possible causes

- The edas-console node is abnormal.
- An error occurs during DNS resolution.

Impact on the system

The EDAS console is unavailable.

Procedure

1. Troubleshoot the edas-console node errors.
   - If the EDAS console becomes accessible again, no further action is required.
   - If the EDAS console remains inaccessible, proceed with the next step.
2. Log on to the ECS instance where the edas-console node is located, go to */home/admin/edas/logs*, and check console.log for the problem.

Result

The EDAS console becomes accessible again.

10.1.5.2.4. Failure to import an ECS instance

This topic describes how to troubleshoot the failure to import an Elastic Compute Service (ECS) instance.

Problem description

An ECS instance fails to be imported.

Possible causes

- An Alibaba Cloud API operation fails to be called.
- An image fails to be replaced.
- The ECS instance fails to be registered.

Impact on the system

The service availability and reliability are compromised.

Procedure

1. Log on the EDAS console, and manually import the ECS instance.
2. If the ECS instance failed to be registered, register it again by running edas init.
3. If the image failed to be registered, Log on the ECS console, and check the specific status.

10.1.5.2.5. TLog data collection errors

This topic describes how to fix TLog data collection errors.

Symptoms

- The application monitoring dashboard is inaccessible.
- Application and service monitoring is inaccessible, and alarms cannot be triggered.
- Infrastructure monitoring is inaccessible, auto scaling is ineffective, and alarms cannot be triggered.
- Traces cannot be queried.

Possible causes

Collection point: Each collection job of TLog is called a collection point.

Collection points are the basic units for task processing by TLog. The monitoring function of EDAS is provided by one or more collection points in TLog. When working properly, collection points are in the activated or running state.

If the collection point for a product encounters an error, the corresponding EDAS monitoring data or page shows an exception.

- The basic data of the monitoring dashboard corresponds to the collection point service group TLog and the collection point infrastructure.
- The service data of the monitoring dashboard corresponds to the collection point service group EagleEye and the collection point stats_logger_agg.
- The zoom-in (more than 30 minutes) function in infrastructure monitoring corresponds to the collection point service group TLog and the collection point infrastructure.
- Service monitoring corresponds to the collection point service group EagleEye and the collection point stats_logger_agg.
- Trace analysis and query corresponds to the collection point service group TLog and the collection point EagleEye.

Impact on the system

An application change fails.

Procedure

1. Identify the corresponding TLog collection point based on the abnormal function.
2. Check whether the collection point has been started properly.

i. On the Collection Points page, locate the row that contains the collection point, and click **More** > **Manually Assign Task** in the Actions column. View the dialog box that appears.

   - If the number in the dialog box is greater than 0, the collection point has been started properly. You can go to the next step.
   - If the collection point is not started properly, return to the Collection Points page and click **Edit/Deployment Process**. On the page shown in the following figure, click **Start** and wait until "Operation successful" appears in the result. If "Operation successful" does not appear in the result, contact EDAS Customer Services and give feedback like "The xxx collection point does not start properly."
   - If "Operation successful" appears in the result, return to the **Collection Points** page, wait for three to five minutes, and click Manually Assign Task again. If the number in the dialog box that appears is greater than 0, the collection point has been started properly. Go to the next step.

3. If the collection point has been started, check whether the collection rules are correctly distributed (operation risk level: G1).
   - On the Collection Points page, check whether the distribution status is Active. If it is Inactive, click **Activate** and **OK** in sequence.
   - Click **Collection Point Details** to go to the **Collector Status** tab. If the status list is not empty, collection rules are distributed properly. Go to the next step.
   - If the status list on the **Collector Status** tab is empty, return to the Collection Points page to manually distribute collection rules as follows: Click **Create Task by Rule** under **Collection Rule**. If the number of created tasks in the dialog box shown in the following figure is greater than 0, click **OK**. Return to the Collection Points page and click **Manually Assign Task** and **OK** in sequence. If manual distribution is successful, a dialog box appears.
   - If the number of created tasks in **Create Task by Rule** is 0, contact EDAS Customer Services for troubleshooting and give feedback like "The xxx collection point has 0 created tasks in Create Task by Rule."
4. If the collection point has been started and collection rules are distributed properly but no data exists, perform troubleshooting as follows (operation risk level: G1):
   - Click **Collection Point Details** to go to the **Collector Status** tab. Check the data in the **Last Collection Attempt** column. Normally, the time in this column is less than 1 minute. If the time in this column is generally greater than 1 minute, contact EDAS Customer Services and give feedback like "On the Collector Status tab for the xxx collection point, the time in the Last Collection Attempt column is generally greater than 1 minute. The collection point must be scaled up."
   - On the **Collector Status** tab, check the data in the Status column. Normally, the states in this column are Normal or File Not Modified. If states such as File Not Found, No Permission, Connection Timeout, and SProxy Not Found appear in this column, contact EDAS Customer Services and give feedback like "On the Collector Status tab for the xxx collection point, the yyy state appears in the Status Column."
   - On the **Collection Points** page, click **More > Perform Health Check**. Then, contact EDAS Customer Services and provide the JSON content on the health check page to help engineers quickly locate the problem.

10.1.6. Log reference

You can check logs to view the status of each EDAS component or locate faults during O&M.

EDAS provides logs for the following components:

- EDAS console
- EDAS admin
- EDAS server
- Cai-fs
- DiamondServer
- ConfigServer
- Cai-address
- EagleEye console

EDAS archives and clears the logs for these components based on predefined policies.

10.1.6.1. EDAS console logs

The EDAS console is the console component of EDAS. It provides the core functions of the PaaS platform, including resource management, application lifecycle management, service governance, and auto scaling.

Log files

EDAS console logs

File	Description
console.log	The EDAS console log.
changeorder.log	The change order log.
openapi.log	The API log.
tengine.log	The TEngine log.
debug.log	The log that records the internal API calls of the EDAS console.

Path

- Logging path: *${user.home}/edas/logs*
- Archive path: *${user.home}/edas/logs/bak*

Format

openapi.log: %msg%n (print log information directly) others: %d{yyyy-MM-dd HH:mm:ss.SSS} [%thread] %-5level %logger{50}:%line - %msg%n (date and time, thread name, log level, class name: number of lines - specific log information)

Archiving policies

EDAS console log archiving policies

Log	Archiving policy
console.log	• Maximum size: 100 MB • The name of the new file takes the format console.{d}.log. Seven logs are retained.
changeorder.log	• A file is created every day. • The name of the new file takes the format changeorder.{yyyy-MM-dd}.log. Logs from the last seven days are retained.
openapi.log	• A file is created every day. • The name of the new file takes the format opanapi.{yyyy-MM-dd}.log. Logs from the last seven days are retained.
tengine.log	• A file is created every day. • The name of the new file takes the format tengine.{yyyy-MM-dd}.log. Logs from the last seven days are retained.
debug.log	• Maximum size: 100 MB • The name of the new file takes the format debug.{d}.log. Three logs are retained.

10.1.6.2. EDAS admin logs

The EDAS admin is a background task service that provides the instance synchronization and application health check functions.

File

EDAS admin logs

File	Description
admin.log	The scheduling task log.
tengine.log	The Tengine log.

Path

- Logging path: *${user.home}/edas/logs*
- Archive path: *${user.home}/edas/logs/bak*

Format

%d{yyyy-MM-dd HH:mm:ss.SSS} [%thread] %-5level %logger{50}:%line - %msg%n (date and time, thread name, log level, category name: number of lines - specific log information)

Archiving policy

EDAS admin log archiving policies

Log	Archiving policy
admin.log	• Maximum size: 100 MB • The name of the new file takes the format admin.{d}.log. Three logs are retained.
tengine.log	• A file is created every day. • The name of the new file takes the format tengine.{yyyy-MM-dd}.log. Logs from the last seven days are retained.

10.1.6.3. EDAS server logs

The EDAS server synchronizes status information with EDAS Agent.

File

EDAS server logs

File	Description
agent-server.log	The log for the instance where EDAS Agent is installed.
changeorder.log	The change order log.
tengine.log	The Tengine log.

Path

- Logging path: *${user.home}/edas/logs*
- Archive path: *${user.home}/edas/logs/bak*

Format

agent-server: %d{HH:mm:ss.SSS} [%thread] %-5level %logger{36}:%line - %msg%n(time, thread name, log level, category name: number of lines - specific log information) others: %d{yyyy-MM-dd HH:mm:ss.SSS} [%thread] %-5level %logger{50}:%line - %msg%n (date and time, thread name, log level, category name: number of lines - specific log information)

Archiving policy

Archiving policy for EDAS server logs

Log	Archiving policy
agent-server.log	• A file is created every day. • The name of the new file takes the format agent-server-.{yyyy-MM-dd}.log. Logs from the last seven days are retained.

Log	Archiving policy
tengine.log	● A file is created every day. ● The name of the new file takes the format tengine.{yyyy-MM-dd}.log. Logs from the last seven days are retained.
changeorder.log	● A file is created every day. ● The name of the new file takes the format changeorder.{yyyy-MM-dd}.log. Logs from the last seven days are retained.

10.1.6.4. DiamondServer logs

A configuration management service. It provides configuration storage, query, and notification functions, and primarily stores database metadata and EDAS function switch configurations in EDAS.

File

DiamondServer logs

File	Description
diamondServer.log	The DiamondServer log.
fata.log	The most important system log, which records database service errors, "master db not found" messages, and other information.
dump.log	The log that records the dumping of configurations to the local device.

Path

- Logging path: *${user.home}/admin/diamond/logs*
- Archive path: *${user.home}/admin/diamond/logs*

Format

[%p] [%t] %d{MM-dd HH:mm:ss,SSS} [%c{1}] - %m%n (log information priority, log event thread name, logging time, log information category, and specific log information)

Archiving policy

The archiving policies vary depending on the version. For example, in the latest version 3.8.8, a log is 15 MB in size and 10 logs are retained.

10.1.6.5. Cai-fs logs

A file server. It stores the EDAS Agent installation package and EDAS application packages.

Log files

EDAS console logs

File	Description
efs-server.log	Cai-fs logs

Path

- Logging path: *${user.home}/efs/logs*
- Archive path: *${user.home}/efs/logs*

Format

%d{HH:mm:ss} [%thread] %-5level %logger{36} - %msg%n (time, thread name, log level, class name: number of lines - specific log information)

Archiving policies

EDAS admin log archiving policies

Log	Archiving policy
efs-server.log	- Maximum size: 100 MB - The name of the new file takes the format efs-server.log.{d}. Three logs are retained.

10.1.6.6. ConfigServer logs

An RPC service registry. It is used to query and store the publishing and subscription data of services.

Log files

EDAS console logs

File	Description
cluster.log	The log that records cluster operations, such as merging tasks and connecting to or disconnecting from other instances in the cluster.
memory.log	The log that records memory statuses, including the total number of subscriptions and the amount of persistent data of an instance.
persistent.log	The data persistence log.
push.log	The data push log.
http.log	The log that records the instance commands called over HTTP.
monitor.log	The warning code log.

Path

- Logging path: *${user.home}/admin/configserver/log*

- Archive path: *${user.home}/admin/configserver/log*

Format

%date %level %msg%n%n (logging time, log level, and specific log information)

Archiving policies

- A file is created every day.
- The name of the new file takes the format {module}.log.%d{yyyy-MM-dd}.log. Logs from the last 15 days are retained.

10.1.6.7. Cai-address logs

An address discovery service. It provides the address lists for DiamondServer and ConfigServer.

Log files

EDAS console logs

File	Description
access.log	All access logs
error.log	Error logs

Path

- Logging path: *${user.home}/admin/cai/logs*
- Archive path: *${user.home}/admin/cai/logs*

Format

"$remote_addr $request_time_usec $http_x_readtime [$time_local] \"$request_method http://$host$request_uri\" $status $body_bytes_sent \"$http_referer\" \"$http_user_agent\" \"$md5_encode_cookie_unb\" \"$md5_encode_$cookie_cookie2\" \"$eagleeye_traceid\""; records the client IP address - request elapsed time - request header - request status - the number of bytes sent to the client - records the link from which the access request is received - records information about the web browser of the client - performs MD5 on cookies to obtain fixed-length cookies - eagleeye trace id

Archiving policies

Log splitting is not performed.

10.1.6.8. EagleEye console logs

You can query and view service traces.

Log files

EDAS console logs

File	Description
eagleeye-console.log	All console access logs
eagleeye-sql.log	Trace query logs

Path

- Logging path: *${user.home}/admin/logs*
- Archive path: *${user.home}/admin/logs*

Format

%d{yyyy-MM-dd HH:mm:ss.SSS} [%thread] %msg%n (time, thread name, and specific log information)

Archiving policies

Archiving policies of EagleEye console access logs

Log	Archiving policy
eagleeye-console.log	Maximum size: 500 MB Retention period: 30 days
eagleeye-sql.log	Maximum size: 200 MB Retention period: 15 days

10.1.7. Configuration reference

You need to complete basic configuration and optimization configuration during the EDAS O&M process.

The configuration during EDAS O&M is divided into component configuration and JVM configuration.

10.1.7.1. Component configuration

You can configure the basic settings of components by using configuration files.

Parameters

Component	Configuration file	Path	Configuration item	Description	Value

Component	Configuration file	Path	Configuration item	Description	Value
EDAS console	config.properties	/home/admin/edas/conf/	dataSource.config.URL	Database connection string	Standard database connection string, such as *jdbc:mysql://edastest.mysql.rds.aliyuncs.com/edas?rewriteBatchedStatements=true*
			dataSource.config.user	Username	Standard database username
			dataSource.config.password	Password	Standard database password
EDAS admin	config.properties	/home/admin/edas/conf/	dataSource.config.URL	Database connection string	Standard database connection string, such as *jdbc:mysql://edastest.mysql.rds.aliyuncs.com/edas?rewriteBatchedStatements=true*
			dataSource.config.user	Username	Standard database username
			dataSource.config.password	Password	Standard database password
Redis console	redis.conf	/home/admin/redis-2.8.17/src/	dataSource.config.URL	Database connection string	Standard database connection string
			dataSource.config.user	Username	Standard database username
			dataSource.config.password	Password	Standard database password

Component	Configuration file	Path	Configuration item	Description	Value
TLog console	tlog-cloud.properties	/home/admin/taobao-tomcat-production-7.0.59.3/lib/	config.tlog.zk.servers	ZooKeeper connection string	Standard ZooKeeper address information, such as *192.168.1.2:2181, 192.168.1.3:2181, and 192.168.1.4:2181*
			config.tlog.hbase.zkServers	ZooKeeper used by HBase	Standard ZooKeeper connection string, which is shared by default and is consistent with the preceding ZooKeeper
			config.tlog.hbase.zkRootNode	HBase root node	Default value: /hbase
			config.nimbus.host	JStorm nimbus node	IP address of the primary node
			config.edas.console.url	EDAS admin address	EDAS admin domain name
HBase	hbase-site.xml	/home/admin/hbase{-Version}/conf/	hbase.rootdir	Host name of the primary instance	Note that the host name cannot be an IP address and must be bound in */etc/hosts* if it cannot be resolved. All HBase-based applications must be bound to the host names of all HBase instances.

Component	Configuration file	Path	Configuration item	Description	Value
			hbase.zookeeper.quorum	ZooKeeper connection string	ZooKeeper connection string
			hbase.zookeeper.property.clientPort	ZooKeeper port	ZooKeeper port
Jstorm	storm.yaml	/home/admin/jstorm/conf/	storm.zookeeper.servers	IP addresses of all storm nodes	IP addresses of all storm nodes
			nimbus.host	Primary node of JStorm nimbus	Primary node of JStorm nimbus
			supervisor.slots.port.cpu.weight	CPU weight	Number of CPUs occupied by each task
ConfigServer	confsrv.conf	/home/admin/configserver/conf/	serverlist	Server list	A list of IP addresses separated with commas (,)
			unitserverlist	Modular server list	The content is the same as that of serverlist.
DiamondServer	config.properties	/home/admin/diamond/target/diamond.war/WEB-INF/classes/	openInnerInterfaceFilter	Indicates whether to enable internal interface access verification.	The default value is false. Enter false to avoid failed verification because Address-Server is typically configured with a virtual IP address rather than a real one.
			OPEN_SPAS	Indicates whether to enable authentication.	The value is true, which indicates that authentication is enabled.

10.1.7.2. JVM configuration

You can optimize system performance through a JVM configuration.

The parameters vary slightly depending on the JDK versions.

Parameters

Name	Description	Applicable JDK version	Reference value
-Xms	Specifies the initial heap memory size for the JVM.	All JDK versions	4 GB
-Xmx	Specifies the maximum heap memory size for the JVM.	All JDK versions	4 GB
-Xmn	Specifies the size of the young generation.	All JDK versions	2 GB
-Xss	Specifies the stack size of each thread.	All JDK versions	2 MB
-XX:+UseCompressedOops	Compresses common object pointers.	All JDK versions	-
-XX:SurvivorRatio	Specifies the ratio of Survivor to Eden.	All JDK versions	10
-XX:+UseConcMarkSweepGC	Uses the Concurrent Mark Sweep (CMS) collector for memory collection.	All JDK versions	-
-XX:+UseCMSCompactAtFullCollection	Instructs the CMS collector to compress the old generation upon full GC.	All JDK versions	-
-XX:CMSMaxAbortablePrecleanTime		All JDK versions	5000
-XX:+CMSClassUnloadingEnabled	Specifies that CMS GC is triggered after class unloading.	All JDK versions	-
-XX:CMSInitiatingOccupancyFraction	Sets the threshold size of the old generation that triggers CMS GC.	All JDK versions	80

Name	Description	Applicable JDK version	Reference value
-XX:PermSize	Specifies the initial value of the permanent generation.	1.7 and earlier versions	196 MB
-XX:MaxPermSize	Specifies the maximum value of the permanent generation.	1.7 and earlier versions	256 MB
MetaspaceSize	Sets the threshold size of the allocated metadata space that triggers full GC.	1.8 and later versions	196 MB
MaxMetaspaceSize	Sets the maximum size of the allocated metadata space that triggers full GC.	1.8 and later versions	256 MB
-XX:+DisableExplicitGC	Disables System.gc().	All JDK versions	-
-XX:+HeapDumpOnOutOfMemoryError		All JDK versions	-
-XX:HeapDumpPath	Specifies the heap dump path.	All JDK versions	/home/admin/logs/oomDump.log

11.Operations of big data products

11.1. Apsara Big Data Manager (ABM) platform

11.1.1. Routine maintenance

11.1.1.1. Perform routine maintenance

You can perform routine maintenance on Apsara Big Data Manager (ABM) through the Apsara Infrastructure Management Framework console.

Apsara Infrastructure Management Framework

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner, and then click **TIANJI** to log on to the Apsara Infrastructure Management Framework console.
3. Go to the **Clusters** page in the ABM console and verify that all containers are in their final state.
4. Go to the **Dashboard** page in the ABM console and verify that alerts have not been generated.

Metrics and alert handling

- Hardware monitoring

  The system retains logs for 30 days and automatically deletes old logs. If a disk alert is triggered when a large volume of logs exhaust disk space, contact technical support.

- System exception

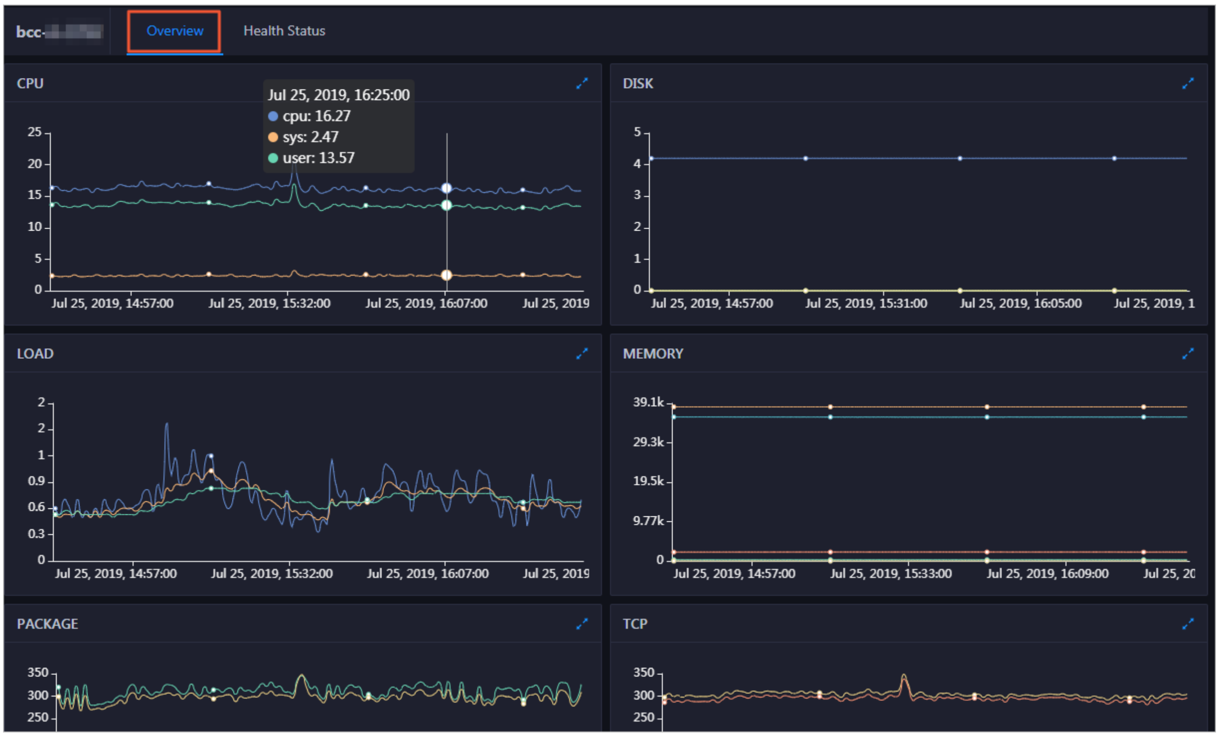
  If a system exception is thrown during the inspection, handle the exception in the ABM console. If the exception message is unclear, contact technical support.

11.1.1.2. View the ABM operating status

ABM monitors its own health and operating metrics. You need to regularly handle ABM alerts and view ABM operating metrics to evaluate system downtime risks in the future.

View ABM operating metrics

In ABM, click **O&M** on the top and click **Clusters**. The **Overview** tab appears.

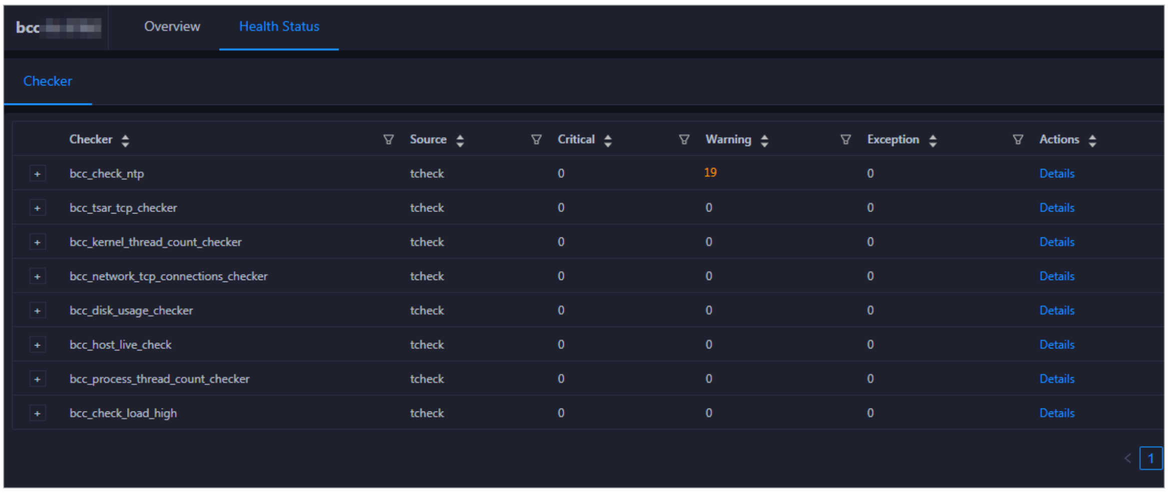


The **Overview** tab displays tendency charts for cluster metrics, including the CPU, memory, disk, load, package, TCP, and disk root directory usage. You need to regularly view and record these metrics to evaluate system downtime risks in the future.

Handle ABM alerts

ABM cluster alerts are classified into Critical, Warning, and Exception alerts. You need to handle these alerts in time, especially Critical and Warning alerts.

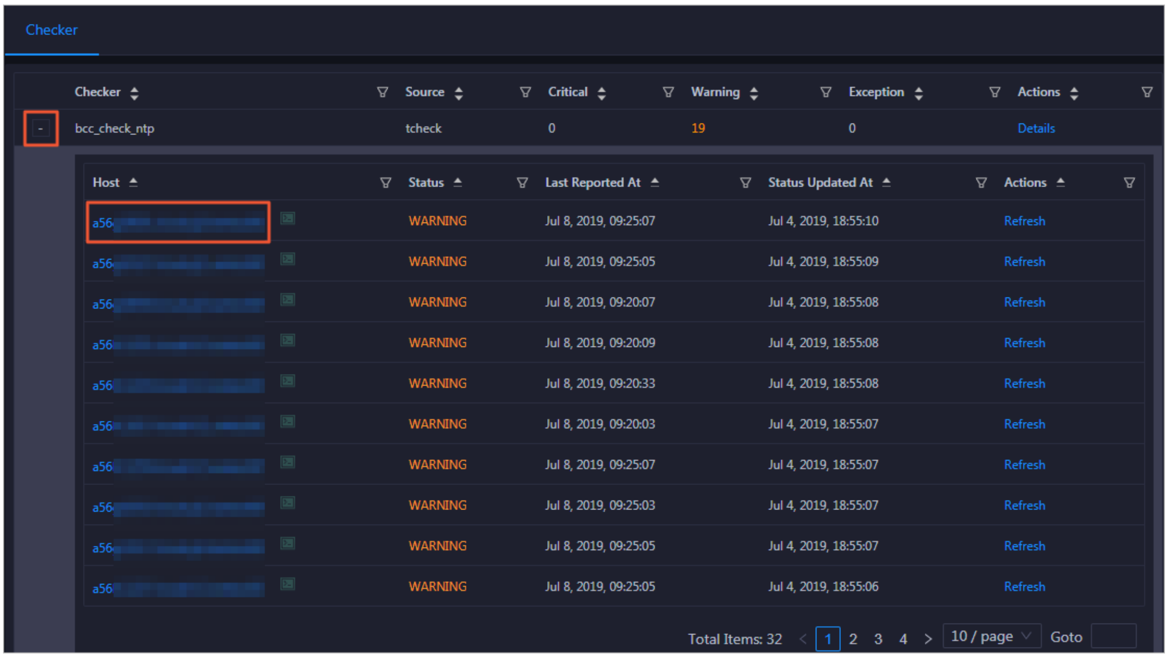
1. On the **Clusters** page, click the **Health Status** tab.



	Checker	Source	Critical	Warning	Exception	Actions
+	bcc_check_ntp	tcheck	0	19	0	Details
+	bcc_tsar_tcp_checker	tcheck	0	0	0	Details
+	bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
+	bcc_network_tcp_connections_checker	tcheck	0	0	0	Details
+	bcc_disk_usage_checker	tcheck	0	0	0	Details
+	bcc_host_live_check	tcheck	0	0	0	Details
+	bcc_process_thread_count_checker	tcheck	0	0	0	Details
+	bcc_check_load_high	tcheck	0	0	0	Details

The **Health Status** tab displays all check items and the alerts that were generated during the check.

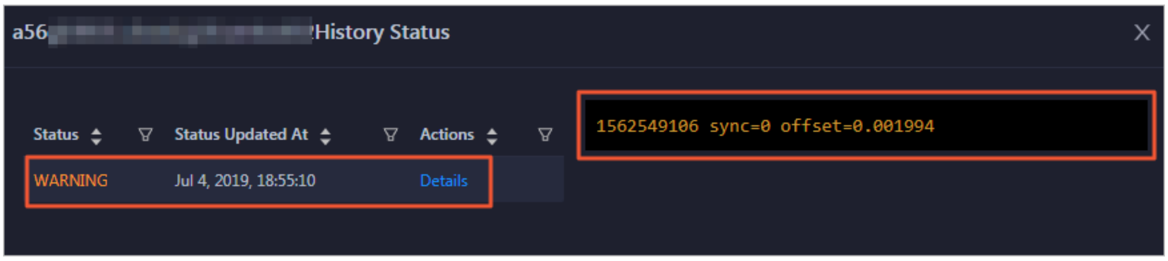
2. Click the **Fold** icon for a check item with alerts. All hosts on which the check item was performed appear.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:06	Refresh

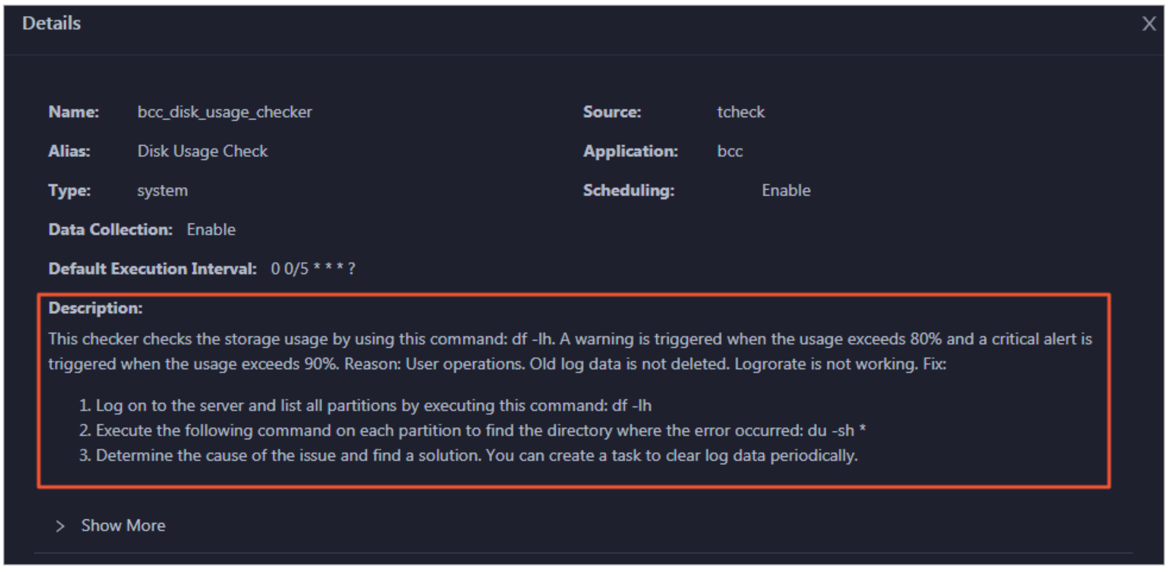
3. Click a host. In the dialog box that appears, click **Details** for an alert. The alert cause appears on the right.


a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

4. Click **Details** for a check item with an alert and view the fix method for the alert in the dialog box that appears.


Details

Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

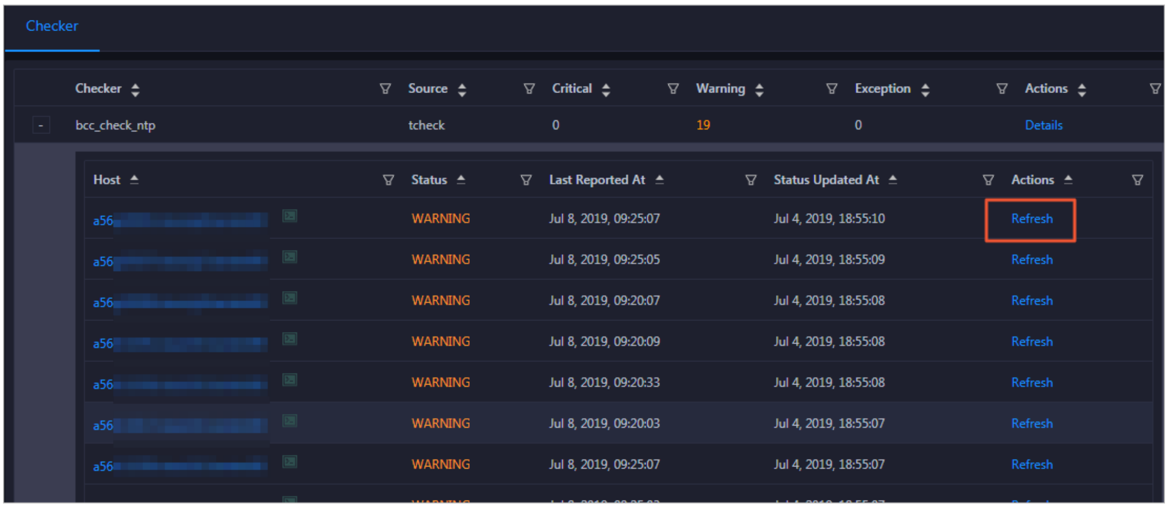
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

5. Handle the alert based on the fix method.

   You may need to log on to the host when handling the alert. For more information, see Log on to a host.

6. After the alert is handled, click **Refresh** for the host to perform the check again in real time. In this way, you can check whether the alert is cleared.



Checker

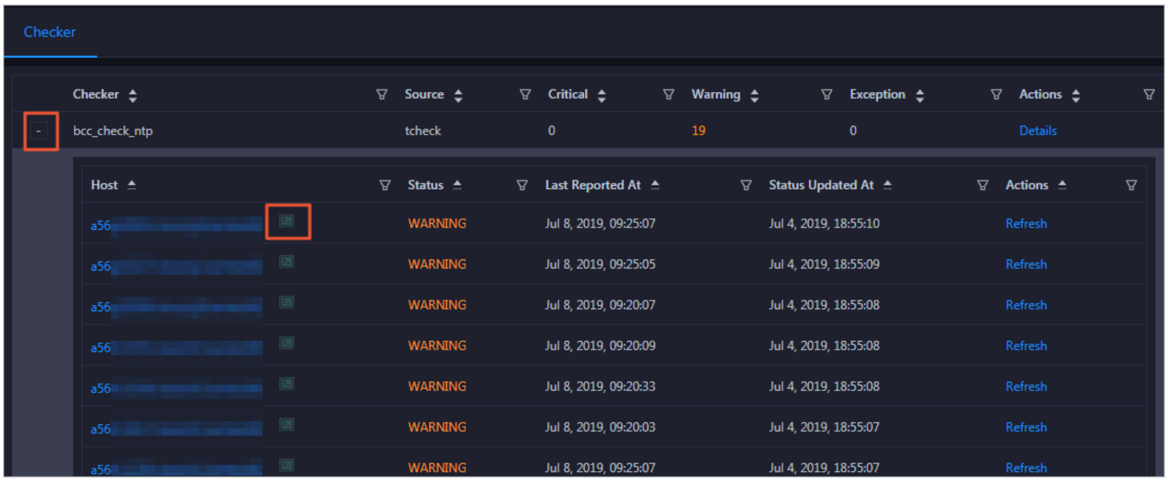
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

Log on to a host

You may need to log on to a host to handle alerts or other issues that occurred on the host.

1. On the Health Status tab, click the **Fold** icon for a check item.

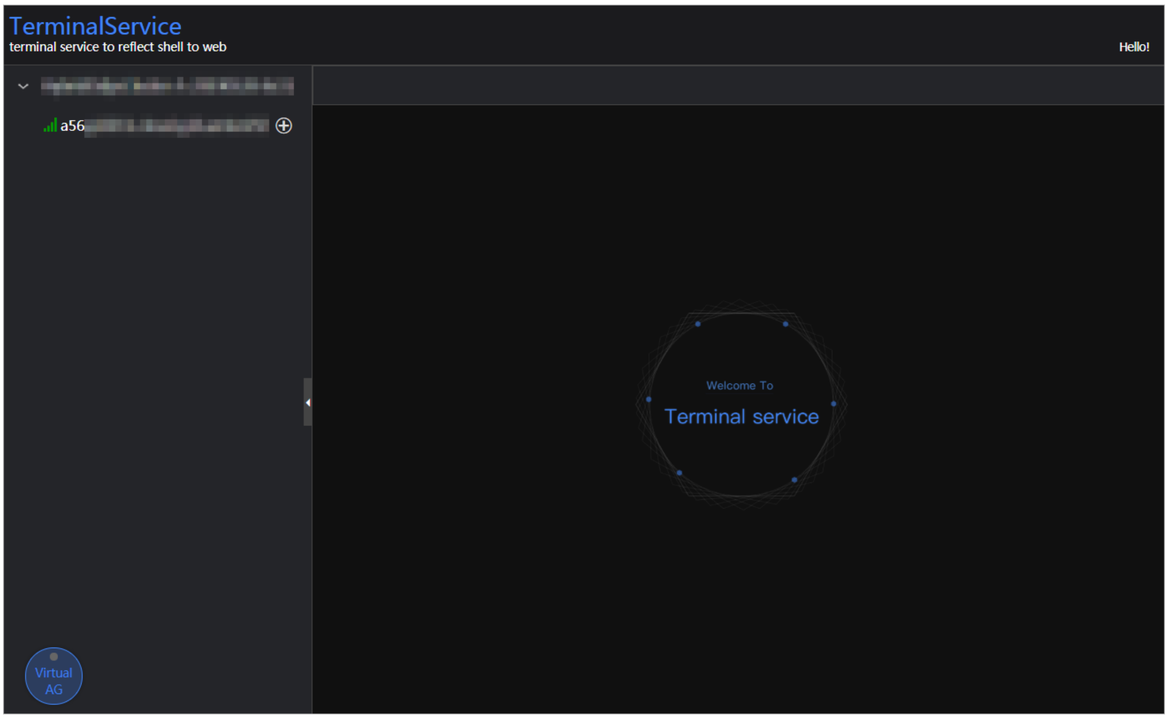


Checker

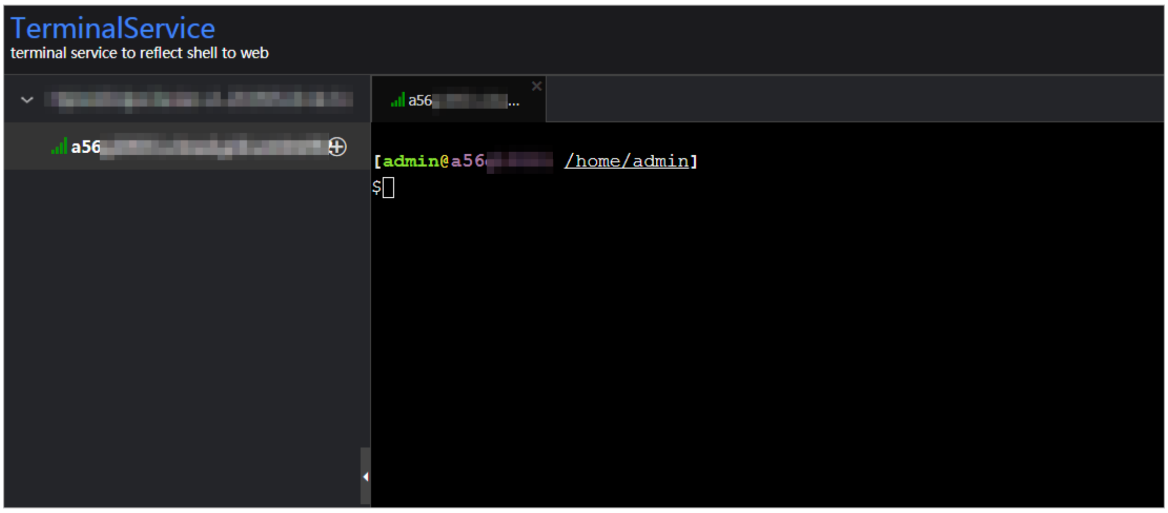
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

2. Click the **Logon** icon for a host. The **TerminalService** page appears.



3. On the **TerminalService** page, select the host on the left to log on to it.



```
[admin@a56[redacted] /home/admin]
$
```

11.1.1.3. Troubleshooting

Common failures

- **Logon failure**

  If you failed to log on to ABM, clear the cache and cookies in your web browser, and then try again.

  Based on the logon failure message that appears, check whether the following issues exist:

  - The password that you entered is incorrect.
  - Your account has been locked.
  - Your account has been disabled.

- **Other failures**

Contact technical support.

11.1.2. Backup and restore

Back up data

ABM uses a high-availability database. You do not need to manually back up data. To obtain full backup data, contact technical support.

Restore data

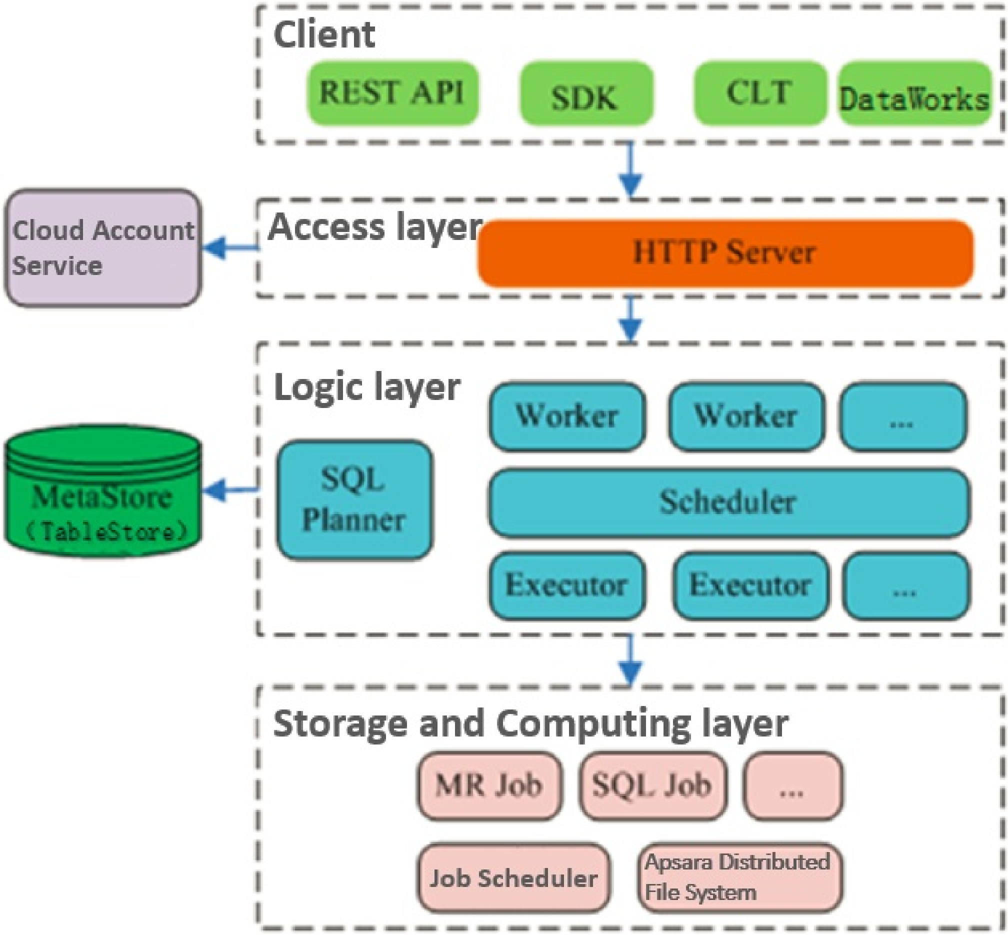
You do not need to restore data for ABM.

11.2. MaxCompute

11.2.1. Concepts and architecture

MaxCompute architecture shows the MaxCompute architecture.

MaxCompute architecture



The MaxCompute service is divided into four parts: **client**, **access layer**, **logic layer**, and **storage and computing layer**. Each layer can be horizontally scaled.

The following methods can be used to implement the functions of a MaxCompute client:

- **API**: RESTful APIs are used to provide offline data processing services.
- **SDK**: RESTful APIs are encapsulated within SDKs. SDKs are currently available in programming languages such as Java.
- **Command line tool (CLT)**: This client-side tool runs on Windows and Linux. CLT allows you to submit commands to manage projects and use DDL and DML.
- **DataWorks**: DataWorks provides upper-layer visual ETL and BI tools that allow you to synchronize data, schedule tasks, and create reports.

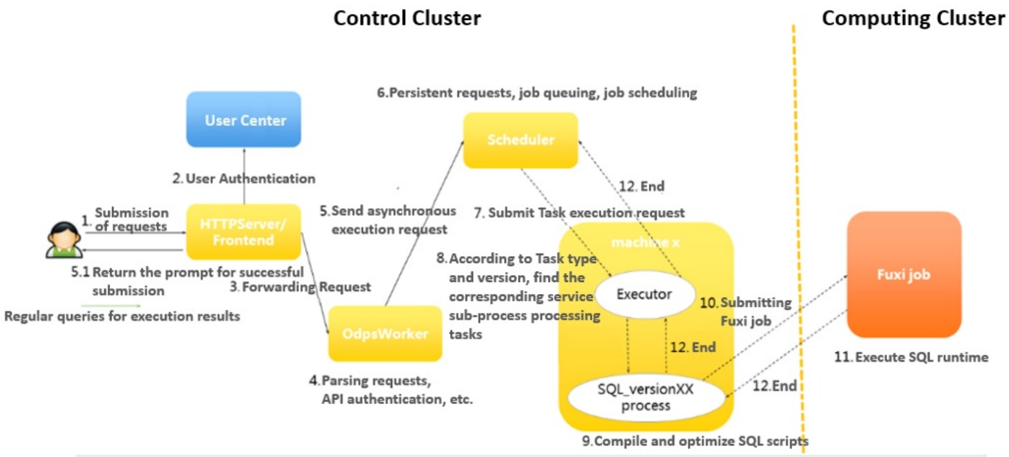
The access layer of MaxCompute supports HTTP, HTTPS, load balancing, user authentication, and service-level access control.

The logic layer is at the core of MaxCompute and supports project and object management, command parsing and execution logic, and data object access control and authorization. The logic layer contains two clusters: control and compute clusters. The control cluster is designed to manage projects and objects, parse and start queries and commands, and control and authorize access to data objects. The compute cluster executes tasks. Both control and compute clusters can be horizontally scaled as needed. The control cluster has three roles: Worker, Scheduler, and Executor. These roles are described as follows:

- **The Worker role processes all RESTful requests** and manages projects, resources, and jobs. Workers forward jobs that need to launch Fuxi tasks (such as SQL, MapReduce, and Graph jobs) to the Scheduler for further processing.
- **The Scheduler role schedules instances**, splits instances into multiple tasks, sorts tasks that are pending for submission, and queries resource usage from FuxiMaster in the compute cluster for throttling. If there are no idle slots in Job Scheduler, the Scheduler stops processing task requests from Executors.
- **The Executor role is responsible for launching SQL and MapReduce tasks.** Executors submit Fuxi tasks to FuxiMaster in the compute cluster and monitor the operating status of these tasks.

When you submit a job request, the web server at the access layer queries the IP addresses of registered Workers and sends API requests to randomly selected Workers. The Workers then send these requests to the Scheduler for scheduling and throttling. Executors actively poll the Scheduler queue. If the necessary resources are available, the Executors start executing tasks and return the task execution status to the Scheduler. The following figure shows the MaxCompute job execution process.

MaxCompute job execution process


Control Cluster
Computing Cluster
6.Persistent requests, job queuing, job scheduling
User Center
Scheduler
2. User Authentication
12. End
1. Submission of requests
HTTPServer/ Frontend
5.Send asynchronous execution request
7. Submit Task execution request
machine x
5.1 Return the prompt for successful submission
3. Forwarding Request
8. According to Task type and version, find the corresponding service sub-process processing tasks
Executor
10. Submitting Fuxi job
Fuxi job
Regular queries for execution results
OdpsWorker
12. End
11. Execute SQL runtime
4. Parsing requests, API authentication, etc.
SQL_versionXX process
12.End
9.Compile and optimize SQL scripts

The following concepts are involved in the MaxCompute job execution process:

1. MaxCompute instance: the instance of a MaxCompute job. A job is anonymous if it is not defined. A MaxCompute job can contain multiple MaxCompute tasks. In a MaxCompute instance, you can submit multiple SQL or MapReduce tasks, and specify whether to run the tasks in parallel or serial mode. This scenario is rarely seen because MaxCompute jobs are not commonly used. In most cases, an instance contains only one task.
2. MaxCompute task: a specific task in MaxCompute. Currently, there are almost 20 task types, such as SQL, MapReduce, Admin, Lot, and Xlib. The execution logic varies greatly depending on the task type. Different tasks in an instance are differentiated by their task name. MaxCompute tasks can run in the control cluster. Simple tasks such as metadata modification can run in the control cluster for their entire lifecycles. To run computing tasks, submit Fuxi jobs to the compute cluster.
3. Fuxi job: a computing model provided by the Job Scheduler module. A Fuxi job corresponds to a Fuxi service. A Fuxi job represents a task that can be completed, while a Fuxi service represents a resident process.
    - The DAG scheduling approach can be used to schedule Fuxi jobs. Each job has a job master to schedule its job resources.
    - For SQL, Fuxi jobs are divided into offline and online jobs. Online jobs evolve from the service mode jobs. An online job is also called a quasi-real-time task. An online job is a resident process that can be executed whenever there are tasks, reducing the time required to start and stop a job.
    - You can submit a MaxCompute task to multiple compute clusters. The primary key name of a Fuxi job is the cluster name followed by the job name.
    - The JSON plan for Job Scheduler to submit a job and the status of a finished job are stored in Apsara Distributed File System.
4. Fuxi task: a sub-concept of Fuxi job. Similar to MaxCompute tasks, different Fuxi tasks represent different execution logics. Fuxi tasks can be linked together as pipes to implement complex logic.
5. Fuxi instance: the instance of a Fuxi task. A Fuxi instance is the smallest unit that can be scheduled by Job Scheduler. During the actual execution process, a task is divided into many logical units to improve the processing speed. Different instances will run on the same execution logic but work with different input and output data.
6. Fuxi worker: an underlying concept of Job Scheduler. A worker represents an operating system

process. A worker can be reused by multiple Fuxi instances, but a worker can only handle one instance at a time.

Note

- InstanceID: the unique identifier of a MaxCompute job. It is commonly used for troubleshooting. You can construct the LogView of the current instance based on the project name and instance ID.
- Service master or job master: a primary node of the service or job type. The primary node is responsible for requesting and scheduling resources, creating work plans for workers, and monitoring workers across their entire lifecycles.

The storage and computing layer of MaxCompute is a core component of the proprietary cloud computing platform of Alibaba Cloud. As the kernel of the Apsara system, this component runs in the compute cluster independent of the control cluster. The architecture diagram illustrates only the major modules.

11.2.2. O&M commands and tools

11.2.2.1. Before you start

Before using MaxCompute O&M commands and tools, you must be aware of the following information:

During the MaxCompute O&M process, the default account is admin. You must run all commands as an admin user. You must use your admin account and sudo to run commands that require sudo privileges.

11.2.2.2. odpscmd commands

You can use the command line to perform operations and maintenance. You must log on to the command line tool before you can run commands. The specific procedure is as follows:

1. Log on to the Apsara Infrastructure Management Framework console. In the left-side navigation pane, choose **Operations > Cluster Operations**. In the **Cluster** search box, enter odps to search for the expected cluster.
2. Click the cluster in the search result. On the Cluster Details page, click the **Services** tab. In the **Services** search box, search for **odps-service-computer**. Click odps-service-computer in the search result.
3. After you access the **odps-service-computer** service, select **ComputerInit#** on the Service Details page. In the Actions column corresponding to the machine, click **Terminal**. In the TerminalService window that appears, you can perform subsequent command line operations.

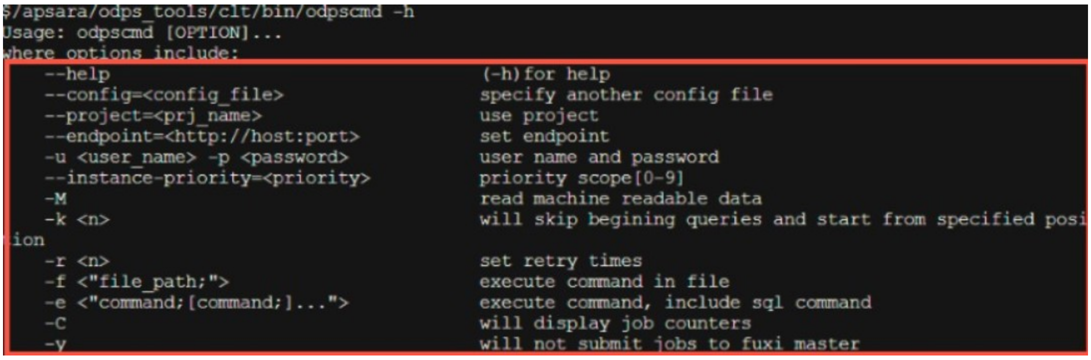
Console command directories and configurations

The MaxCompute client is located in the clt folder under the */apsara/odps_tools* directory of odpsag. The client configuration file is located in the conf directory under the clt folder. The access_id, access_key, end_point, log_view, and tunnel_point parameters are configured by default. You can use the `./clt/bin/odpscmd` command to view information such as the version number in interactive mode. For example, run the `HTTP GET /projects/admin_task_project/system;` command to check the version information of MaxCompute.

Description of client command options

The following figure shows the client command options.

Client command options



```
$/apsara/odps_tools/clt/bin/odpscmd -h
Usage: odpscmd [OPTION]...
where options include:
    --help                                  (-h)for help
    --config=<config_file>                  specify another config file
    --project=<prj_name>                    use project
    --endpoint=<http://host:port>           set endpoint
    -u <user_name> -p <password>            user name and password
    --instance-priority=<priority>          priority scope[0-9]
    -M                                      read machine readable data
    -k <n>                                  will skip begining queries and start from specified posi
ion
    -r <n>                                  set retry times
    -f <"file_path;">                       execute command in file
    -e <"command;[command;]...">            execute command, include sql command
    -C                                      will display job counters
    -y                                      will not submit jobs to fuxi master
```

- **-e**: The MaxCompute client does not execute SQL statements in interactive mode.
- **--project, -u, and -p**: The client directly uses the specified values for the project, user, and pass parameters. If you do not specify a parameter, the client uses the corresponding value configured in the conf file.
- **-k and -f**: The client directly executes local SQL files.
- **--instance-priority**: This option is used to assign a priority to the current task. Valid values: 0 to 9. A lower value indicates a higher priority.
- **-r**: This option indicates the number of times a failed command will be retried. It is commonly used in scripting jobs.

Commonly used SQL commands for O&M

The following table lists the commonly used commands.

Commonly used commands

Command	Description
whoami;	Allows you to view your Apsara Stack tenant account and endpoint information.
show p;	Allows you to view information about all instances that have been run.
wait <instanceid>;	Allows you to re-generate the LogView and Fuxi job information of a task. To run this command, you must have owner permissions, and the LogView and Fuxi job information must be stored in the same project.
kill <instanceid>;	Allows you to terminate specified instances.
tunnel upload/download;	Allows you to test whether Tunnel is functioning.

Command	Description
desc project <projectname> -extended;	Allows you to view the project usage. - **desc extended table**: allows you to view table information. - **desc table_name partition(pt_spec)**: allows you to view partition information. - **desc resource $resource_name**: allows you to view project resource information. - **desc project $project_name -extended**: allows you to view cluster information.
export <project name> local_file_path;	Allows you to export DDL statements of all tables in a project.
create table tablename (...) ;	Allows you to create a table.
select count(*) from tablename;	Allows you to search for a table.
Explain	Allows you to create plans without submitting Fuxi jobs to view resources required for tasks.
list	Allows you to list tables, resources, and roles.
show	Allows you to view table and partition information.
purge	Allows you to remove all data from the MaxCompute recycle bin directly to the Apsara Distributed File System recycle bin. - **purge table <tablename>**: allows you to purge a single table. - **purge all**: allows you to purge all tables from the current project.

11.2.2.3. Tunnel commands

The client provides Tunnel commands that implement the original functions of the Dship tool. Tunnel commands are mainly used to upload or download data.

Tunnel commands

Command	Description
tunnel upload	Allows you to upload data to MaxCompute tables. You can upload files or level-1 directories. Data can only be uploaded to a single table or table partition each time. The destination partition must be specified for partitioned tables.
tunnel download	Allows you to download data from MaxCompute tables. You can only download data to a single file. Only data in one table or partition can be downloaded to one file each time. For partitioned tables, the source partition must be specified.

Command	Description
tunnel resume	If an error occurs because of network or Tunnel service faults, you can resume file or directory transmission after interruption. This command only allows you to resume the previous data upload. Every data upload or download operation is called a session. Run the resume command and specify the ID of the session to be resumed.
tunnel show	Allows you to view historical task information.
tunnel purge	Purges the session directory. Sessions from the last three days are purged by default.

Tunnel commands allow you to view help information by using the Help sub-command on the client. The sub-commands of each Tunnel command are described as follows:

Upload

Imports data of a local file into a MaxCompute table. The following example shows how to use the sub-commands:

```
odps@ project_name>tunnel help upload;
usage: tunnel upload [options] <path> <[project.]table[/partition]>
          upload data from local file
 -acp,-auto-create-partition <ARG>   auto create target partition if not
                          exists, default false
 -bs,-block-size <ARG>           block size in MiB, default 100
 -c,-charset <ARG>              specify file charset, default ignore.
                          set ignore to download raw data
 -cp,-compress <ARG>             compress, default true
 -dbr,-discard-bad-records <ARG>     specify discard bad records
                          action(true|false), default false
 -dfp,-date-format-pattern <ARG>     specify date format pattern, default
                          yyyy-MM-dd HH:mm:ss
 -fd,-field-delimiter <ARG>        specify field delimiter, support
                          unicode, eg \u0001. default ","
 -h,-header <ARG>               if local file should have table
                          header, default false
 -mbr,-max-bad-records <ARG>       max bad records, default 1000
 -ni,-null-indicator <ARG>         specify null indicator string,
                          default ""(empty string)
 -rd,-record-delimiter <ARG>       specify record delimiter, support
                          unicode, eg \u0001. default "\r\n"
 -s,-scan <ARG>                specify scan file
                          action(true|false|only), default true
 -sd,-session-dir <ARG>           set session dir, default
                          D:\software\odpscmd_public\plugins\ds
                          hip
 -ss,-strict-schema <ARG>         specify strict schema mode. If false,
                          extra data will be abandoned and
                          insufficient field will be filled
                          with null. Default true
 -te,-tunnel_endpoint <ARG>       tunnel endpoint
   -threads <ARG>               number of threads, default 1
 -tz,-time-zone <ARG>            time zone, default local timezone:
                          Asia/Shanghai
Example:
  tunnel upload log.txt test_project.test_table/p1="b1",p2="b2"
```

Parameters:

- -acp: indicates whether to automatically create the destination partition if it does not exist. No destination partition is created by default.
- -bs: specifies the size of each data block uploaded with Tunnel. Default value: 100 MiB (MiB = 1024 * 1024B).
- -c: specifies the local data file encoding format. Default value: UTF-8. If this parameter is not set, the encoding format of the downloaded source data is used by default.
- -cp: indicates whether to compress the local data file before it is uploaded to reduce network traffic. By default, the local data file is compressed before it is uploaded.
- -dbr: indicates whether to ignore dirty data (such as additional columns, missing columns, and columns with mismatched data types).
    - If this parameter is set to true, all data that does not comply with table definitions is ignored.

- If this parameter is set to false, an error is returned when dirty data is found, so that raw data in the destination table is not contaminated.

- -dfp: specifies the DateTime format. Default value: yyyy-MM-dd HH:mm:ss.
- -fd: specifies the column delimiter used in the local data file. Default value: comma (,).
- -h: indicates whether the data file contains the header. If this parameter is set to true, Dship skips the header row and starts uploading data from the second row.
- -mbr: terminates any attempts to upload more than 1,000 rows of dirty data. This parameter allows you to adjust the maximum allowable volume of dirty data.
- -ni: specifies the NULL data identifier. Default value: an empty string ("").
- -rd: specifies the row delimiter used in the local data file. Default value: \r\n.
- -s: indicates whether to scan the local data file. Default value: false.
    - If this parameter is set to true, the system scans the source data first, and then imports the data if the format is correct.
    - If this parameter is set to false, the system imports data directly without scanning.
    - If this parameter is set to only, the system only scans the source data, and does not import the data after scanning.
- -sd: sets the session directory.
- -te: specifies the Tunnel endpoint.
- -threads: specifies the number of threads. Default value: 1.
- -tz: specifies the time zone. Default value: Asia/Shanghai.

Show

Displays historical records. The following example shows how to use the sub-commands:

```
odps@ project_name>tunnel help show;
usage: tunnel show history [options]
         show session information
 -n,-number <ARG>   lines
Example:
  tunnel show history -n 5
  tunnel show log
```

Parameters:

-n: specifies the number of rows to be displayed.

Resume

Resumes the execution of historical operations (only applicable to data upload). The following example shows how to use the sub-commands:

```
odps@  project_name>tunnel help resume;
usage: tunnel resume [session_id] [-force]
         resume an upload session
 -f,-force   force resume
Example:
  tunnel resume
```

Download

The following example shows how to use the sub-commands:

```
odps@ project_name>tunnel help download;
usage: tunnel download [options] <[project.]table[/partition]> <path>
         download data to local file
 -c,-charset <ARG>            specify file charset, default ignore.
                        set ignore to download raw data
 -ci,-columns-index <ARG>       specify the columns index(starts from
                        0) to download, use comma to split each
                        index
 -cn,-columns-name <ARG>        specify the columns name to download,
                        use comma to split each name
 -cp,-compress <ARG>          compress, default true
 -dfp,-date-format-pattern <ARG>   specify date format pattern, default
                        yyyy-MM-dd HH:mm:ss
 -e,-exponential <ARG>          When download double values, use
                        exponential express if necessary.
                        Otherwise at most 20 digits will be
                        reserved. Default false
 -fd,-field-delimiter <ARG>      specify field delimiter, support
                        unicode, eg \u0001. default ","
 -h,-header <ARG>             if local file should have table header,
                        default false
   -limit <ARG>             specify the number of records to
                        download
 -ni,-null-indicator <ARG>       specify null indicator string, default
                        ""(empty string)
 -rd,-record-delimiter <ARG>      specify record delimiter, support
                        unicode, eg \u0001. default "\r\n"
 -sd,-session-dir <ARG>         set session dir, default
                        D:\software\odpscmd_public\plugins\dshi
                        p
 -te,-tunnel_endpoint <ARG>      tunnel endpoint
   -threads <ARG>            number of threads, default 1
 -tz,-time-zone <ARG>          time zone, default local timezone:
                        Asia/Shanghai
usage: tunnel download [options] instance://<[project/]instance_id> <path>
         download instance result to local file
 -c,-charset <ARG>            specify file charset, default ignore.
                        set ignore to download raw data
 -ci,-columns-index <ARG>       specify the columns index(starts from
                        0) to download, use comma to split each
                        index
 -cn,-columns-name <ARG>        specify the columns name to download,
                        use comma to split each name
 -cp,-compress <ARG>          compress, default true
 -dfp,-date-format-pattern <ARG>   specify date format pattern, default
                        yyyy-MM-dd HH:mm:ss
 -e,-exponential <ARG>          When download double values, use
                        exponential express if necessary.
                        Otherwise at most 20 digits will be
                        reserved. Default false
 -fd,-field-delimiter <ARG>      specify field delimiter, support
```

```
-fd,-field-delimiter <ARG>     specify field delimiter, support
                      unicode, eg \u0001. default ","
-h,-header <ARG>             if local file should have table header,
                      default false
  -limit <ARG>             specify the number of records to
                      download
-ni,-null-indicator <ARG> specify null indicator string, default
                      ""(empty string)
-rd,-record-delimiter <ARG>     specify record delimiter, support
                      unicode, eg \u0001. default "\r\n"
-sd,-session-dir <ARG>        set session dir, default
                      D:\software\odpscmd_public\plugins\dshi
                      p
-te,-tunnel_endpoint <ARG>      tunnel endpoint
  -threads <ARG>            number of threads, default 1
-tz,-time-zone <ARG>          time zone, default local timezone:
                      Asia/Shanghai
Example:
  tunnel download test_project.test_table/p1="b1",p2="b2" log.txt
  tunnel download instance://test_project/test_instance log.txt
```

Parameters:

- -c: specifies the local data file encoding format. Default value: UTF-8.
- -ci: specifies the column index (starting from 0) for downloading. Separate multiple entries with commas (,).
- -cn: specifies the names of columns to be downloaded. Separate multiple entries with commas (,).
- -cp, -compress: indicates whether to compress the data file before it is uploaded to reduce network traffic. By default, a data file is compressed by it is uploaded.
- -dfp: specifies the DateTime format. Default value: yyyy-MM-dd HH:mm:ss.
- -e: allows you to express the values as exponential functions when you download Double type data. If this parameter is not set, a maximum of 20 digits can be retained.
- -fd: specifies the column delimiter used in the local data file. Default value: comma (,).
- -h: indicates whether the data file contains a header. If this parameter is set to true, Dship skips the header row and starts downloading data from the second row.

> Note `-h=true` and `threads>1` cannot be used together.

- -limit: specifies the number of files to be downloaded.
- -ni: specifies the NULL data identifier. Default value: an empty string ("").
- -rd: specifies the row delimiter used in the local data file. Default value: \r\n.
- -sd: sets the session directory.
- -te: specifies the Tunnel endpoint.
- -threads: specifies the number of threads. Default value: 1.
- -tz: specifies the time zone. Default value: Asia/Shanghai.

Purge

Purges the session directory. Sessions from the last three days are purged by default. The following example shows how to use the sub-commands:

```
odps@ project_name>tunnel help purge;
usage: tunnel purge [n]
        force session history to be purged.([n] days before, default
        3 days)
Example:
  tunnel purge 5
```

11.2.2.4. LogView tool

11.2.2.4.1. Before you start

You must confirm the LogView process status before using LogView. If the process status is off, you must start the LogView process.

The procedure for querying the process status and starting the process is as follows:

1. Log on to the Apsara Infrastructure Management Framework console. In the left-side navigation pane, choose **Operations > Cluster Operations**. In the **Cluster** search box, enter odps to search for the expected cluster.
2. Click the cluster in the search result. On the Cluster Details page, click the **Services** tab. In the **Service** search box, search for **odps-service-console**. Click odps-service-console in the search result.
3. After you access the **odps-service-console** service, select **LogView#** on the Service Details page. In the Actions column corresponding to the machine, click **Terminal** to open the TerminalService window.
4. Run the following command to find the Docker container where LogView resides:

   ```
   docker ps|grep logview
   ```

5. Run the following commands to view the LogView process status:

   ```
   ps -aux|grep logview
   ```

   ```
   netstat -ntulp|grep 9000
   ```

6. If the process status is off, run the following command to start the process:

   ```
   /opt/aliyun/app/logview/bin/control start
   ```

The following sections describe what is LogView and how to use LogView to perform basic operations.

11.2.2.4.2. LogView introduction

LogView is a tool for checking and debugging a job submitted to MaxCompute. LogView allows you to check the running details of a job.

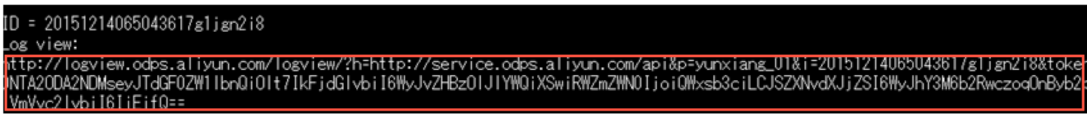
LogView functions

LogView allows you to check the running status, details, and results of a job, and the progress of each phase.

LogView endpoint

Take the odpscmd client as an example. After you submit an SQL task on the client, a long string starting with logview is returned.

A long string starting with logview



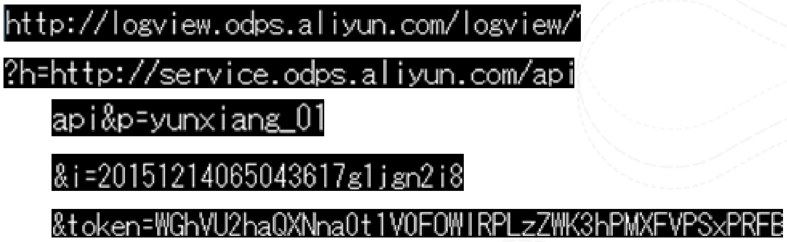
```
ID = 20151214065043617g1jgn2i8
Log view:
http://logview.odps.aliyun.com/logview/?h=http://service.odps.aliyun.com/api&p=yunxiang_01&i=20151214065043617g1jgn2i8&toke
NTA2ODA2NDMseyJTdGF0ZW1lbnQiOlt7IkFjdGlvbiI6WyJvZHBzOlJIYWQiXSwiRWZmZWN0IjoiQWxsb3ciLCJSZXNvdXJjZSI6WyJhY3M6b2RwczoqOnByb2
VmVyc2lvbiI6IjEifQ==
```

Enter the string with all carriage return and line feed characters removed in the address bar of the browser.

Composition of a LogView string

A LogView string consists of five parts, as shown in the following figure.

Composition of a LogView string



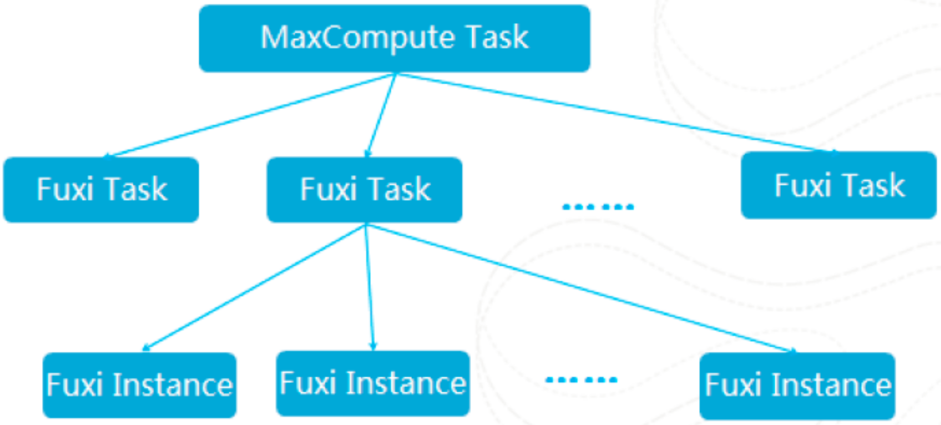
```
http://logview.odps.aliyun.com/logview/`
?h=http://service.odps.aliyun.com/api
    api&p=yunxiang_01
    &i=20151214065043617g1jgn2i8
    &token=WGhVU2haQXNna0t1V0FOWIRPLzZWK3hPMXFVPSxPRFB
```

11.2.2.4.3. Preliminary knowledge of LogView

For complex SQL queries, you must have an in-depth knowledge of the relationships between MaxCompute tasks and Fuxi instances before you can understand LogView.

In short, a MaxCompute task consists of one or more Fuxi jobs. Each Fuxi job consists of one or more Fuxi tasks. Each Fuxi task consists of one or more Fuxi instances.

Relationships between MaxCompute tasks and Fuxi instances

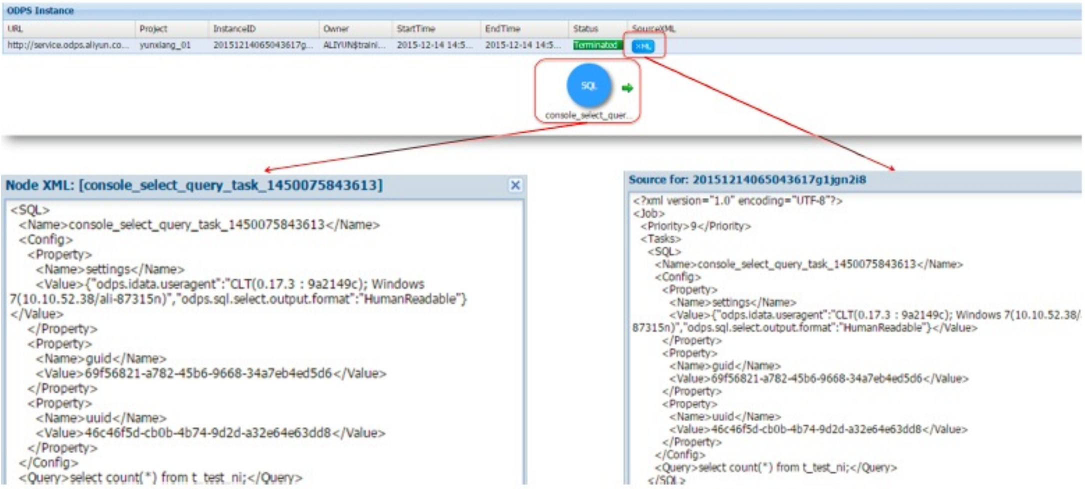


The following figures show the relevant information in LogView.

MaxCompute Instance

MaxCompute Instance

MaxCompute instance



ODPS Instance

URL	Project	InstanceID	Owner	StartTime	EndTime	Status	SourceXML
http://service.odps.aliyun.co...	yunxiang_01	20151214065043617g...	ALIYUN$traini...	2015-12-14 14:5...	2015-12-14 14:5...	Terminated	XML

Node XML: [console_select_query_task_1450075843613]

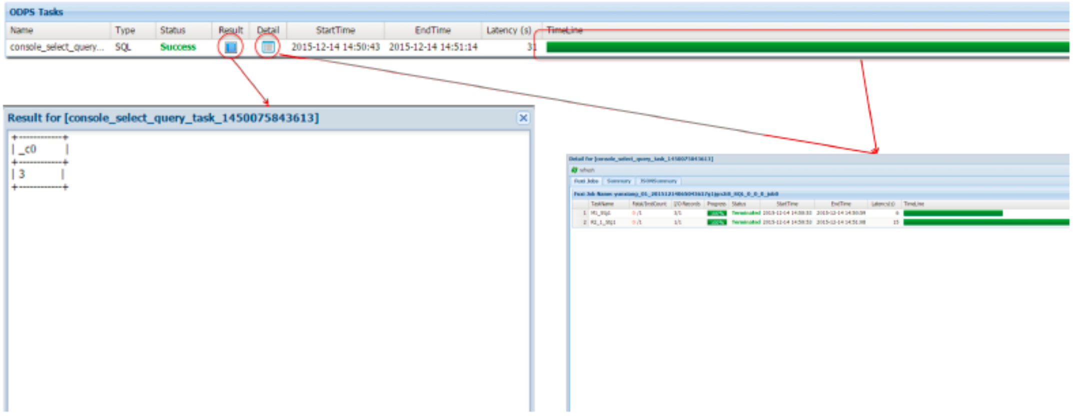
```
<SQL>
  <Name>console_select_query_task_1450075843613</Name>
  <Config>
    <Property>
      <Name>settings</Name>
      <Value>{"odps.idata.useragent":"CLT(0.17.3 : 9a2149c); Windows 
7(10.10.52.38/ali-87315n)","odps.sql.select.output.format":"HumanReadable"}
</Value>
    </Property>
    <Property>
      <Name>guid</Name>
      <Value>69f56821-a782-45b6-9668-34a7eb4ed5d6</Value>
    </Property>
    <Property>
      <Name>uuid</Name>
      <Value>46c46f5d-cb0b-4b74-9d2d-a32e64e63dd8</Value>
    </Property>
  </Config>
  <Query>select count(*) from t_test_ni;</Query>
```

Source for: 20151214065043617g1jgn2i8

```
<?xml version="1.0" encoding="UTF-8"?>
<Job>
  <Priority>9</Priority>
  <Tasks>
    <SQL>
      <Name>console_select_query_task_1450075843613</Name>
      <Config>
        <Property>
          <Name>settings</Name>
          <Value>{"odps.idata.useragent":"CLT(0.17.3 : 9a2149c); Windows 7(10.10.52.38/
87315n)","odps.sql.select.output.format":"HumanReadable"}</Value>
        </Property>
        <Property>
          <Name>guid</Name>
          <Value>69f56821-a782-45b6-9668-34a7eb4ed5d6</Value>
        </Property>
        <Property>
          <Name>uuid</Name>
          <Value>46c46f5d-cb0b-4b74-9d2d-a32e64e63dd8</Value>
        </Property>
      </Config>
      <Query>select count(*) from t_test_ni;</Query>
    </SQL>
```

MaxCompute Task

MaxCompute Task



ODPS Tasks

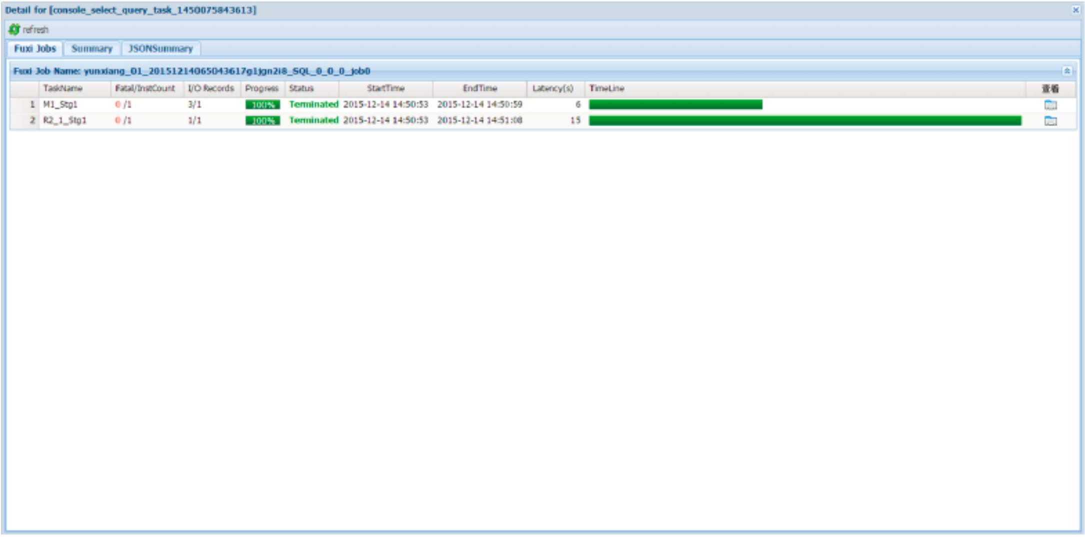
Name	Type	Status	Result	Detail	StartTime	EndTime	Latency (s)	TimeLine
console_select_query...	SQL	Success			2015-12-14 14:50:43	2015-12-14 14:51:14	31	

Result for [console_select_query_task_1450075843613]

```
+------------+
| _c0        |
+------------+
| 3          |
+------------+
```

Task Detail - Fuxi Job

Task Detail - Fuxi Job(1)

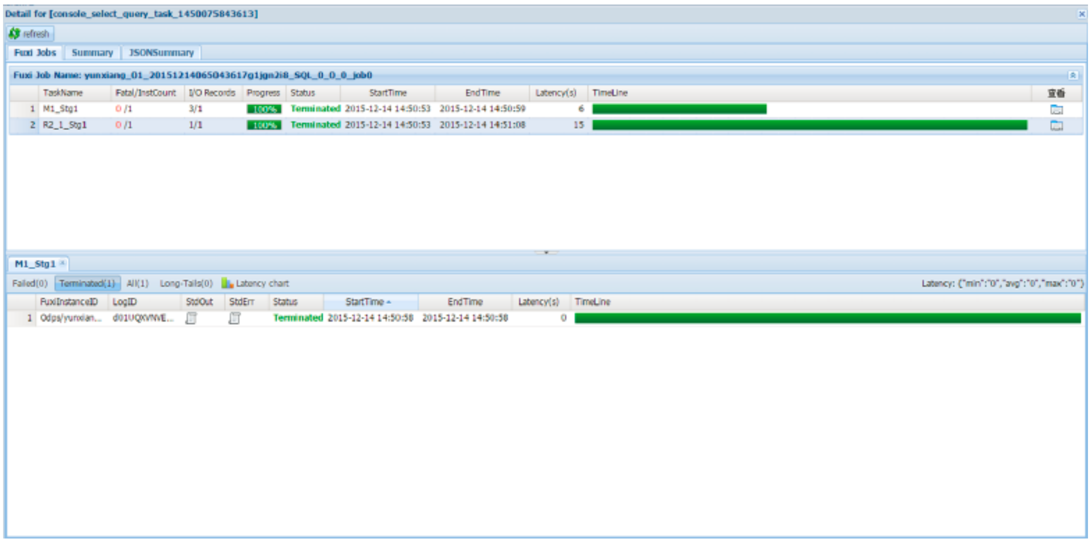


Detail for [console_select_query_task_1450075843613]

Fuxi Job Name: yunxiang_01_20151214065043617g1jgn2i8_SQL_0_0_0_job0

	TaskName	Fatal/InstCount	I/O Records	Progress	Status	StartTime	EndTime	Latency(s)	TimeLine	查看
1	M1_Stg1	0 /1	3/1	100%	Terminated	2015-12-14 14:50:53	2015-12-14 14:50:59	6		
2	R2_1_Stg1	0 /1	1/1	100%	Terminated	2015-12-14 14:50:53	2015-12-14 14:51:08	15		

Task Detail - Fuxi Job(2)



Detail for [console_select_query_task_1450075843613]

Fuxi Job Name: yunxiang_01_20151214065043617g1jgn2i8_SQL_0_0_0_job0

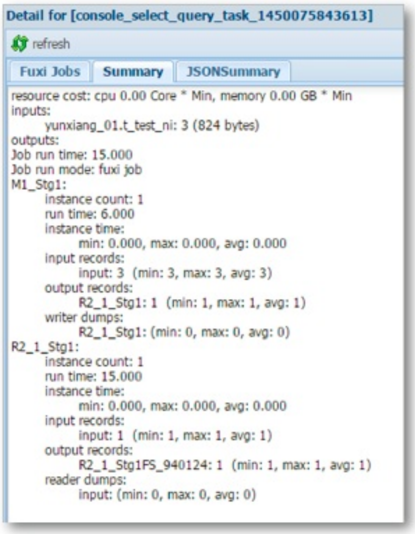
	TaskName	Fatal/InstCount	I/O Records	Progress	Status	StartTime	EndTime	Latency(s)	TimeLine	查看
1	M1_Stg1	0 /1	3/1	100%	Terminated	2015-12-14 14:50:53	2015-12-14 14:50:59	6		
2	R2_1_Stg1	0 /1	1/1	100%	Terminated	2015-12-14 14:50:53	2015-12-14 14:51:08	15		

Latency: {"min":"0","avg":"0","max":"0"}

	FuxiInstanceID	LogID	StdOut	StdErr	Status	StartTime	EndTime	Latency(s)	TimeLine
1	Odps/yunxian...	d01UQXVNVE...			Terminated	2015-12-14 14:50:58	2015-12-14 14:50:58	0	

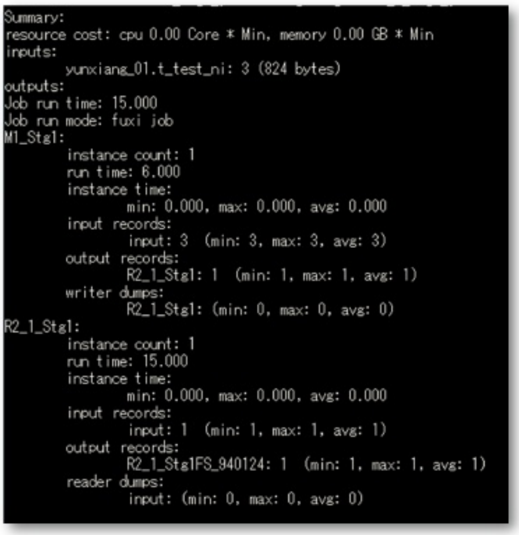
Task Detail - Summary

Task Detail - Summary



Detail for [console_select_query_task_1450075843613]

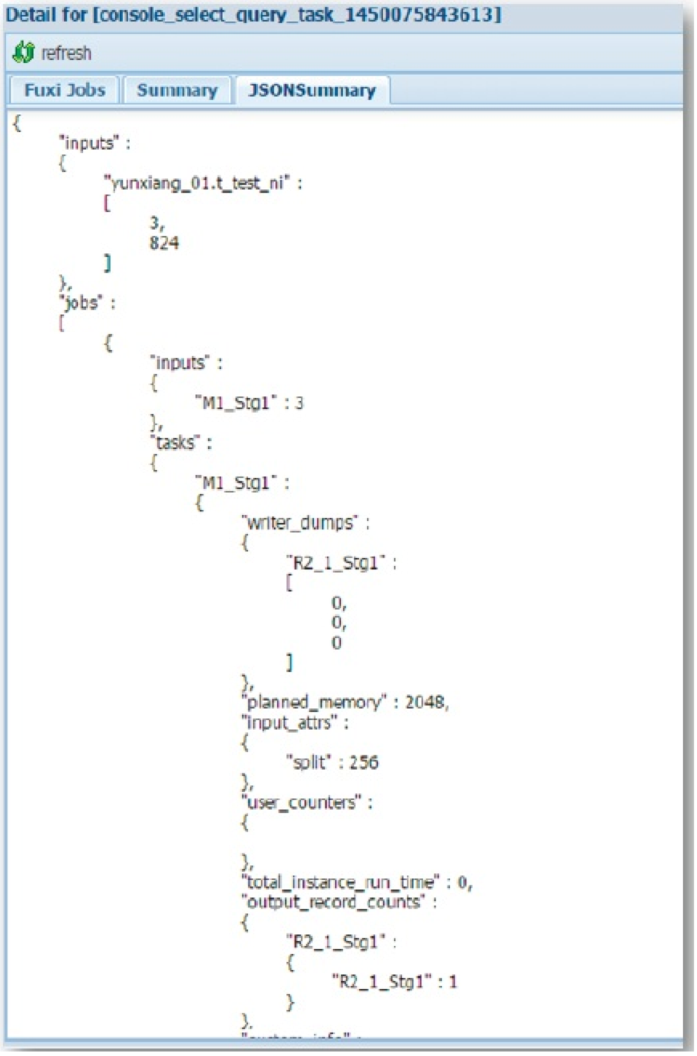
```
resource cost: cpu 0.00 Core * Min, memory 0.00 GB * Min
inputs:
        yunxiang_01.t_test_ni: 3 (824 bytes)
outputs:
Job run time: 15.000
Job run mode: fuxi job
M1_Stg1:
        instance count: 1
        run time: 6.000
        instance time:
                min: 0.000, max: 0.000, avg: 0.000
        input records:
                input: 3  (min: 3, max: 3, avg: 3)
        output records:
                R2_1_Stg1: 1  (min: 1, max: 1, avg: 1)
        writer dumps:
                R2_1_Stg1: (min: 0, max: 0, avg: 0)
R2_1_Stg1:
        instance count: 1
        run time: 15.000
        instance time:
                min: 0.000, max: 0.000, avg: 0.000
        input records:
                input: 1  (min: 1, max: 1, avg: 1)
        output records:
                R2_1_Stg1FS_940124: 1  (min: 1, max: 1, avg: 1)
        reader dumps:
                input: (min: 0, max: 0, avg: 0)
```



```
Summary:
resource cost: cpu 0.00 Core * Min, memory 0.00 GB * Min
inputs:
        yunxiang_01.t_test_ni: 3 (824 bytes)
outputs:
Job run time: 15.000
Job run mode: fuxi job
M1_Stg1:
        instance count: 1
        run time: 6.000
        instance time:
                min: 0.000, max: 0.000, avg: 0.000
        input records:
                input: 3  (min: 3, max: 3, avg: 3)
        output records:
                R2_1_Stg1: 1  (min: 1, max: 1, avg: 1)
        writer dumps:
                R2_1_Stg1: (min: 0, max: 0, avg: 0)
R2_1_Stg1:
        instance count: 1
        run time: 15.000
        instance time:
                min: 0.000, max: 0.000, avg: 0.000
        input records:
                input: 1  (min: 1, max: 1, avg: 1)
        output records:
                R2_1_Stg1FS_940124: 1  (min: 1, max: 1, avg: 1)
        reader dumps:
                input: (min: 0, max: 0, avg: 0)
```

Task Detail - JSONSummary

Task Detail - JSONSummary



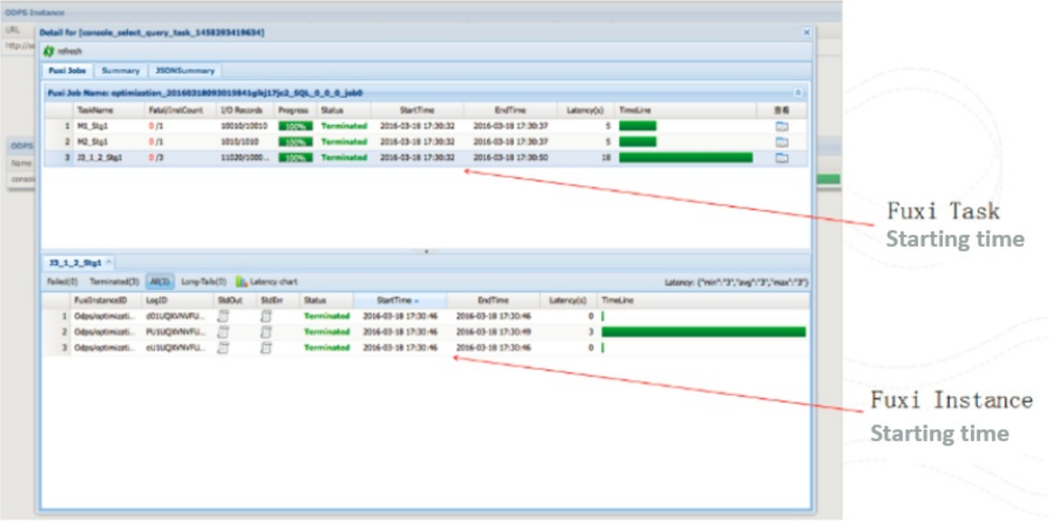
Detail for [console_select_query_task_1450075843613]

```
{
        "inputs" :
        {
                "yunxiang_01.t_test_ni" :
                [
                        3,
                        824
                ]
        },
        "jobs" :
        [
                {
                        "inputs" :
                        {
                                "M1_Stg1" : 3
                        },
                        "tasks" :
                        {
                                "M1_Stg1" :
                                {
                                        "writer_dumps" :
                                        {
                                                "R2_1_Stg1" :
                                                [
                                                        0,
                                                        0,
                                                        0
                                                ]
                                        },
                                        "planned_memory" : 2048,
                                        "input_attrs" :
                                        {
                                                "split" : 256
                                        },
                                        "user_counters" :
                                        {

                                        },
                                        "total_instance_run_time" : 0,
                                        "output_record_counts" :
                                        {
                                                "R2_1_Stg1" :
                                                {
                                                        "R2_1_Stg1" : 1
                                                }
                                        },
                                        "custom_info" :
```

11.2.2.4.4. Basic operations and examples

View each point in time in the life cycle of a job.

View each point in time in the life cycle of a job



Detail for [console_select_query_task_1458293419634]

Fuxi Job Name: optimization_20160318093019841g9kj17jc2_SQL_0_0_0_job0

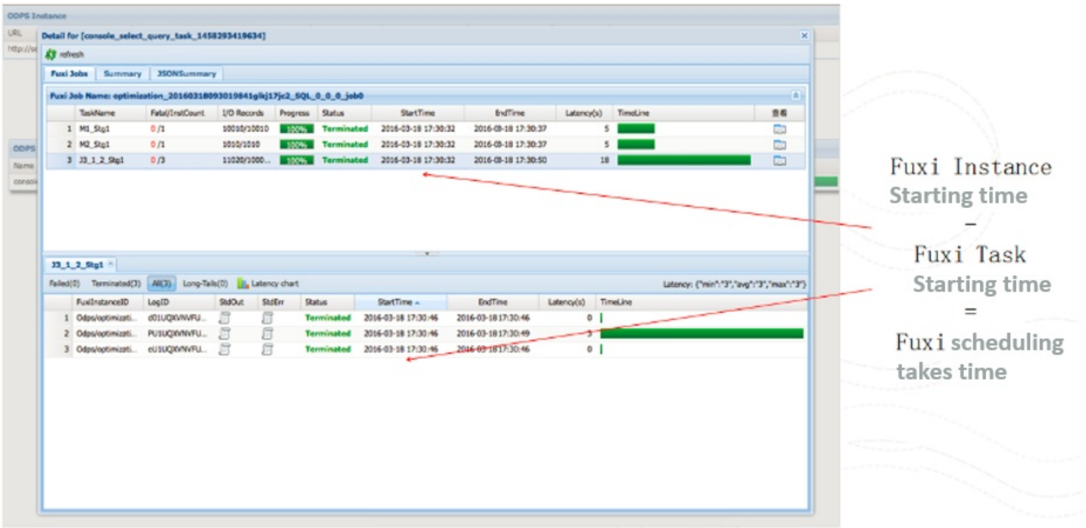
	TaskName	Fatal/InstCount	I/O Records	Progress	Status	StartTime	EndTime	Latency(s)	TimeLine	
1	M1_Stg1	0 /1	10010/10010	100%	Terminated	2016-03-18 17:30:32	2016-03-18 17:30:37	5		
2	M2_Stg1	0 /1	1010/1010	100%	Terminated	2016-03-18 17:30:32	2016-03-18 17:30:37	5		
3	J3_1_2_Stg1	0 /3	11020/1000...	100%	Terminated	2016-03-18 17:30:32	2016-03-18 17:30:50	18		

Latency: {"min":"3","avg":"3","max":"3"}

	FuxiInstanceID	LogID	StdOut	StdErr	Status	StartTime	EndTime	Latency(s)	TimeLine
1	Odps/optimizati...	d01UQXVNVFU...			Terminated	2016-03-18 17:30:46	2016-03-18 17:30:46	0	
2	Odps/optimizati...	PU1UQXVNVFU...			Terminated	2016-03-18 17:30:46	2016-03-18 17:30:49	3	
3	Odps/optimizati...	eU1UQXVNVFU...			Terminated	2016-03-18 17:30:46	2016-03-18 17:30:46	0	

View the time it takes for Job Scheduler to schedule an instance.

View the time it takes for Job Scheduler to schedule an instance



Detail for [console_select_query_task_1458293419634]

Fuxi Job Name: optimization_20160318093019841glkj17jc2_SQL_0_0_0_job0

	TaskName	Fatal/InstCount	I/O Records	Progress	Status	StartTime	EndTime	Latency(s)	TimeLine	查看
1	M1_Stg1	0 /1	10010/10010	100%	Terminated	2016-03-18 17:30:32	2016-03-18 17:30:37	5		
2	M2_Stg1	0 /1	1010/1010	100%	Terminated	2016-03-18 17:30:32	2016-03-18 17:30:37	5		
3	J3_1_2_Stg1	0 /3	11020/1000...	100%	Terminated	2016-03-18 17:30:32	2016-03-18 17:30:50	18		

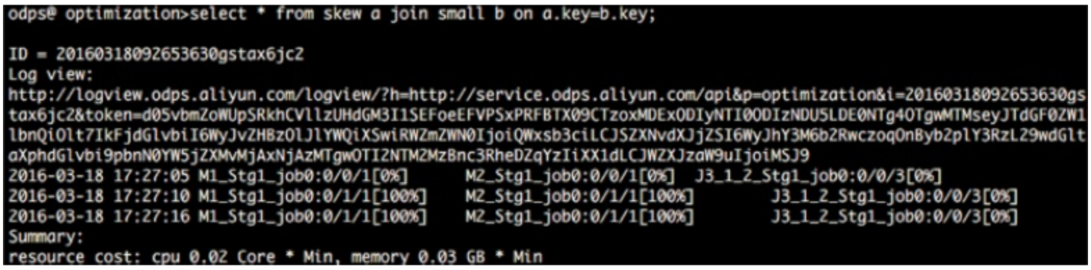
Latency: {"min":"3","avg":"3","max":"3"}

	FuxiInstanceID	LogID	StdOut	StdErr	Status	StartTime	EndTime	Latency(s)	TimeLine
1	Odps/optimizati...	d01UQXVNVFU...			Terminated	2016-03-18 17:30:46	2016-03-18 17:30:46	0	
2	Odps/optimizati...	PU1UQXVNVFU...			Terminated	2016-03-18 17:30:46	2016-03-18 17:30:49	3	
3	Odps/optimizati...	eU1UQXVNVFU...			Terminated	2016-03-18 17:30:46	2016-03-18 17:30:46	0	

Fuxi Instance Starting time
−
Fuxi Task Starting time
=
Fuxi scheduling takes time

View the polling interval.

View the polling interval

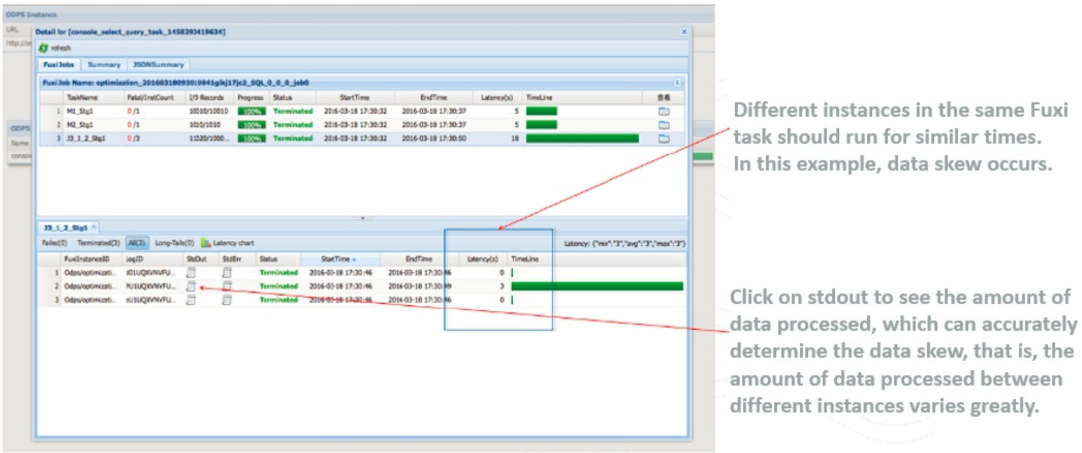


```
odps@ optimization>select * from skew a join small b on a.key=b.key;

ID = 20160318092653630gstax6jc2
Log view:
http://logview.odps.aliyun.com/logview/?h=http://service.odps.aliyun.com/api&p=optimization&i=20160318092653630gs
tax6jc2&token=d05vbmZoWUpSRkhCVllzUHdGM3I1SEFoeEFVPSxPRFBTX09CTzoxMDExODIyNTI0ODIzNDU5LDE0NTg4OTgwMTMseyJTdGF0ZW1
lbnQiOlt7IkFjdGlvbiI6WyJvZHBzOlJlYWQiXSwiRWZmZWN0IjoiQWxsb3ciLCJSZXNvdXJjZSI6WyJhY3M6b2RwczoqOnByb2plY3RzL29wdGlt
aXphdGlvbi9pbnN0YW5jZXMvMjAxNjAzMTgwOTI2NTM2MzBnc3RheDZqYzIiXX1dLCJWZXJzaW9uIjoiMSJ9
2016-03-18 17:27:05 M1_Stg1_job0:0/0/1[0%]     M2_Stg1_job0:0/0/1[0%]  J3_1_2_Stg1_job0:0/0/3[0%]
2016-03-18 17:27:10 M1_Stg1_job0:0/1/1[100%]   M2_Stg1_job0:0/1/1[100%]        J3_1_2_Stg1_job0:0/0/3[0%]
2016-03-18 17:27:16 M1_Stg1_job0:0/1/1[100%]   M2_Stg1_job0:0/1/1[100%]        J3_1_2_Stg1_job0:0/0/3[0%]
Summary:
resource cost: cpu 0.02 Core * Min, memory 0.03 GB * Min
```

After a MaxCompute instance is submitted, odpscmd polls the execution status of the job at a specified interval of approximately 5s.

Check for data skews

Check for data skews



Detail for [console_select_query_task_1458293419634]

Fuxi Job Name: optimization_20160318093019841glkj17jc2_SQL_0_0_0_job0

	TaskName	Fatal/InstCount	I/O Records	Progress	Status	StartTime	EndTime	Latency(s)	TimeLine	查看
1	M1_Stg1	0 /1	10010/10010	100%	Terminated	2016-03-18 17:30:32	2016-03-18 17:30:37	5		
2	M2_Stg1	0 /1	1010/1010	100%	Terminated	2016-03-18 17:30:32	2016-03-18 17:30:37	5		
3	J3_1_2_Stg1	0 /3	11020/1000...	100%	Terminated	2016-03-18 17:30:32	2016-03-18 17:30:50	18		

Latency: {"min":"3","avg":"3","max":"3"}

	FuxiInstanceID	LogID	StdOut	StdErr	Status	StartTime	EndTime	Latency(s)	TimeLine
1	Odps/optimizati...	d01UQXVNVFU...			Terminated	2016-03-18 17:30:46	2016-03-18 17:30:46	0	
2	Odps/optimizati...	PU1UQXVNVFU...			Terminated	2016-03-18 17:30:46	2016-03-18 17:30:49	3	
3	Odps/optimizati...	eU1UQXVNVFU...			Terminated	2016-03-18 17:30:46	2016-03-18 17:30:46	0	

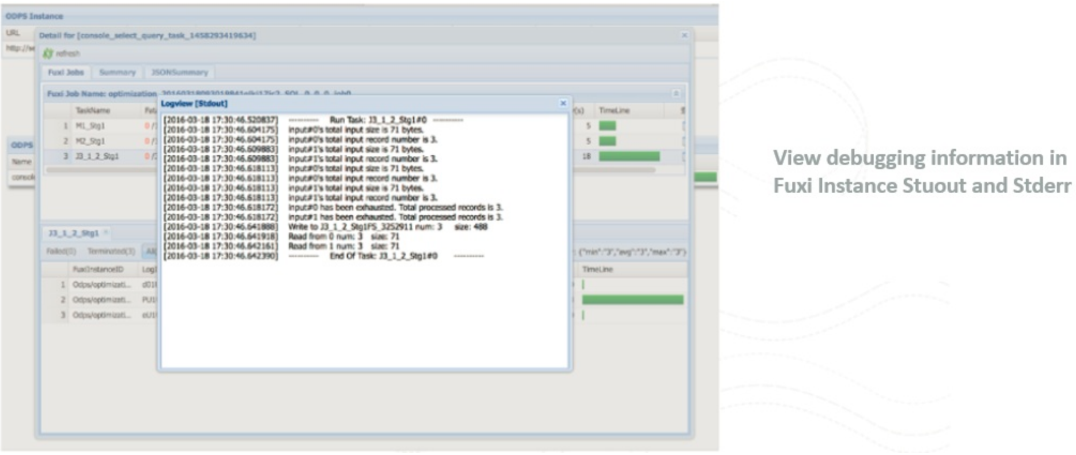
Different instances in the same Fuxi task should run for similar times. In this example, data skew occurs.

Click on stdout to see the amount of data processed, which can accurately determine the data skew, that is, the amount of data processed between different instances varies greatly.

View the UDF and MR debugging information

View the UDF and MR debugging information

View the UDF and MR debugging information

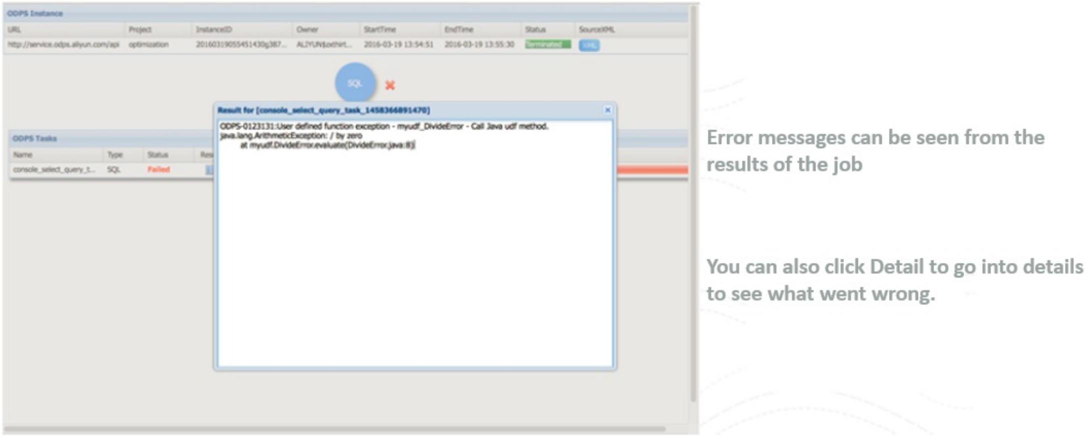

Logview [Stdout]

```
[2016-03-18 17:30:46.520837]    ---------    Run Task: J3_1_2_Stg1#0   ---------
[2016-03-18 17:30:46.604175]    input#0's total input size is 71 bytes.
[2016-03-18 17:30:46.604175]    input#0's total input record number is 3.
[2016-03-18 17:30:46.609883]    input#1's total input size is 71 bytes.
[2016-03-18 17:30:46.609883]    input#1's total input record number is 3.
[2016-03-18 17:30:46.618113]    input#0's total input size is 71 bytes.
[2016-03-18 17:30:46.618113]    input#0's total input record number is 3.
[2016-03-18 17:30:46.618113]    input#1's total input size is 71 bytes.
[2016-03-18 17:30:46.618113]    input#1's total input record number is 3.
[2016-03-18 17:30:46.618172]    input#0 has been exhausted. Total processed records is 3.
[2016-03-18 17:30:46.618172]    input#1 has been exhausted. Total processed records is 3.
[2016-03-18 17:30:46.641888]    Write to J3_1_2_Stg1FS_3252911 num: 3    size: 488
[2016-03-18 17:30:46.641918]    Read from 0 num: 3    size: 71
[2016-03-18 17:30:46.642161]    Read from 1 num: 3    size: 71
[2016-03-18 17:30:46.642390]    ---------    End Of Task: J3_1_2_Stg1#0    ---------
```

View debugging information in Fuxi Instance Stuout and Stderr

View the task status - Terminated

View the task status - Terminated



URL	Project	InstanceID	Owner	StartTime	EndTime	Status	SourceXML
http://service.odps.aliyun.com/api	optimization	20160319055451430g387...	ALIYUN$odhirt...	2016-03-19 13:54:51	2016-03-19 13:55:30	Terminated	XML

Name	Type	Status
console_select_query_t...	SQL	Failed

Result for [console_select_query_task_1458366891470]

```
ODPS-0123131:User defined function exception - myudf_DivideError - Call Java udf method.
java.lang.ArithmeticException: / by zero
        at myudf.DivideError.evaluate(DivideError.java:8)
```

Error messages can be seen from the results of the job

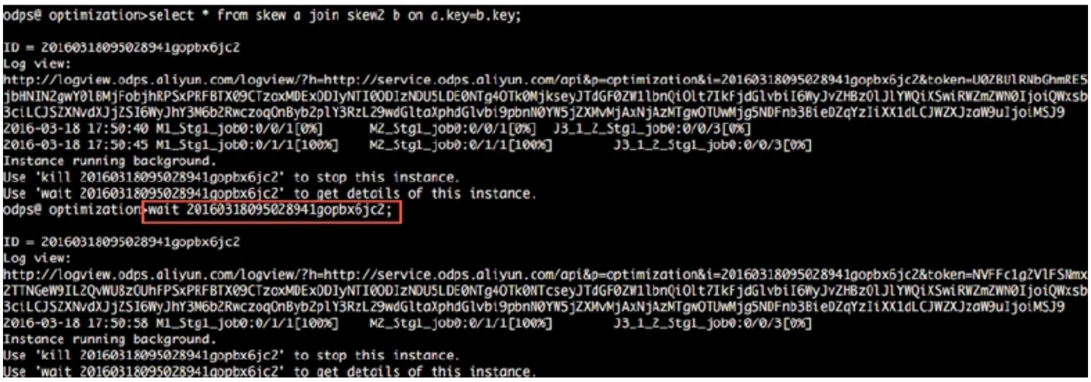
You can also click Detail to go into details to see what went wrong.

11.2.2.4.5. Best practices

Locate LogView based on the instance ID

After you submit a job, you can press Ctrl+C to return to odpscmd and perform other operations. You can run the `wait <instanceid>;` command to locate LogView and obtain the job status.

Locate LogView based on the instance ID

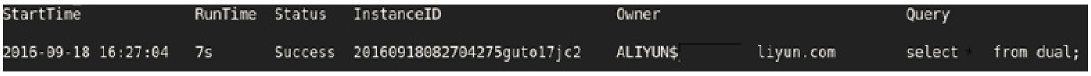


```
odps@ optimization>select * from skew a join skew2 b on a.key=b.key;

ID = 20160318095028941gopbx6jc2
Log view:
http://logview.odps.aliyun.com/logview/?h=http://service.odps.aliyun.com/api&p=optimization&i=20160318095028941gopbx6jc2&token=U0ZBUlRNbGhmRES
jbHNIN2gwY0lBMjFobjhRPSxPRFBTX09CTzoxMDExODIyNTI0ODIzNDU5LDE0NTg4OTk0NjkseyJTdGF0ZW1lbnQiOlt7IkFjdGlvbiI6WyJvZHBzOlJlYWQiXSwiRWZmZWN0IjoiQWxsb
3ciLCJSZXNvdXJjZSI6WyJhY3M6b2RwczoqOnByb2plY3RzL29wdGltaXphdGlvbi9pbnN0YW5jZXMvMjAxNjAzMTgwOTUwMjg5NDFnb3BieDZqYzIiXX1dLCJWZXJzaW9uIjoiMSJ9
2016-03-18 17:50:40 M1_Stg1_job0:0/0/1[0%]      M2_Stg1_job0:0/0/1[0%]  J3_1_2_Stg1_job0:0/0/3[0%]
2016-03-18 17:50:45 M1_Stg1_job0:0/1/1[100%]    M2_Stg1_job0:0/1/1[100%]        J3_1_2_Stg1_job0:0/0/3[0%]
Instance running background.
Use 'kill 20160318095028941gopbx6jc2' to stop this instance.
Use 'wait 20160318095028941gopbx6jc2' to get details of this instance.
odps@ optimization>wait 20160318095028941gopbx6jc2;

ID = 20160318095028941gopbx6jc2
Log view:
http://logview.odps.aliyun.com/logview/?h=http://service.odps.aliyun.com/api&p=optimization&i=20160318095028941gopbx6jc2&token=NVFFc1gZVlFSNmx
ZTTNGeW9IL2QvWU8zOUhFPSxPRFBTX09CTzoxMDExODIyNTI0ODIzNDU5LDE0NTg4OTk0NTcseyJTdGF0ZW1lbnQiOlt7IkFjdGlvbiI6WyJvZHBzOlJlYWQiXSwiRWZmZWN0IjoiQWxsb
3ciLCJSZXNvdXJjZSI6WyJhY3M6b2RwczoqOnByb2plY3RzL29wdGltaXphdGlvbi9pbnN0YW5jZXMvMjAxNjAzMTgwOTUwMjg5NDFnb3BieDZqYzIiXX1dLCJWZXJzaW9uIjoiMSJ9
2016-03-18 17:50:58 M1_Stg1_job0:0/1/1[100%]    M2_Stg1_job0:0/1/1[100%]        J3_1_2_Stg1_job0:0/0/3[0%]
Instance running background.
Use 'kill 20160318095028941gopbx6jc2' to stop this instance.
Use 'wait 20160318095028941gopbx6jc2' to get details of this instance.
```

Locate running tasks

After you exit the control window, you can run the `show p;` command to locate currently running tasks and historical tasks.

Locate running tasks



```
StartTime            RunTime  Status   InstanceID                   Owner                          Query
2016-09-18 16:27:04  7s       Success  20160918082704275guto17jc2   ALIYUN$[redacted]liyun.com     select *  from dual;
```

11.2.2.5. Apsara Big Data Manager

Apsara Big Data Manager (ABM) supports O&M on big data services from the perspectives of business, services, clusters, and hosts. You can also update big data services, customize alert configurations, and view the O&M history in the ABM console.

On-site Apsara Stack engineers can use ABM to easily manage big data services by performing actions, such as viewing resource usage, checking and handling alerts, and modifying configurations.

For more information about how to log on to the ABM console and perform O&M operations in the console, see *MaxCompute O&M*.

11.2.3. Routine O&M

11.2.3.1. Configurations

MaxCompute configurations are stored in the */apsara/odps_service/deploy/env.cfg* directory in odpsag. The configuration file contains the following content:

```
odps_worker_num=3
executor_worker_num=3
hiveserver_worker_num=3
replication_server_num=3
messager_partition_num=3
```

You can modify these parameter values based on your requirements and start the corresponding MaxCompute services based on the configured values. For more information, see *Restart a MaxCompute service*.

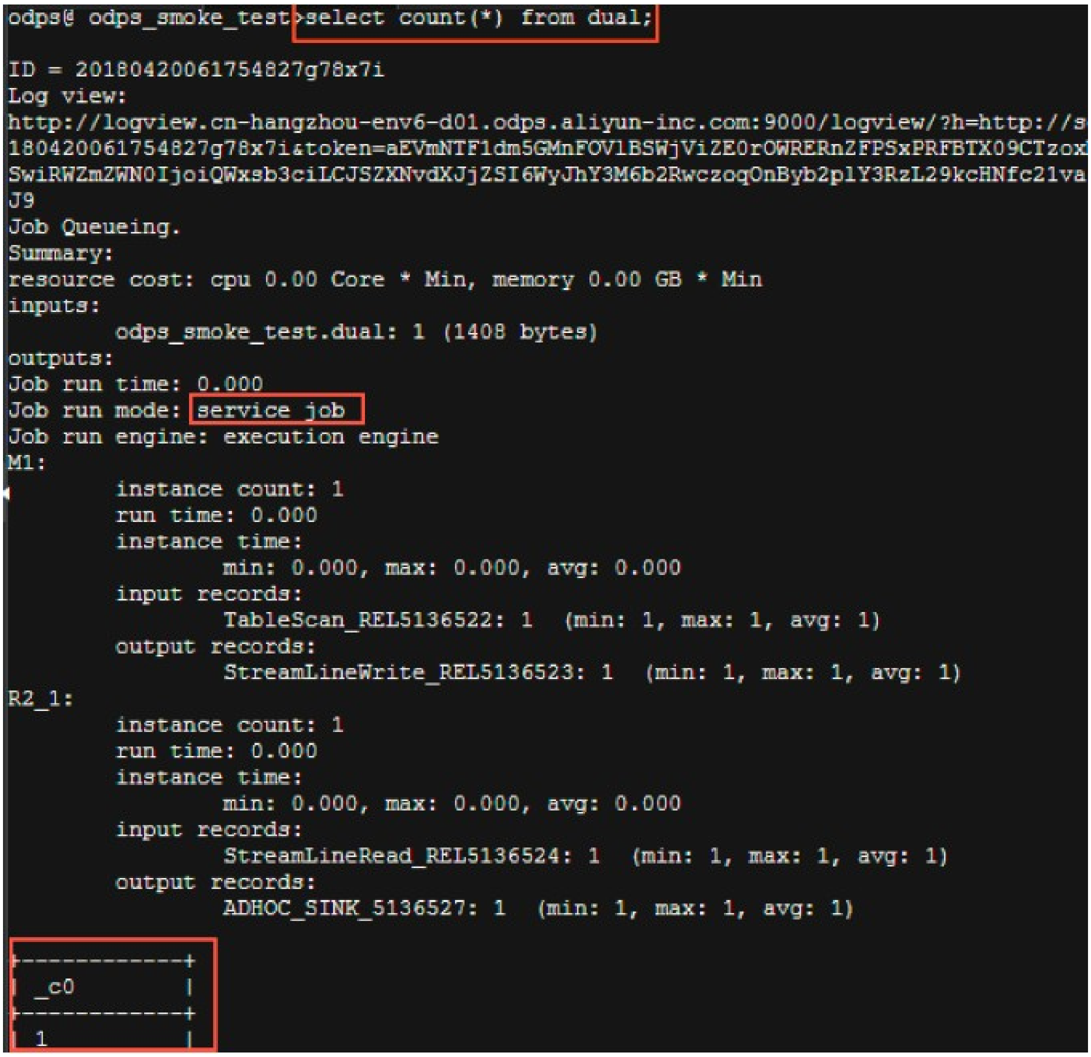
If you add `xstream_max_worker_num=3` at the end of the configuration file, XStream will be started with three running workers.

11.2.3.2. Routine inspections

1. On the Cluster Operations page in Apsara Infrastructure Management Framework, check whether all machines have reached the desired state.
    i. Log on to the Apsara Infrastructure Management Framework console. In the left-side navigation pane, choose **Operations > Cluster Operations**. In the **Cluster** search box, enter odps and click the search icon to search for the expected cluster.
    ii. Check whether all machines have reached the desired state based on the information in the Status, Machine Status, and Server Role Status columns. The following figure shows that some machines have not reached the desired state.
    iii. Click the exceptions in the Machine Status and Server Role status columns to view the exception details.

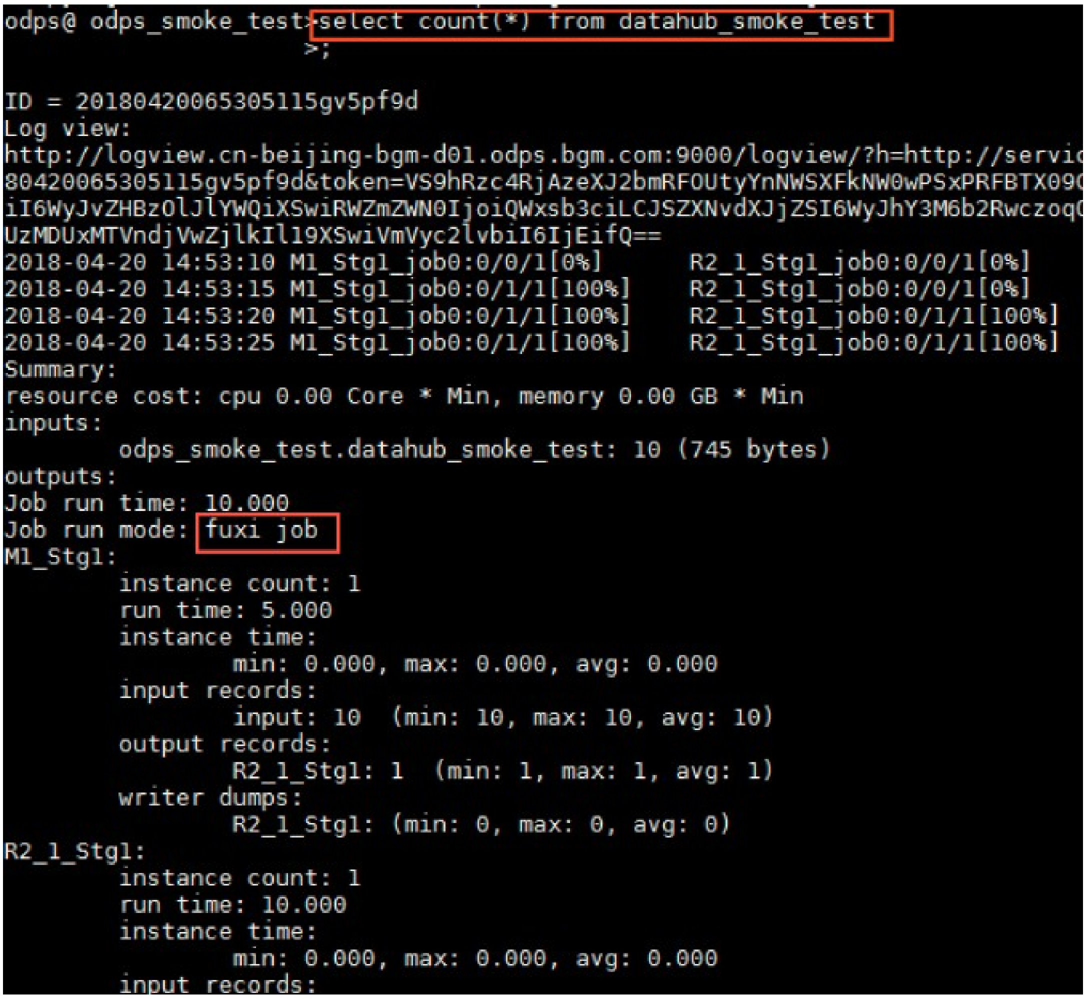
2. Go to the */home/admin/odps/odps_tools/clt/bin/odpscmd -e* directory and run the following command:

   ```
   select count(*) from datahub_smoke_test;
   ```

   ```
   odps@ odps_smoke_test>select count(*) from dual;

   ID = 20180420061754827g78x7i
   Log view:
   http://logview.cn-hangzhou-env6-d01.odps.aliyun-inc.com:9000/logview/?h=http://s
   180420061754827g78x7i&token=aEVmNTF1dm5GMnFOV1BSWjViZE0rOWRERnZFPSxPRFBTX09CTzox
   SwiRWZmZWN0IjoiQWxsb3ciLCJSZXNvdXJjZSI6WyJhY3M6b2RwczoqOnByb2plY3RzL29kcHNfc21va
   J9
   Job Queueing.
   Summary:
   resource cost: cpu 0.00 Core * Min, memory 0.00 GB * Min
   inputs:
           odps_smoke_test.dual: 1 (1408 bytes)
   outputs:
   Job run time: 0.000
   Job run mode: service job
   Job run engine: execution engine
   M1:
           instance count: 1
           run time: 0.000
           instance time:
                   min: 0.000, max: 0.000, avg: 0.000
           input records:
                   TableScan_REL5136522: 1  (min: 1, max: 1, avg: 1)
           output records:
                   StreamLineWrite_REL5136523: 1  (min: 1, max: 1, avg: 1)
   R2_1:
           instance count: 1
           run time: 0.000
           instance time:
                   min: 0.000, max: 0.000, avg: 0.000
           input records:
                   StreamLineRead_REL5136524: 1  (min: 1, max: 1, avg: 1)
           output records:
                   ADHOC_SINK_5136527: 1  (min: 1, max: 1, avg: 1)

   +------------+
   | _c0        |
   +------------+
   | 1          |
   ```

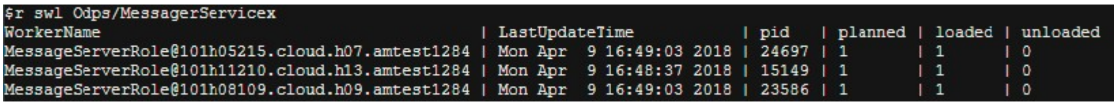
   The following figure shows that fuxi job is running. The command output indicates that fuxi job functions properly.



```
odps@ odps_smoke_test>select count(*) from datahub_smoke_test
                     >;

ID = 20180420065305115gv5pf9d
Log view:
http://logview.cn-beijing-bgm-d01.odps.bgm.com:9000/logview/?h=http://servic
80420065305115gv5pf9d&token=VS9hRzc4RjAzeXJ2bmRFOUtyYnNWSXFkNW0wPSxPRFBTX09C
iI6WyJvZHBzOlJlYWQiXSwiRWZmZWN0IjoiQWxsb3ciLCJSZXNvdXJjZSI6WyJhY3M6b2RwczoqC
UzMDUxMTVndjVwZjlkIl19XSwiVmVyc2lvbiI6IjEifQ==
2018-04-20 14:53:10 M1_Stg1_job0:0/0/1[0%]      R2_1_Stg1_job0:0/0/1[0%]
2018-04-20 14:53:15 M1_Stg1_job0:0/1/1[100%]    R2_1_Stg1_job0:0/0/1[0%]
2018-04-20 14:53:20 M1_Stg1_job0:0/1/1[100%]    R2_1_Stg1_job0:0/1/1[100%]
2018-04-20 14:53:25 M1_Stg1_job0:0/1/1[100%]    R2_1_Stg1_job0:0/1/1[100%]
Summary:
resource cost: cpu 0.00 Core * Min, memory 0.00 GB * Min
inputs:
        odps_smoke_test.datahub_smoke_test: 10 (745 bytes)
outputs:
Job run time: 10.000
Job run mode: fuxi job
M1_Stg1:
        instance count: 1
        run time: 5.000
        instance time:
                min: 0.000, max: 0.000, avg: 0.000
        input records:
                input: 10  (min: 10, max: 10, avg: 10)
        output records:
                R2_1_Stg1: 1  (min: 1, max: 1, avg: 1)
        writer dumps:
                R2_1_Stg1: (min: 0, max: 0, avg: 0)
R2_1_Stg1:
        instance count: 1
        run time: 10.000
        instance time:
                min: 0.000, max: 0.000, avg: 0.000
        input records:
```

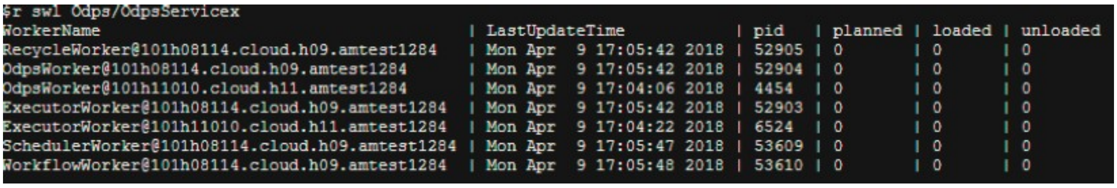
3. Run the following commands to check whether the following workers exist and whether they have been restarted recently:

   i. `r swl Odps/MessagerServicex`



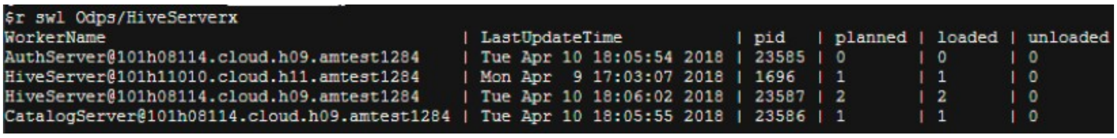
```
$r swl Odps/MessagerServicex
WorkerName                                 | LastUpdateTime           | pid   | planned | loaded | unloaded
MessageServerRole@101h05215.cloud.h07.amtest1284 | Mon Apr  9 16:49:03 2018 | 24697 | 1       | 1      | 0
MessageServerRole@101h11210.cloud.h13.amtest1284 | Mon Apr  9 16:48:37 2018 | 15149 | 1       | 1      | 0
MessageServerRole@101h08109.cloud.h09.amtest1284 | Mon Apr  9 16:49:03 2018 | 23586 | 1       | 1      | 0
```

   ii. `r swl Odps/OdpsServicex`



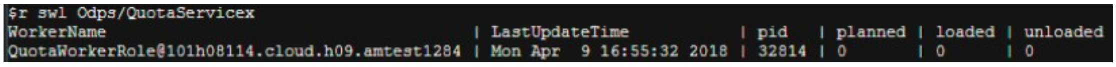
```
$r swl Odps/OdpsServicex
WorkerName                                  | LastUpdateTime           | pid   | planned | loaded | unloaded
RecycleWorker@101h08114.cloud.h09.amtest1284   | Mon Apr  9 17:05:42 2018 | 52905 | 0       | 0      | 0
OdpsWorker@101h08114.cloud.h09.amtest1284      | Mon Apr  9 17:05:42 2018 | 52904 | 0       | 0      | 0
OdpsWorker@101h11010.cloud.h11.amtest1284      | Mon Apr  9 17:04:06 2018 | 4454  | 0       | 0      | 0
ExecutorWorker@101h08114.cloud.h09.amtest1284  | Mon Apr  9 17:05:42 2018 | 52903 | 0       | 0      | 0
ExecutorWorker@101h11010.cloud.h11.amtest1284  | Mon Apr  9 17:04:22 2018 | 6524  | 0       | 0      | 0
SchedulerWorker@101h08114.cloud.h09.amtest1284 | Mon Apr  9 17:05:47 2018 | 53609 | 0       | 0      | 0
WorkflowWorker@101h08114.cloud.h09.amtest1284  | Mon Apr  9 17:05:48 2018 | 53610 | 0       | 0      | 0
```

   iii. `r swl Odps/HiveServerx`



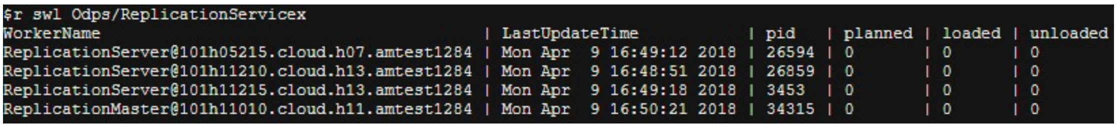
```
$r swl Odps/HiveServerx
WorkerName                                   | LastUpdateTime           | pid   | planned | loaded | unloaded
AuthServer@101h08114.cloud.h09.amtest1284      | Tue Apr 10 18:05:54 2018 | 23585 | 0       | 0      | 0
HiveServer@101h11010.cloud.h11.amtest1284      | Mon Apr  9 17:03:07 2018 | 1696  | 1       | 1      | 0
HiveServer@101h08114.cloud.h09.amtest1284      | Tue Apr 10 18:06:02 2018 | 23587 | 2       | 2      | 0
CatalogServer@101h08114.cloud.h09.amtest1284 | Tue Apr 10 18:05:55 2018 | 23586 | 1       | 1      | 0
```

   iv. `r swl Odps/QuotaServicex`



```
$r swl Odps/QuotaServicex
WorkerName                                   | LastUpdateTime           | pid   | planned | loaded | unloaded
QuotaWorkerRole@101h08114.cloud.h09.amtest1284 | Mon Apr  9 16:55:32 2018 | 32814 | 0       | 0      | 0
```

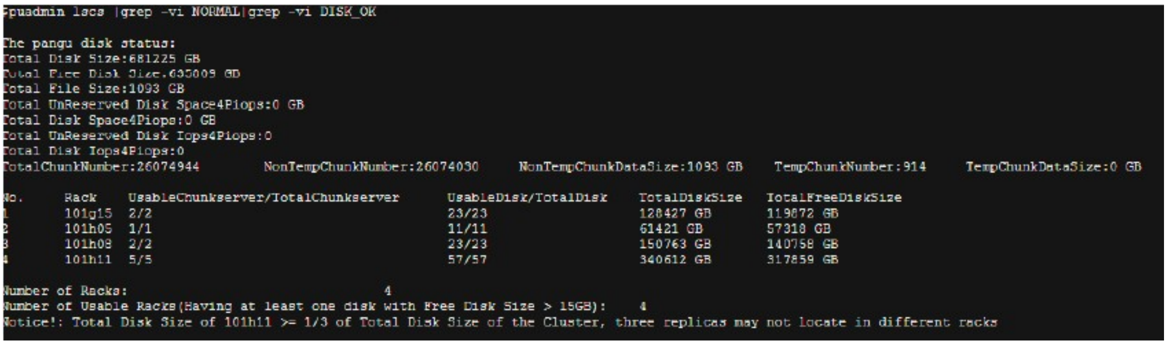
v. `r swl Odps/ReplicationServicex`



```
$r swl Odps/ReplicationServicex
WorkerName                                  | LastUpdateTime            | pid   | planned | loaded | unloaded
ReplicationServer@101h05215.cloud.h07.amtest1284 | Mon Apr  9 16:49:12 2018 | 26594 | 0       | 0      | 0
ReplicationServer@101h11210.cloud.h13.amtest1284 | Mon Apr  9 16:48:51 2018 | 26859 | 0       | 0      | 0
ReplicationServer@101h11215.cloud.h13.amtest1284 | Mon Apr  9 16:49:18 2018 | 3453  | 0       | 0      | 0
ReplicationMaster@101h11010.cloud.h11.amtest1284 | Mon Apr  9 16:50:21 2018 | 34315 | 0       | 0      | 0
```

4. Run the following command to check for errors:

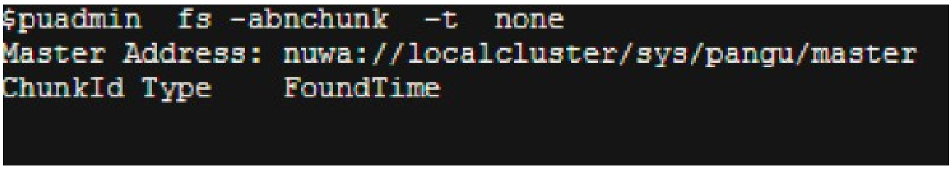
```
puadmin lscs |grep -vi NORMAL|grep -vi DISK_OK
```



```
$puadmin lscs |grep -vi NORMAL|grep -vi DISK_OK

The pangu disk status:
Total Disk Size:681225 GB
Total Free Disk Size:635009 GB
Total File Size:1093 GB
Total UnReserved Disk Space4Piops:0 GB
Total Disk Space4Piops:0 GB
Total UnReserved Disk Iops4Piops:0
Total Disk Iops4Piops:0
TotalChunkNumber:26074944        NonTempChunkNumber:26074030      NonTempChunkDataSize:1093 GB    TempChunkNumber:914      TempChunkDataSize:0 GB

No.     Rack     UsableChunkserver/TotalChunkserver      UsableDisk/TotalDisk     TotalDiskSize    TotalFreeDiskSize
1       101g15   2/2                                     23/23                    128427 GB        119872 GB
2       101h05   1/1                                     11/11                    61421 GB         57318 GB
3       101h08   2/2                                     23/23                    150763 GB        140758 GB
4       101h11   5/5                                     57/57                    340612 GB        317859 GB

Number of Racks:                                4
Number of Usable Racks(Having at least one disk with Free Disk Size > 15GB):     4
Notice!: Total Disk Size of 101h11 >= 1/3 of Total Disk Size of the Cluster, three replicas may not locate in different racks
```

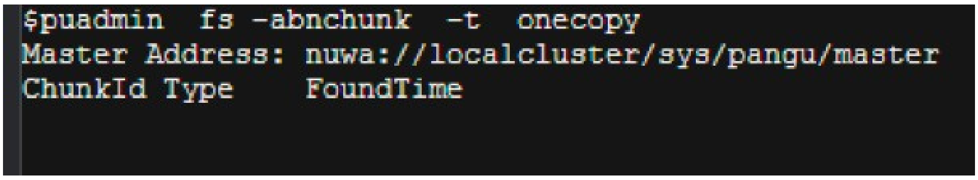
5. Run the following commands to check data integrity:

i. `puadmin fs -abnchunk -t none`



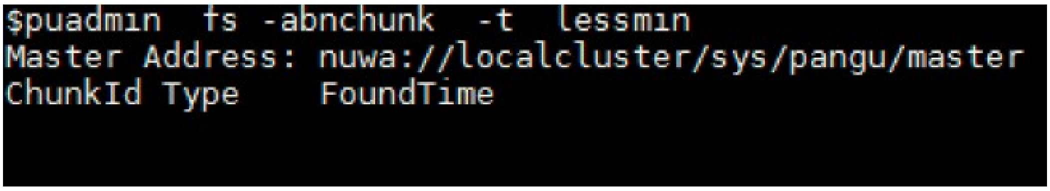
```
$puadmin  fs -abnchunk  -t  none
Master Address: nuwa://localcluster/sys/pangu/master
ChunkId Type     FoundTime
```

ii. `puadmin fs -abnchunk -t onecopy`



```
$puadmin  fs -abnchunk  -t  onecopy
Master Address: nuwa://localcluster/sys/pangu/master
ChunkId Type     FoundTime
```

iii. `puadmin fs -abnchunk -t lessmin`



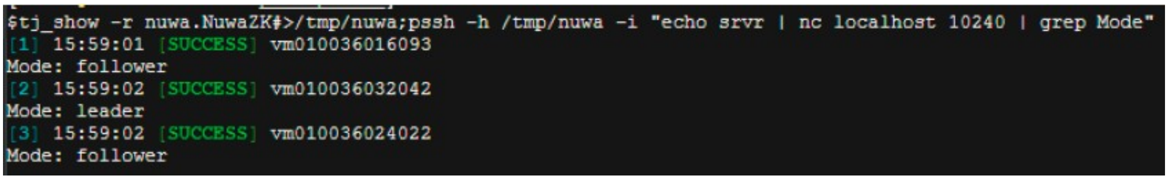
```
$puadmin  fs -abnchunk  -t  lessmin
Master Address: nuwa://localcluster/sys/pangu/master
ChunkId Type     FoundTime
```

6. Log on to the machine where Apsara Name Service and Distributed Lock Synchronization System resides.

```
echo srvr | nc localhost 10240 | grep Mode
```

Examples:

```
tj_show -r nuwa.NuwaZK#>/tmp/nuwa;pssh -h /tmp/nuwa -i "echo srvr | nc localhost 10240 | grep Mode
"
```

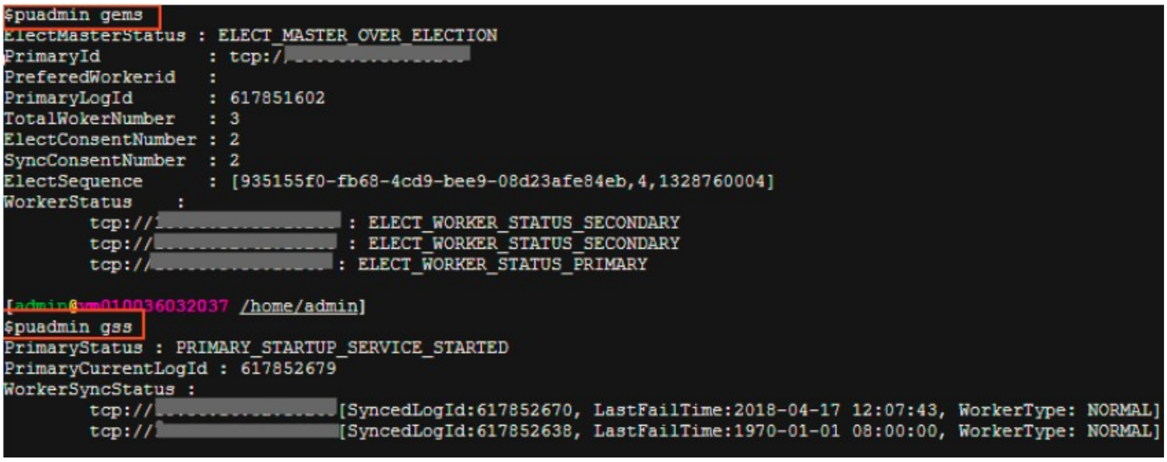


```
$tj_show -r nuwa.NuwaZK#>/tmp/nuwa;pssh -h /tmp/nuwa -i "echo srvr | nc localhost 10240 | grep Mode"
[1] 15:59:01 [SUCCESS] vm010036016093
Mode: follower
[2] 15:59:02 [SUCCESS] vm010036032042
Mode: leader
[3] 15:59:02 [SUCCESS] vm010036024022
Mode: follower
```

7. Run the following commands to check whether Apsara Distributed File System functions properly:

```
puadmin gems
```

```
puadmin gss
```



```
$puadmin gems
ElectMasterStatus : ELECT_MASTER_OVER_ELECTION
PrimaryId          : tcp:/[redacted]
PreferedWorkerid   :
PrimaryLogId       : 617851602
TotalWokerNumber   : 3
ElectConsentNumber : 2
SyncConsentNumber  : 2
ElectSequence      : [935155f0-fb68-4cd9-bee9-08d23afe84eb,4,1328760004]
WorkerStatus     :
        tcp://[redacted] : ELECT_WORKER_STATUS_SECONDARY
        tcp://[redacted] : ELECT_WORKER_STATUS_SECONDARY
        tcp://[redacted] : ELECT_WORKER_STATUS_PRIMARY

[admin@vm010036032037 /home/admin]
$puadmin gss
PrimaryStatus : PRIMARY_STARTUP_SERVICE_STARTED
PrimaryCurrentLogId : 617852679
WorkerSyncStatus :
        tcp://[redacted][SyncedLogId:617852670, LastFailTime:2018-04-17 12:07:43, WorkerType: NORMAL]
        tcp://[redacted][SyncedLogId:617852638, LastFailTime:1970-01-01 08:00:00, WorkerType: NORMAL]
```

8. Perform daily inspections in Apsara Big Data Manager (ABM) to check disk usage.

11.2.3.3. Shut down a chunkserver, perform maintenance, and then clone the chunkserver

Prerequisites

- A customer has asked to fix a faulty instance of odps_cs and clone a new one.
- You must inform the customer that this operation will temporarily render a chunkserver in the cluster unavailable, but will not affect the overall operation of the service.
- All MaxCompute services have reached the desired state and are functioning properly.
- All services on the OPS1 server have reached the desired state and are functioning properly.
- You must ensure that the disk space available is sufficient for data migration triggered when a node goes offline.
- If the primary node exists on the machine to be brought offline, you must ensure that services are switched from the primary node to the secondary node.

Procedure

1. In Apsara Infrastructure Management Framework, find **ComputerInit#** in the odps-service-computer service of the odps cluster, and open the corresponding TerminalService window. Run the following commands to check the data integrity of Apsara Distributed File System:

```
puadmin abnchunk fs -t none
-- Check for any missing files. If no output is displayed, no files are missing.
puadmin abnchunk fs -t onecopy
-- Check whether each file has only one copy. If no output is displayed, each file has only one copy.
puadmin abnchunk fs -t lessmin
-- Check whether the number of files is smaller than the minimum number of backups. If no output is dis
played, the number of files is smaller than the minimum number of backups.
```

2. Add the machine to be shut down to a Job Scheduler blacklist.

   i. Run the following command to enable the blacklisting function of Job Scheduler (ignore this step if the function has been enabled):

   ```
   /apsara/deploy/rpc_caller --Server=nuwa://localcluster/sys/fuxi/master/ForClient --Method=/fuxi/S
   etGlobalFlag --Parameter={\"fuxi_Enable_BadNodeManager\":false}
   ```

   ii. Run the following command to check the hostnames in the existing blacklist:

   ```
   /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster get
   ```

   iii. Run the following command to add the machine to be shut down to the blacklist:

   ```
   /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster add $hostname
   ```

   iv. Run the following command to check whether the machine to be shut down is already included in the blacklist:

   ```
   /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster get
   ```

3. Shut down the machine, perform maintenance, and then restart the machine.

   > Note Do not compromise the system during maintenance.

4. Run the following commands to remove the Job Scheduler blacklist:

   ```
   /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster remove $hostname
   /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster get
   ```

5. Set the status of rma to pending for the faulty machine.

i. Log on to the OPS1 server. Set the status of the rma action to pending for the faulty machine. The hostname of the faulty machine is m1.

Run the following command:

curl "http://127.0.0.1:7070/api/v5/SetMachineAction?hostname=m1" -d '{"action_name":"rma", "action_status":"pending"}'

The command output is as follows:

```
{
  "err_code": 0,
  "err_msg": "",
  "data": [
    {
      "hostname": "m1"
    }
  ]
}
```

ii. Run the following command to configure the audit log:

curl "http://127.0.0.1:7070/api/v5/AddAuditLog?object=/m/m1&category=action" -d '{"category":"action", "from":"tianji.HealingService#", "object":"/m/m1", "content": "{\n \"action\" : \"/action/rma\",\n \"description\" : \"/monitor/rma=error, mtime: 1513488046851649\",\n \"status\" : \"pending\"\n}\n" }'

The mtime parameter, which represents action_description@mtime, is set to 1513488046851649 in the example. Set the parameter to the current system time when you configure the audit log. Run the following command to query the mtime value:

curl "http://127.0.0.1:7070/api/v5/GetMachineInfo?hostname=m1&attr=action_name,action_status,action_description@mtime"

The command output is as follows:

```
{
  "err_code": 0,
  "err_msg": "",
  "data": {
    "action_description": "",
    "action_description@mtime": 1516168642565661,
    "action_name": "rma",
    "action_name@mtime": 1516777552688111,
    "action_status": "pending",
    "action_status@mtime": 1516777552688111,
    "hostname": "m1",
    "hostname@mtime": 1516120875605211
  }
}
```

6. Wait for approval.

i. Wait until the status of the rma action becomes approved or doing on the machine. Check the action status.

   Run the following command to obtain the machine information:

   ```
   curl "http://127.0.0.1:7070/api/v5/GetMachineInfo?hostname=m1"
   ```

   Command output:

   A large amount of information is returned. You can locate the following keyword: "action_status": "pending".

ii. Check the SR approval status on the machine. pending indicates that the SR is being approved. approved, doing, or done indicates that the SR has been approved. If no action was taken, the SR was not approved.

   Run the following query command:

   ```
   curl http://127.0.0.1:7070/api/v5/GetMachineInfoPackage?
   hostname=m1&attr=sr.id,sr.action_name,sr.action_status
   ```

   Command output: A large amount of information is returned. You can also view items in the doing state on the webpage.

7. Shut down the machine when the status of rma becomes approved or doing. After the maintenance is completed, start the machine.

   > ⓘ **Note** If you need to clone the machine after the maintenance is completed, proceed with the next step. Otherwise, skip the next step.

8. Clone the machine.

   i. After the maintenance is completed, run the following command to clone the machine on the OPS1 server:

   ```
   curl "http://127.0.0.1:7070/api/v5/SetMachineAction?
   hostname=m1&action_name=rma&action_status=doing" -d
   '{"action_name":"clone", "action_status":"approved", "action_description":"",
   "force":true}'
   ```

   The command output is as follows:

   ```
   {
   "err_code": 0,
   "err_msg": "",
   "data": [
   {
   "hostname": "m1"
   }
   ]
   }
   ```

ii. Access the clone container. Run the following commands to check the clone status and confirm whether the clone operation takes effect.

a. Run the following command to query the clone container:

docker ps|grep clone

The command output is as follows:

```
18c1339340ab reg.docker.god7.cn/tianji/ops_service:1f147fec4883e082646715cb79c3710f7b2
ae9c6e6851fa9a9452b92b4b3366a ops.OpsClone__.clone.1514969139
```

b. Run the following command to log on to the container:

docker ps|grep clone

c. Run the following command to query the clone task:

/home/tops/bin/python /root/opsbuild/bin/opsbuild.py acli list --status=ALL -n 10000 | vim -

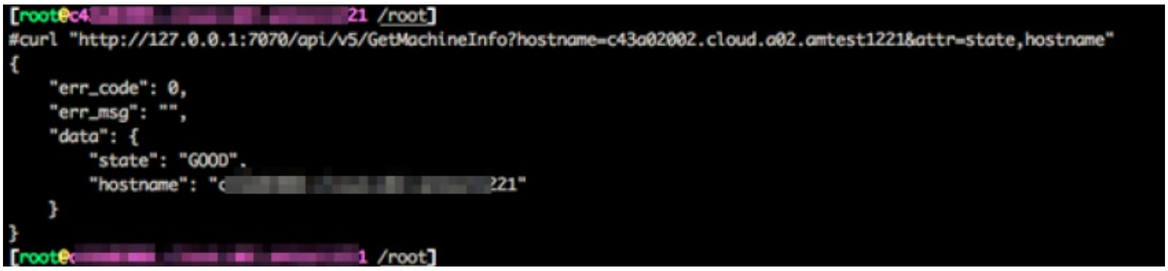
9. Run the following command to restore the machine status:

curl "http://127.0.0.1:7070/api/v5/SetMachineAction?hostname=m1&action_name=rma" -d '{"action_name":"rma","action_status":"done", "force":true}'

10. Check the machine status through the command or Apsara Infrastructure Management Framework. If the status is GOOD, the machine is normal.

Run the following command to check the machine status:

curl "http://127.0.0.1:7070/api/v5/GetMachineInfo?hostname=m1&attr=state,hostname"



```
[root@c4[redacted]21 /root]
#curl "http://127.0.0.1:7070/api/v5/GetMachineInfo?hostname=c43a02002.cloud.a02.amtest1221&attr=state,hostname"
{
    "err_code": 0,
    "err_msg": "",
    "data": {
        "state": "GOOD",
        "hostname": "c[redacted]221"
    }
}
[root@[redacted]1 /root]
```

11. Check whether the cluster has reached the desired state. Ensure that all services on the machine being brought online have reached the desired state.

12. Run the following commands to remove the Job Scheduler blacklist:

```
/apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster remove $hostname
/apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster get
```

11.2.3.4. Shut down a chunkserver for maintenance without compromising the system

Prerequisites

Check that all MaxCompute services have reached the final status and are functioning properly.

Procedure

1. In Apsara Infrastructure Management Framework, locate **ComputerInit#** in the odps-service-computer service of the odps cluster, and open the corresponding TerminalService window. Run the following commands to check the data integrity of Apsara Distributed File System:

   ```
   puadmin abnchunk fs -t none
   -- Check for any missing files. If no output is displayed, no files are missing.
   puadmin abnchunk fs -t onecopy
   -- Check whether each file has only one copy. If no output is displayed, each file has only one copy.
   puadmin abnchunk fs -t lessmin
   -- Check whether the number of files is smaller than the minimum number of backups. If no output is displayed, the number of files is smaller than the minimum number of backups.
   ```

2. Add the machine to be shut down to a Job Scheduler blacklist.

   i. Run the following command to enable the blacklisting function of Job Scheduler (ignore this step if the function has been enabled):

      ```
      /apsara/deploy/rpc_caller --Server=nuwa://localcluster/sys/fuxi/master/ForClient --Method=/fuxi/SetGlobalFlag --Parameter={\"fuxi_Enable_BadNodeManager\":false}
      ```

   ii. Run the following command to check the hostnames in the existing blacklist:

      ```
      /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster get
      ```

   iii. Run the following command to add the machine to be shut down to the blacklist:

      ```
      /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster add $hostname
      ```

   iv. Run the following command to check whether the machine to be shut down is already included in the blacklist:

      ```
      /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster get
      ```

3. Shut down the machine for maintenance and then restart the machine.

   > **Note** Do not compromise the system during maintenance.

4. Run the following commands to remove the Job Scheduler blacklist:

   ```
   /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster remove $hostname
   /apsara/deploy/rpc_wrapper/rpc.sh blacklist cluster get
   ```

Expected results

During the shutdown of Pangu_chunkserver, Apsara Distributed File System will keep trying to read data, and SQL tasks will remain in the running state. The tasks are completed after seven to eight minutes, or after the machine resumes operation.

11.2.3.5. Adjust the virtual resources of the Apsara system in MaxCompute

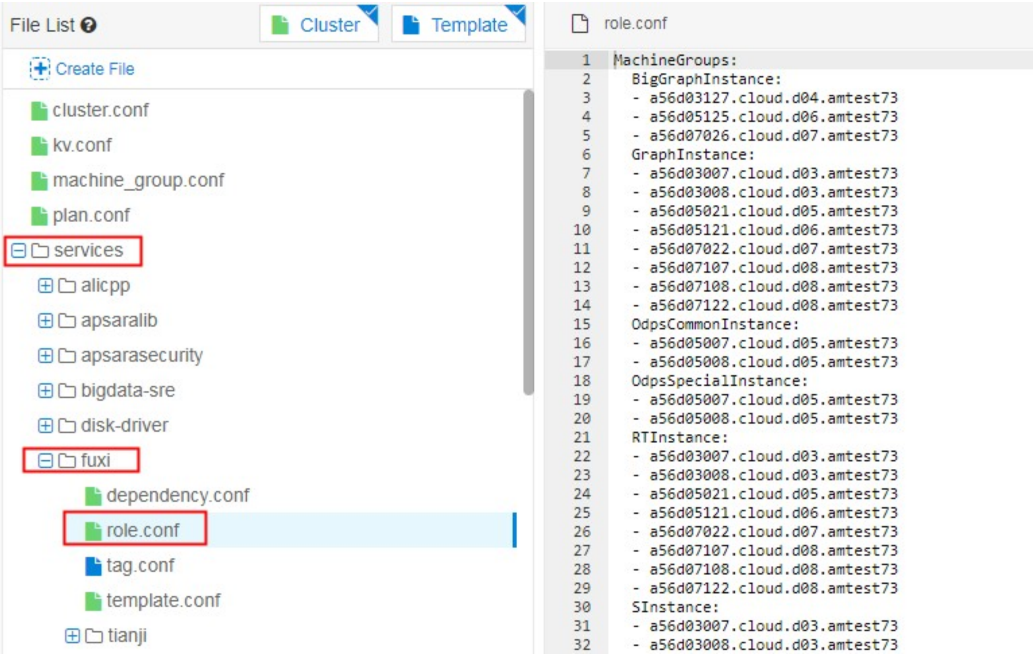
Prerequisites

All MaxCompute services have reached the desired state and are functioning properly.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console. In the left-side navigation pane, choose **Operations > Cluster Operations**. In the **Cluster** search box, enter odps to search for the expected cluster.
2. Click the cluster in the search result. On the Cluster Details page, click the **Cluster Configuration** tab. In the left-side file list, find the role.conf file in the fuxi directory.

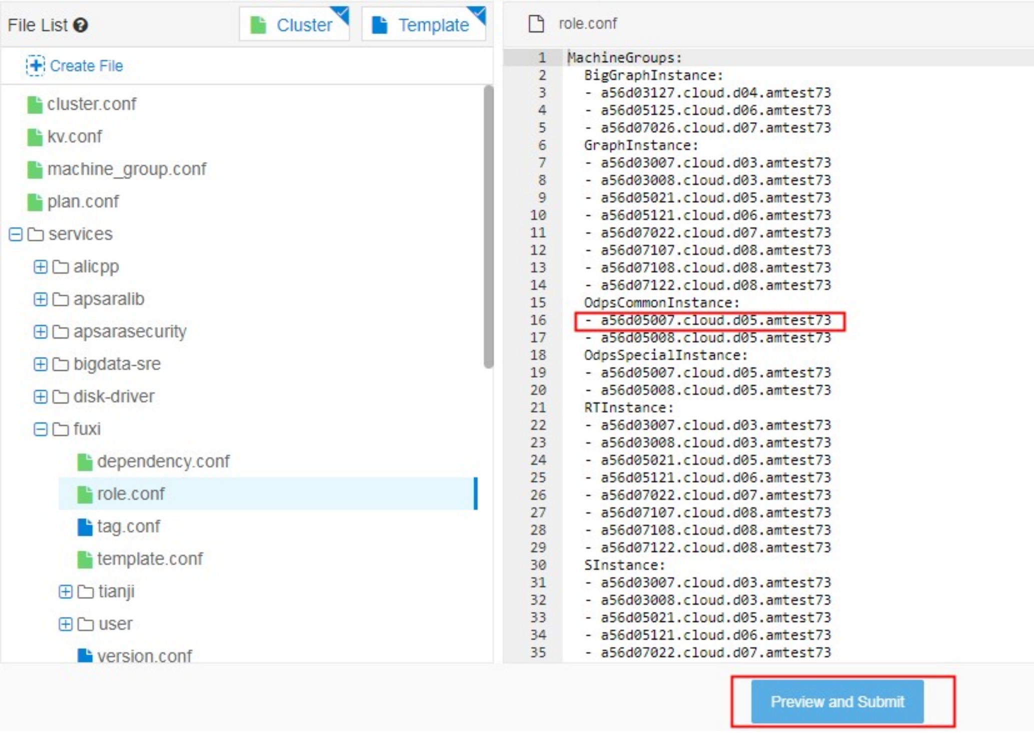
   role.conf file

   ```
   MachineGroups:
     BigGraphInstance:
     - a56d03127.cloud.d04.amtest73
     - a56d05125.cloud.d06.amtest73
     - a56d07026.cloud.d07.amtest73
     GraphInstance:
     - a56d03007.cloud.d03.amtest73
     - a56d03008.cloud.d03.amtest73
     - a56d05021.cloud.d05.amtest73
     - a56d05121.cloud.d06.amtest73
     - a56d07022.cloud.d07.amtest73
     - a56d07107.cloud.d08.amtest73
     - a56d07108.cloud.d08.amtest73
     - a56d07122.cloud.d08.amtest73
     OdpsCommonInstance:
     - a56d05007.cloud.d05.amtest73
     - a56d05008.cloud.d05.amtest73
     OdpsSpecialInstance:
     - a56d05007.cloud.d05.amtest73
     - a56d05008.cloud.d05.amtest73
     RTInstance:
     - a56d03007.cloud.d03.amtest73
     - a56d03008.cloud.d03.amtest73
     - a56d05021.cloud.d05.amtest73
     - a56d05121.cloud.d06.amtest73
     - a56d07022.cloud.d07.amtest73
     - a56d07107.cloud.d08.amtest73
     - a56d07108.cloud.d08.amtest73
     - a56d07122.cloud.d08.amtest73
     SInstance:
     - a56d03007.cloud.d03.amtest73
     - a56d03008.cloud.d03.amtest73
   ```

3. Adjust the machine tags on the right and click **Preview and Submit**.

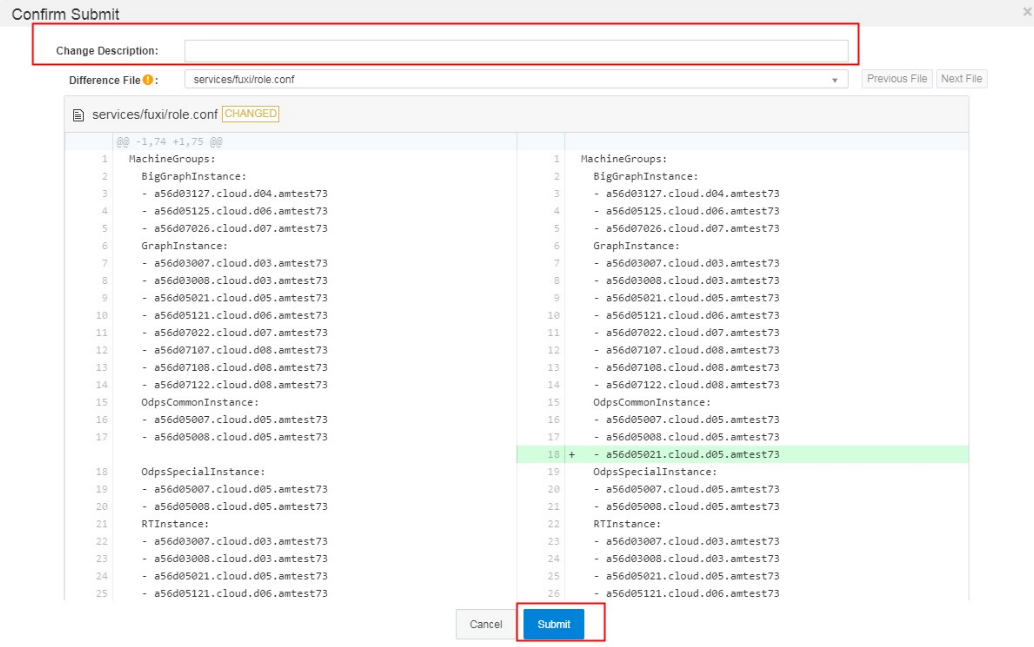
   Adjust machine tags



```
MachineGroups:
  BigGraphInstance:
  - a56d03127.cloud.d04.amtest73
  - a56d05125.cloud.d06.amtest73
  - a56d07026.cloud.d07.amtest73
  GraphInstance:
  - a56d03007.cloud.d03.amtest73
  - a56d03008.cloud.d03.amtest73
  - a56d05021.cloud.d05.amtest73
  - a56d05121.cloud.d06.amtest73
  - a56d07022.cloud.d07.amtest73
  - a56d07107.cloud.d08.amtest73
  - a56d07108.cloud.d08.amtest73
  - a56d07122.cloud.d08.amtest73
  OdpsCommonInstance:
  - a56d05007.cloud.d05.amtest73
  - a56d05008.cloud.d05.amtest73
  OdpsSpecialInstance:
  - a56d05007.cloud.d05.amtest73
  - a56d05008.cloud.d05.amtest73
  RTInstance:
  - a56d03007.cloud.d03.amtest73
  - a56d03008.cloud.d03.amtest73
  - a56d05021.cloud.d05.amtest73
  - a56d05121.cloud.d06.amtest73
  - a56d07022.cloud.d07.amtest73
  - a56d07107.cloud.d08.amtest73
  - a56d07108.cloud.d08.amtest73
  - a56d07122.cloud.d08.amtest73
  SInstance:
  - a56d03007.cloud.d03.amtest73
  - a56d03008.cloud.d03.amtest73
  - a56d05021.cloud.d05.amtest73
  - a56d05121.cloud.d06.amtest73
  - a56d07022.cloud.d07.amtest73
```

4. In the **Confirm and Submit** dialog box that appears, enter the change description and click **Submit**.

   Submit



Change Description:

Difference File: services/fuxi/role.conf

services/fuxi/role.conf CHANGED

```
@@ -1,74 +1,75 @@
MachineGroups:
  BigGraphInstance:
  - a56d03127.cloud.d04.amtest73
  - a56d05125.cloud.d06.amtest73
  - a56d07026.cloud.d07.amtest73
  GraphInstance:
  - a56d03007.cloud.d03.amtest73
  - a56d03008.cloud.d03.amtest73
  - a56d05021.cloud.d05.amtest73
  - a56d05121.cloud.d06.amtest73
  - a56d07022.cloud.d07.amtest73
  - a56d07107.cloud.d08.amtest73
  - a56d07108.cloud.d08.amtest73
  - a56d07122.cloud.d08.amtest73
  OdpsCommonInstance:
  - a56d05007.cloud.d05.amtest73
  - a56d05008.cloud.d05.amtest73
+ - a56d05021.cloud.d05.amtest73
  OdpsSpecialInstance:
  - a56d05007.cloud.d05.amtest73
  - a56d05008.cloud.d05.amtest73
  RTInstance:
  - a56d03007.cloud.d03.amtest73
  - a56d03008.cloud.d03.amtest73
  - a56d05021.cloud.d05.amtest73
  - a56d05121.cloud.d06.amtest73
```

5. The cluster starts rolling and the changes start to take effect.

   > Note You can check the task status in the operation log. If the changes take effect, the status becomes Successful.

6. After the changes are made, run the `rttrl` command in the TerminalService window to confirm the changes.

11.2.3.6. Restart MaxCompute services

Procedure

1. Log on to the Apsara Infrastructure Management Framework console. In the left-side navigation pane, choose **Operations > Cluster Operations**. In the **Cluster** search box, enter odps to search for the expected cluster.
2. Click the cluster in the search result. On the Cluster Details page, click the **Services** tab. In the **Service** search box, search for **odps-service-computer**. Click odps-service-computer in the search result.
3. After you access the **odps-service-computer** service, select **ComputerInit#** on the Service Details page. In the Actions column corresponding to the machine, click **Terminal**. In the TerminalService window that appears, you can perform subsequent command line operations.
4. Run the following command to obtain the number of machines:

   ```
   tj_show -r fuxi.Tubo#
   ```

5. Divide the number of machines by 3 to obtain the workernum value.

   > ? **Note** The workernum value ranges from 1 to 3.

6. Modify workernum in *vim /apsara/odps_service/deploy/env.cfg*.

   ```
   odps_worker_num = 2
   executor_worker_num = 2
   hiveserver_worker_num = 2
   replication_server_num = 2
   messager_partition_num = 2
   -- The values here are used as an example. Set these values as needed.
   ```

7. Restart Hive and MaxCompute.

   ```
   /apsara/odps_service/deploy/install_odps.sh restart_hiveservice
   -- Restart Hive.
   /apsara/odps_service/deploy/install_odps.sh restart_odpsservice
   -- Restart MaxCompute.
   ```

   ```
   r swl Odps/OdpsServicex
   r swl Odps/HiveServerx
   -- Check the service update status and time after restart.
   ```

8. Restart the messager service.

   ```
   cd /apsara/odps_service/deploy/; sh install_odps.sh pedeploymessagerservice
   -- Restart the messager service.
   ```

   ```
   r swl Odps/MessagerServicex
   -- Check the service update status and time after restart.
   ```

9. Restart the quota service.

```
cd /apsara/odps_service/deploy/; sh install_odps.sh pedeployquotaservice
-- Restart the quota service.
```

```
r swl Odps/QuotaServicex
-- Check the service update status and time after restart.
```

10. Restart the replication service.

```
cd /apsara/odps_service/deploy/; sh install_odps.sh pedeployreplicationservice
-- Restart the replication service.
```

```
r swl Odps/ReplicationServicex
-- Check the service update status and time after restart.
```

11. Restart the service mode.

```
r plan Odps/CGServiceControllerx >/home/admin/servicemode.json
r sstop Odps/CGServiceControllerx
r start /home/admin/servicemode.json
-- Restart the service mode.
```

```
r swl Odps/CGServiceControllerx
-- Check the CGServiceControllerx service update status and time after restart.
```

11.2.4. Common issues and solutions

11.2.4.1. View and allocate MaxCompute cluster resources

This topic describes how to view the storage and computing resources in a MaxCompute cluster. This topic also describes the quota group-related concepts, relationships between a quota group and a MaxCompute project, and quota group division policies.

Resources that can be allocated to projects in a MaxCompute cluster

- Storage resources: The total sum of storage resources available in a MaxCompute cluster is limited and can be calculated based on the number of compute nodes in the entire cluster. The storage capacity in a MaxCompute cluster is managed through Apsara Distributed File System. You can run Apsara Distributed File System commands to view the total storage capacity, such as the current storage usage statistics. The following metrics are available for measuring storage resources:
    - Storage capacity metric: indicates the total size of files that can be stored in a cluster. You can calculate the total file size in a cluster based on the following formula: Total file size in a cluster = Number of machines * (Size of a single disk * (Number of disks on a single machine - 1)) * System security level * System compression ratio/Number of distributed replicas.

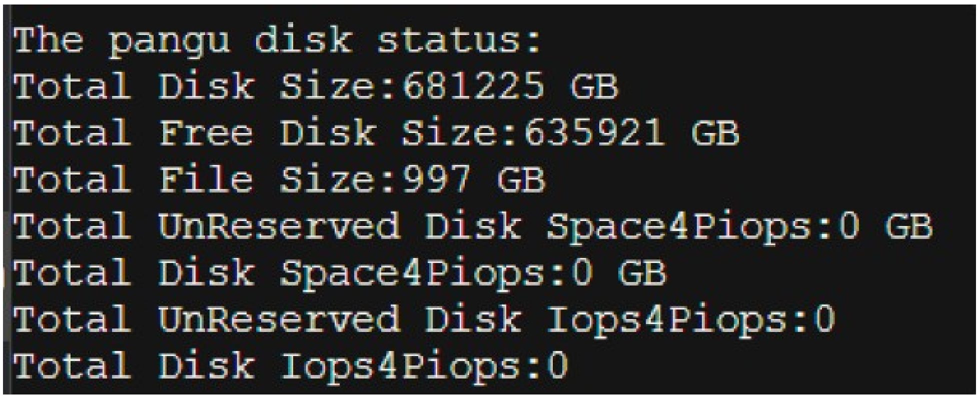
Note

- Based on the standard TPC-H test data set, the ratio of the original data size to the compressed data size is 3:1. The ratio varies depending on the characteristics of business data.
- Typically, three replicas are stored in a distributed manner.
- Security level: **The default value is 0.85 in the MaxCompute system.** You can set a custom security level as required. For example, when the business data increases rapidly and reaches 85% of the total storage quota, the security level is low. You must scale out the system as required or delete unnecessary data.

How to view the storage capacity of a MaxCompute cluster

- Run the `puadmin lscs` command on the cluster AG. The total disk size, total free disk size, and total file size are displayed at the end of the command output.

  Capacity information



```
The pangu disk status:
Total Disk Size:681225 GB
Total Free Disk Size:635921 GB
Total File Size:997 GB
Total UnReserved Disk Space4Piops:0 GB
Total Disk Space4Piops:0 GB
Total UnReserved Disk Iops4Piops:0
Total Disk Iops4Piops:0
```

Note Parameters:

- Total Disk Size: the total amount of physical space. Each file is stored in three copies. The logical space is one third the size of the physical space.
- Total Free Disk Size: the total size of available disks, excluding recycle bins on chunkservers.
- Total File Size: the total amount of physical space used by Apsara Distributed File System files, including the /deleted/ directory.

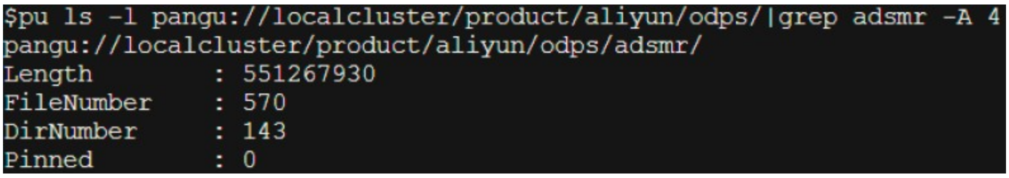
- Run the following command on the cluster AG to view the storage capacity used by all projects:

  ```
  pu ls -l pangu://localcluster/product/aliyun/odps/
  ```

  Example:

  ```
  pu ls -l pangu://localcluster/product/aliyun/odps/|grep adsmr -A 4
  -- View the capacity used by a single project, such as adsmr.
  ```

  Project capacity information

  ```
  $pu ls -l pangu://localcluster/product/aliyun/odps/|grep adsmr -A 4
  pangu://localcluster/product/aliyun/odps/adsmr/
  Length        : 551267930
  FileNumber    : 570
  DirNumber     : 143
  Pinned        : 0
  ```

  > **Note** Parameters:
  >
  > - Length: the logical length used by a project. The physical length required is three times the logical length.
  > - FileNumber: the number of files used.
  > - DirNumber: the number of directories used.

- File size metric: The total size of files that can be stored in a cluster is limited based on the memory capacity of PanguMaster. The existence of a large number of small files or an improper number of files in a cluster can also affect the stability of the cluster and its services.

  The Apsara Distributed File System index files, including the information of Apsara Distributed File System files and directories, are stored in the PanguMaster memory. Each file in PanguMaster corresponds to a file node. Each file node uses XXX bytes of memory, each level of directory uses XXX bytes of memory, and each chunk uses XXX bytes of memory. A large file is split into multiple chunks in Apsara Distributed File System. Therefore, the factors that affect PanguMaster memory usage include the number of files, directory hierarchy, and number of chunks.

  If the size of the original files in Apsara Distributed File System is large, the memory usage of PanguMaster is relatively low. When a large number of small files exist, the memory usage of PanguMaster is relatively high.

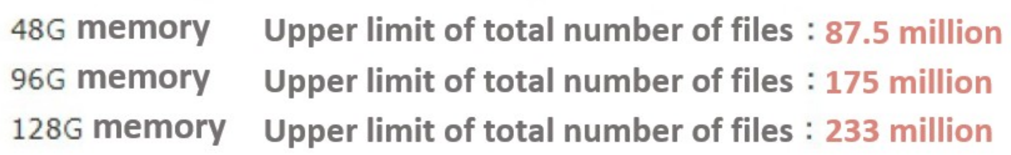
  We recommend that you perform the following operations to reduce the memory usage of PanguMaster:

  - Reduce or even delete empty directories which occupy memory, and reduce the number of directory levels.
  - Do not create directories. A directory is created automatically when you create a file.
  - Store multiple files in a directory. However, a maximum of 100,000 files can be stored.
  - Decrease the length of file names and directory names to reduce the memory usage and network traffic in PanguMaster.
  - Reduce the number of small tables and files. We recommend that you use Tunnel to upload and commit MaxCompute tables only when the table data size reaches 64 MB.

  The following figure shows the numbers of files that can be stored in Apsara Distributed File System for different PanguMaster memory capacities.

  Numbers of files that can be stored for different PanguMaster memory capacities

Numbers of files that can be stored for different PanguMaster memory capacities



48G memory Upper limit of total number of files : 87.5 million

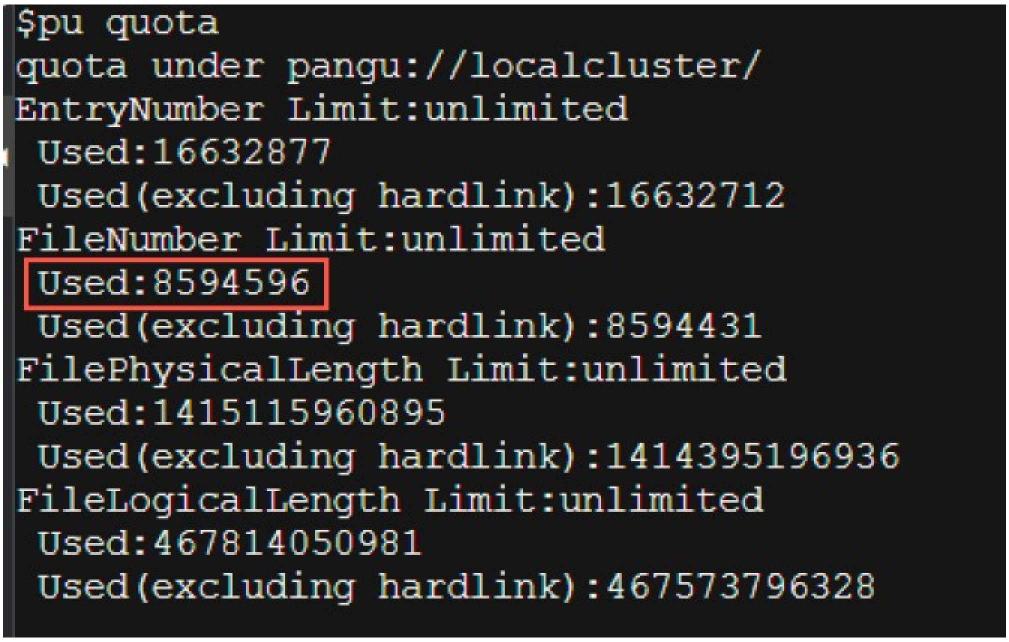
96G memory Upper limit of total number of files : 175 million

128G memory Upper limit of total number of files : 233 million

How to view the number of files stored in a MaxCompute cluster

- Run the `pu quota` command on the cluster AG to view the total number of files stored in a MaxCompute cluster.

  Total number of files

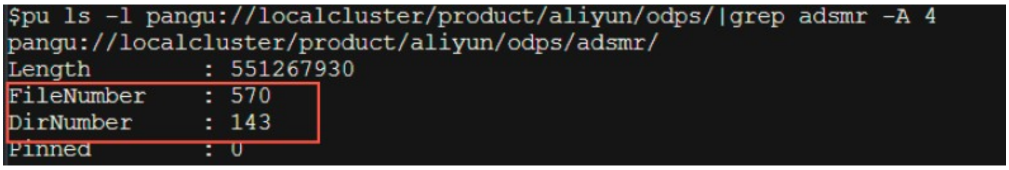
  

  ```
  $pu quota
  quota under pangu://localcluster/
  EntryNumber Limit:unlimited
   Used:16632877
   Used(excluding hardlink):16632712
  FileNumber Limit:unlimited
   Used:8594596
   Used(excluding hardlink):8594431
  FilePhysicalLength Limit:unlimited
   Used:1415115960895
   Used(excluding hardlink):1414395196936
  FileLogicalLength Limit:unlimited
   Used:467814050981
   Used(excluding hardlink):467573796328
  ```

- This example uses the adsmr project to demonstrate how to view the number of files. Run the following command on the cluster AG to view the number of files for a single project in a MaxCompute cluster:

  ```
  pu ls -l pangu://localcluster/product/aliyun/odps/|grep adsmr -A 4
  ```

  Number of files for a single project

  ```
  $pu ls -l pangu://localcluster/product/aliyun/odps/|grep adsmr -A 4
  pangu://localcluster/product/aliyun/odps/adsmr/
  Length          : 551267930
  FileNumber      : 570
  DirNumber       : 143
  Pinned          : 0
  ```

  Note Parameters:

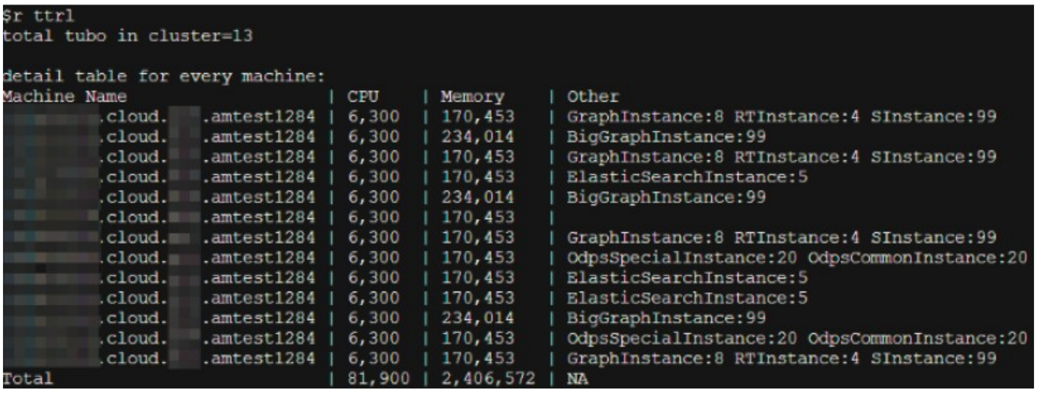
  - FileNumber: the number of files used.
  - DirNumber: the number of directories used.
  - FileNumber + DirNumber = Number of files for the current project.

- Computing resources: CPU and memory are typically referred to as computing resources in a MaxCompute cluster. The total amount of computing resources is calculated based on the following formula: Total amount of computing resources = (Number of CPU cores + Memory size of each machine) * Number of machines. For example, each machine has 56 CPU cores. One core on each machine is used by the system. The remaining 55 cores are managed by the distributed scheduling system and are scheduled for use by the MaxCompute service. The memory (aside from the chunk of memory for system overhead) is allocated by Job Scheduler. Typically, 4 GB of memory is allocated per CPU core in each MaxCompute task. The ratio varies depending on MaxCompute tasks.

How to view computing resources

- Run the `r ttrl` command on the cluster AG to view all computing resources.

  All computing resources

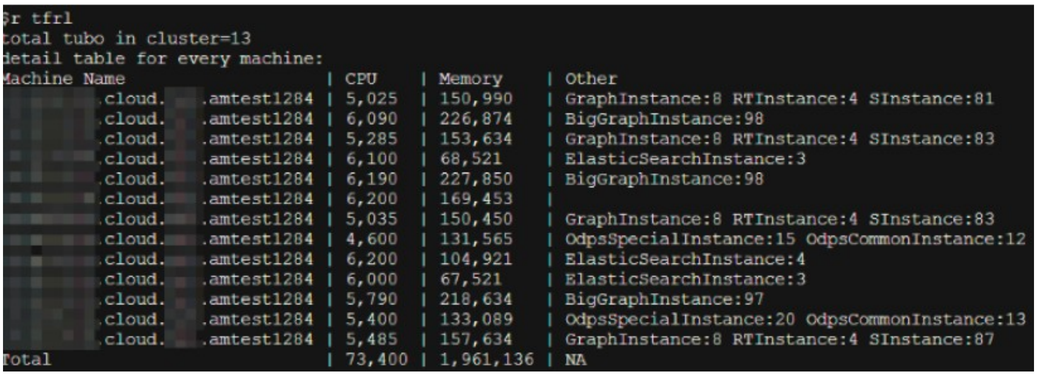
  

```
$r ttrl
total tubo in cluster=13

detail table for every machine:
Machine Name                       | CPU     | Memory      | Other
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     | GraphInstance:8 RTInstance:4 SInstance:99
[redacted].cloud.[redacted].amtest1284 | 6,300   | 234,014     | BigGraphInstance:99
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     | GraphInstance:8 RTInstance:4 SInstance:99
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     | ElasticSearchInstance:5
[redacted].cloud.[redacted].amtest1284 | 6,300   | 234,014     | BigGraphInstance:99
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     |
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     | GraphInstance:8 RTInstance:4 SInstance:99
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     | OdpsSpecialInstance:20 OdpsCommonInstance:20
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     | ElasticSearchInstance:5
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     | ElasticSearchInstance:5
[redacted].cloud.[redacted].amtest1284 | 6,300   | 234,014     | BigGraphInstance:99
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     | OdpsSpecialInstance:20 OdpsCommonInstance:20
[redacted].cloud.[redacted].amtest1284 | 6,300   | 170,453     | GraphInstance:8 RTInstance:4 SInstance:99
Total                              | 81,900 | 2,406,572 | NA
```

  ⓘ **Note** In the command output, the domain name, total CPU capacity (Unit: U. 100 U = 1 core), and total memory (Unit: MB) of each Tubo machine, as well as the role of each Tubo machine in Job Scheduling System are listed in four columns.

- Run the `r tfrl` command on the cluster AG to view the remaining computing resources.

  Remaining computing resources

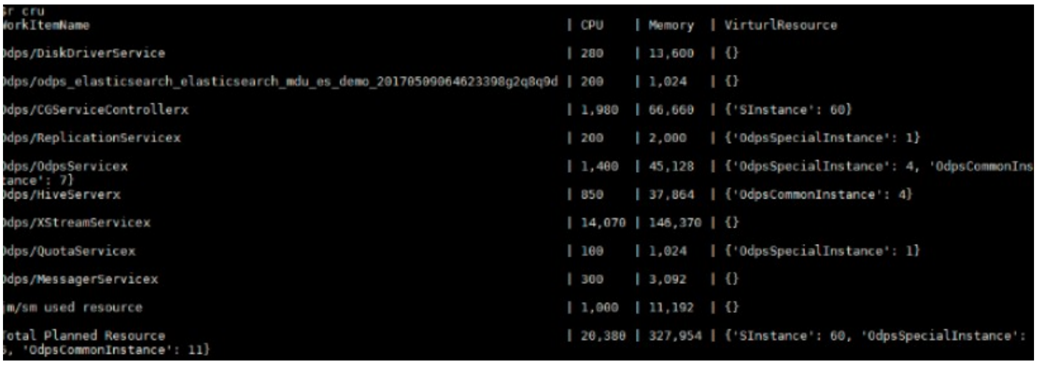
  

```
$r tfrl
total tubo in cluster=13
detail table for every machine:
Machine Name                       | CPU     | Memory      | Other
[redacted].cloud.[redacted].amtest1284 | 5,025   | 150,990     | GraphInstance:8 RTInstance:4 SInstance:81
[redacted].cloud.[redacted].amtest1284 | 6,090   | 226,874     | BigGraphInstance:98
[redacted].cloud.[redacted].amtest1284 | 5,285   | 153,634     | GraphInstance:8 RTInstance:4 SInstance:83
[redacted].cloud.[redacted].amtest1284 | 6,100   | 68,521      | ElasticSearchInstance:3
[redacted].cloud.[redacted].amtest1284 | 6,190   | 227,850     | BigGraphInstance:98
[redacted].cloud.[redacted].amtest1284 | 6,200   | 169,453     |
[redacted].cloud.[redacted].amtest1284 | 5,035   | 150,450     | GraphInstance:8 RTInstance:4 SInstance:83
[redacted].cloud.[redacted].amtest1284 | 4,600   | 131,565     | OdpsSpecialInstance:15 OdpsCommonInstance:12
[redacted].cloud.[redacted].amtest1284 | 6,200   | 104,921     | ElasticSearchInstance:4
[redacted].cloud.[redacted].amtest1284 | 6,000   | 67,521      | ElasticSearchInstance:3
[redacted].cloud.[redacted].amtest1284 | 5,790   | 218,634     | BigGraphInstance:97
[redacted].cloud.[redacted].amtest1284 | 5,400   | 133,089     | OdpsSpecialInstance:20 OdpsCommonInstance:13
[redacted].cloud.[redacted].amtest1284 | 5,485   | 157,634     | GraphInstance:8 RTInstance:4 SInstance:87
Total                              | 73,400 | 1,961,136 | NA
```

  ⓘ **Note** In the command output, the domain name, total CPU capacity (Unit: U. 100 U = 1 core), and total memory (Unit: MB) of each Tubo machine, as well as the role of each Tubo machine in Job Scheduling System are listed in four columns.

- Run the `r cru` command on the cluster AG to view the resources used by all running jobs in MaxCompute.

  Resources used by all running jobs

  ```
  $r cru
  WorkItemName                                                      | CPU    | Memory  | VirturlResource
  
  Odps/DiskDriverService                                            | 280    | 13,600  | {}
  
  Odps/odps_elasticsearch_elasticsearch_mdu_es_demo_20170509064623398g2q8q9d | 200    | 1,024   | {}
  
  Odps/CGServiceControllerx                                         | 1,980  | 66,660  | {'SInstance': 60}
  
  Odps/ReplicationServicex                                          | 200    | 2,000   | {'OdpsSpecialInstance': 1}
  
  Odps/OdpsServicex                                                 | 1,400  | 45,128  | {'OdpsSpecialInstance': 4, 'OdpsCommonIns
  tance': 7}
  Odps/HiveServerx                                                  | 850    | 37,864  | {'OdpsCommonInstance': 4}
  
  Odps/XStreamServicex                                              | 14,070 | 146,370 | {}
  
  Odps/QuotaServicex                                                | 100    | 1,024   | {'OdpsSpecialInstance': 1}
  
  Odps/MessagerServicex                                             | 300    | 3,092   | {}
  
  nm/sm used resource                                               | 1,000  | 11,192  | {}
  
  Total Planned Resource                                            | 20,380 | 327,954 | {'SInstance': 60, 'OdpsSpecialInstance':
  6, 'OdpsCommonInstance': 11}
  ```

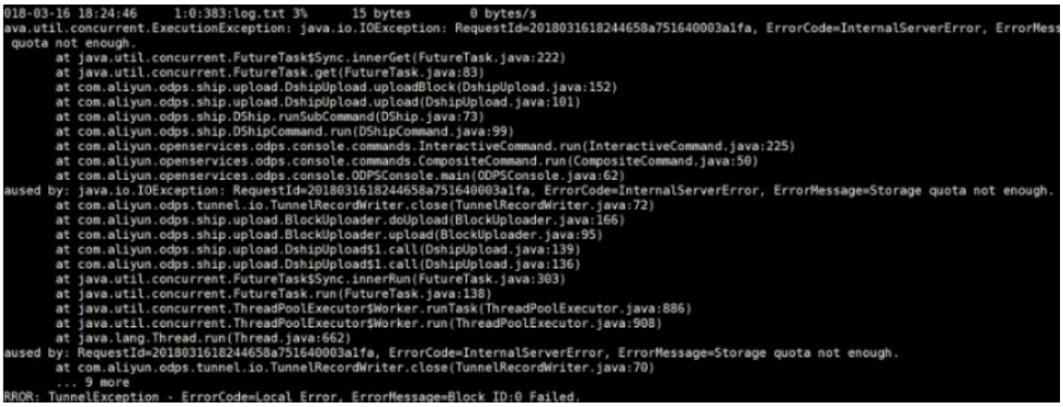
  > **Note** The name, total CPU capacity, total memory of each job, as well as the number of Fuxi instances started in the role of each job in Job Scheduling System are listed in four columns.

How to allocate project resources in a MaxCompute cluster

- Storage resource allocation: Based on the characteristics of a project, the space size and file size limit are configured when you create the project.

  If the following error messages are displayed, the file size limit of the project has been exceeded. In this case, you must organize the data in the project by deleting unnecessary table data or increasing the storage resource quota.

  Error messages

  ```
  018-03-16 18:24:46     1:0:383:log.txt 3%      15 bytes        0 bytes/s
  ava.util.concurrent.ExecutionException: java.io.IOException: RequestId=2018031618244658a751640003a1fa, ErrorCode=InternalServerError, ErrorMess
   quota not enough.
          at java.util.concurrent.FutureTask$Sync.innerGet(FutureTask.java:222)
          at java.util.concurrent.FutureTask.get(FutureTask.java:83)
          at com.aliyun.odps.ship.upload.DshipUpload.uploadBlock(DshipUpload.java:152)
          at com.aliyun.odps.ship.upload.DshipUpload.upload(DshipUpload.java:101)
          at com.aliyun.odps.ship.DShip.runSubCommand(DShip.java:73)
          at com.aliyun.odps.ship.DShipCommand.run(DShipCommand.java:99)
          at com.aliyun.openservices.odps.console.commands.InteractiveCommand.run(InteractiveCommand.java:225)
          at com.aliyun.openservices.odps.console.commands.CompositeCommand.run(CompositeCommand.java:50)
          at com.aliyun.openservices.odps.console.ODPSConsole.main(ODPSConsole.java:62)
  aused by: java.io.IOException: RequestId=2018031618244658a751640003a1fa, ErrorCode=InternalServerError, ErrorMessage=Storage quota not enough.
          at com.aliyun.odps.tunnel.io.TunnelRecordWriter.close(TunnelRecordWriter.java:72)
          at com.aliyun.odps.ship.upload.BlockUploader.doUpload(BlockUploader.java:166)
          at com.aliyun.odps.ship.upload.BlockUploader.upload(BlockUploader.java:95)
          at com.aliyun.odps.ship.upload.DshipUpload$1.call(DshipUpload.java:139)
          at com.aliyun.odps.ship.upload.DshipUpload$1.call(DshipUpload.java:136)
          at java.util.concurrent.FutureTask$Sync.innerRun(FutureTask.java:303)
          at java.util.concurrent.FutureTask.run(FutureTask.java:138)
          at java.util.concurrent.ThreadPoolExecutor$Worker.runTask(ThreadPoolExecutor.java:886)
          at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:908)
          at java.lang.Thread.run(Thread.java:662)
  aused by: RequestId=2018031618244658a751640003a1fa, ErrorCode=InternalServerError, ErrorMessage=Storage quota not enough.
          at com.aliyun.odps.tunnel.io.TunnelRecordWriter.close(TunnelRecordWriter.java:70)
          ... 9 more
  RROR: TunnelException - ErrorCode=Local Error, ErrorMessage=Block ID:0 Failed.
  ```

  > **Notice** The sum of the storage capacity of all projects cannot exceed the total allowable storage capacity of a service. Similarly, the total file size of all projects cannot exceed the total allowable file size. Therefore, you must properly allocate the storage space and file size limit by project and make timely adjustment based on your business requirements.

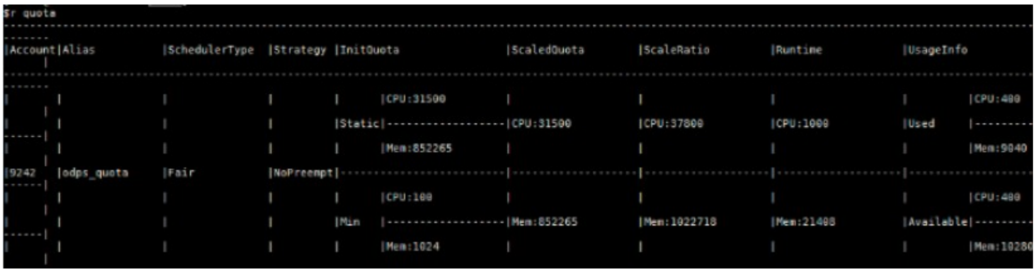
- Computing resource allocation: division of quota groups.
  - What is a quota group?

A MaxCompute cluster allows you to divide computing resources into different quota groups, and schedule them as required. A quota group represents a certain amount of CPU and memory resources. MinQuota and MaxQuota are used for CPU and memory configurations. MinQuota is the minimum quota allowed for the quota group, and MaxQuota is the maximum quota allowed for the quota group. For example, MinCPU=500 indicates that the quota group has been assigned at least 500/100=5 cores. MaxCPU=2000 indicates that the quota group has been assigned at least 2000/100=20 cores.

MaxCompute uses a FAIR scheduling policy and a first-in-first-out (FIFO) scheduling policy by default. The difference between the FAIR and FIFO scheduling polices lies in the keys by which tasks in waiting queues are sorted. If each schedule unit has its own priority, both FAIR and FIFO scheduling policies allocate high-priority schedule units first. If all schedule units share the same priority, the FIFO scheduling policy sorts the schedule units by the time when they are submitted. The earlier they are submitted, the higher priority they have. The FAIR scheduling policy sorts the scheduling units by the slotNum allocated to them. The smaller the slotNum is, the higher priority they have. For the FAIR policy group, this can basically ensure that the same amount of resources are assigned to schedule units with the same priority.

You can run the `r quota` command on the cluster AG to view quota group settings.

View quota group settings



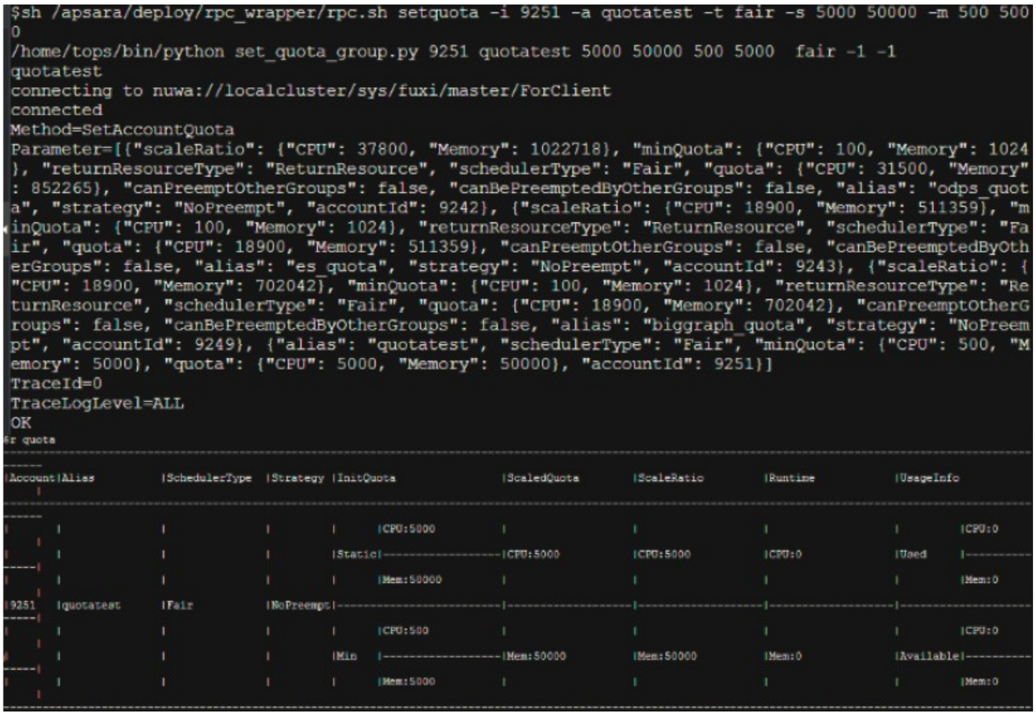
```
$r quota
----------------------------------------------------------------------------------------------------------------------------------------
-------
|Account|Alias          |SchedulerType  |Strategy |InitQuota                |ScaledQuota      |ScaleRatio       |Runtime          |UsageInfo
      |
----------------------------------------------------------------------------------------------------------------------------------------
-------
|       |               |               |         |      |CPU:31500         |                 |                 |                 |          |CPU:400
      |
|       |               |               |         |Static|------------------|CPU:31500        |CPU:37800        |CPU:1000         |Used      |---------
------|
|       |               |               |         |      |Mem:852265        |                 |                 |                 |          |Mem:9040
      |
|9242   |odps_quota     |Fair           |NoPreempt|-------------------------|-----------------|-----------------|-----------------|--------------------
------|
|       |               |               |         |      |CPU:100           |                 |                 |                 |          |CPU:400
      |
|       |               |               |         |Min   |------------------|Mem:852265       |Mem:1022718      |Mem:21408        |Available|---------
------|
|       |               |               |         |      |Mem:1024          |                 |                 |                 |          |Mem:10280
      |
```

You can run the following command on the cluster AG to create and modify a quota as needed:

```
sh /apsara/deploy/rpc_wrapper/rpc.sh setquota -i $QUOTAID -a $QUOTANAME -t fair -s $max_cpu_quota $max_mem_quota -m $min_cpu_quota $min_mem_quota
```

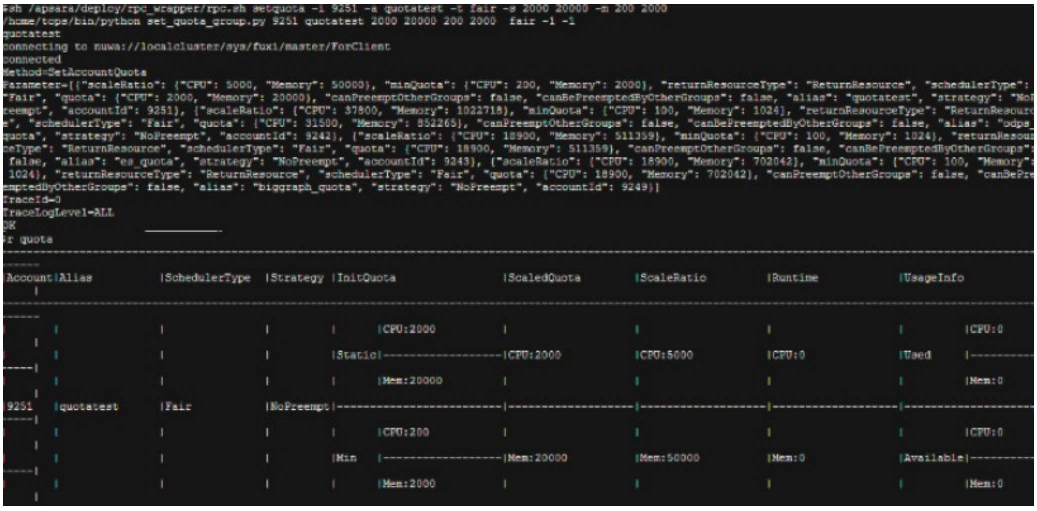
Note The command with $QUOTAID is used to modify a quota. The command without $QUOTAID is used to create a quota.

Create a quota



```
$sh /apsara/deploy/rpc_wrapper/rpc.sh setquota -i 9251 -a quotatest -t fair -s 5000 50000 -m 500 500
0
/home/tops/bin/python set_quota_group.py 9251 quotatest 5000 50000 500 5000  fair -1 -1
quotatest
connecting to nuwa://localcluster/sys/fuxi/master/ForClient
connected
Method=SetAccountQuota
Parameter=[{"scaleRatio": {"CPU": 37800, "Memory": 1022718}, "minQuota": {"CPU": 100, "Memory": 1024
}, "returnResourceType": "ReturnResource", "schedulerType": "Fair", "quota": {"CPU": 31500, "Memory"
: 852265}, "canPreemptOtherGroups": false, "canBePreemptedByOtherGroups": false, "alias": "odps_quot
a", "strategy": "NoPreempt", "accountId": 9242}, {"scaleRatio": {"CPU": 18900, "Memory": 511359}, "m
inQuota": {"CPU": 100, "Memory": 1024}, "returnResourceType": "ReturnResource", "schedulerType": "Fa
ir", "quota": {"CPU": 18900, "Memory": 511359}, "canPreemptOtherGroups": false, "canBePreemptedByOth
erGroups": false, "alias": "es_quota", "strategy": "NoPreempt", "accountId": 9243}, {"scaleRatio": {
"CPU": 18900, "Memory": 702042}, "minQuota": {"CPU": 100, "Memory": 1024}, "returnResourceType": "Re
turnResource", "schedulerType": "Fair", "quota": {"CPU": 18900, "Memory": 702042}, "canPreemptOtherG
roups": false, "canBePreemptedByOtherGroups": false, "alias": "biggraph_quota", "strategy": "NoPreem
pt", "accountId": 9249}, {"alias": "quotatest", "schedulerType": "Fair", "minQuota": {"CPU": 500, "M
emory": 5000}, "quota": {"CPU": 5000, "Memory": 50000}, "accountId": 9251}]
TraceId=0
TraceLogLevel=ALL
OK
$r quota
---------------------------------------------------------------------------------------------------------------
------
|Account|Alias          |SchedulerType  |Strategy |InitQuota               |ScaledQuota       |ScaleRatio        |Runtime           |UsageInfo
      |
---------------------------------------------------------------------------------------------------------------
------
|       |               |               |         |      |CPU:5000         |                  |                  |                  |          |CPU:0
      |
|       |               |               |         |Static|-----------------|CPU:5000          |CPU:5000          |CPU:0             |Used      |----------
------|
|       |               |               |         |      |Mem:50000        |                  |                  |                  |          |Mem:0
      |
|9251   |quotatest      |Fair           |NoPreempt|------------------------|------------------|------------------|------------------|---------------------
------|
|       |               |               |         |      |CPU:500          |                  |                  |                  |          |CPU:0
      |
|       |               |               |         |Min   |-----------------|Mem:50000         |Mem:50000         |Mem:0             |Available|----------
------|
|       |               |               |         |      |Mem:5000         |                  |                  |                  |          |Mem:0
      |
---------------------------------------------------------------------------------------------------------------
```

Modify a quota



```
$sh /apsara/deploy/rpc_wrapper/rpc.sh setquota -i 9251 -a quotatest -t fair -s 2000 20000 -m 200 2000
/home/tops/bin/python set_quota_group.py 9251 quotatest 2000 20000 200 2000  fair -1 -1
quotatest
connecting to nuwa://localcluster/sys/fuxi/master/ForClient
connected
Method=SetAccountQuota
Parameter=[{"scaleRatio": {"CPU": 5000, "Memory": 50000}, "minQuota": {"CPU": 200, "Memory": 2000}, "returnResourceType": "ReturnResource", "schedulerType":
"Fair", "quota": {"CPU": 2000, "Memory": 20000}, "canPreemptOtherGroups": false, "canBePreemptedByOtherGroups": false, "alias": "quotatest", "strategy": "NoP
reempt", "accountId": 9251}, {"scaleRatio": {"CPU": 37800, "Memory": 1022718}, "minQuota": {"CPU": 100, "Memory": 1024}, "returnResourceType": "ReturnResourc
e", "schedulerType": "Fair", "quota": {"CPU": 31500, "Memory": 852265}, "canPreemptOtherGroups": false, "canBePreemptedByOtherGroups": false, "alias": "odps_
quota", "strategy": "NoPreempt", "accountId": 9242}, {"scaleRatio": {"CPU": 18900, "Memory": 511359}, "minQuota": {"CPU": 100, "Memory": 1024}, "returnResou
ceType": "ReturnResource", "schedulerType": "Fair", "quota": {"CPU": 18900, "Memory": 511359}, "canPreemptOtherGroups": false, "canBePreemptedByOtherGroups":
 false, "alias": "es_quota", "strategy": "NoPreempt", "accountId": 9243}, {"scaleRatio": {"CPU": 18900, "Memory": 702042}, "minQuota": {"CPU": 100, "Memory":
 1024}, "returnResourceType": "ReturnResource", "schedulerType": "Fair", "quota": {"CPU": 18900, "Memory": 702042}, "canPreemptOtherGroups": false, "canBePre
emptedByOtherGroups": false, "alias": "biggraph_quota", "strategy": "NoPreempt", "accountId": 9249}]
TraceId=0
TraceLogLevel=ALL
OK
$r quota
---------------------------------------------------------------------------------------------------------------
------
|Account|Alias          |SchedulerType  |Strategy |InitQuota               |ScaledQuota       |ScaleRatio        |Runtime           |UsageInfo
      |
---------------------------------------------------------------------------------------------------------------
------
|       |               |               |         |      |CPU:2000         |                  |                  |                  |          |CPU:0
      |
|       |               |               |         |Static|-----------------|CPU:2000          |CPU:5000          |CPU:0             |Used      |----------
------|
|       |               |               |         |      |Mem:20000        |                  |                  |                  |          |Mem:0
      |
|9251   |quotatest      |Fair           |NoPreempt|------------------------|------------------|------------------|------------------|---------------------
------|
|       |               |               |         |      |CPU:200          |                  |                  |                  |          |CPU:0
      |
|       |               |               |         |Min   |-----------------|Mem:20000         |Mem:50000         |Mem:0             |Available|----------
------|
|       |               |               |         |      |Mem:2000         |                  |                  |                  |          |Mem:0
      |
```

- How to divide quota groups

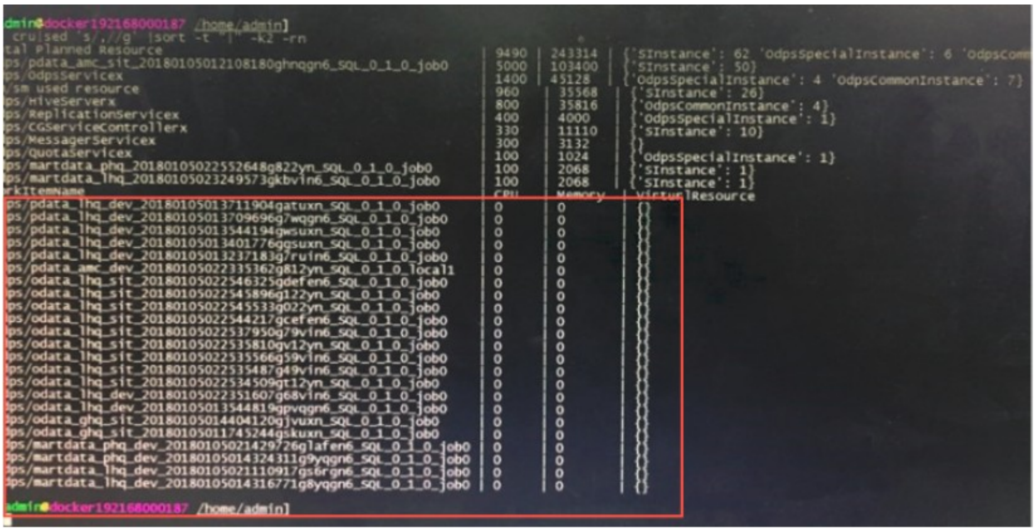
  To divide quota groups correctly, you must understand the relationship between a MaxCompute project and a quota group.

  You can select the quota group to which a project belongs upon project creation or modify the quota group after project creation.

  Resources in a quota group can be used by all running tasks of all projects in this quota group. Therefore, the project tasks in the same quota group may be affected during peak hours. That is, one or several large tasks may take up all resources in the quota group, while other computing tasks can only wait for resources.

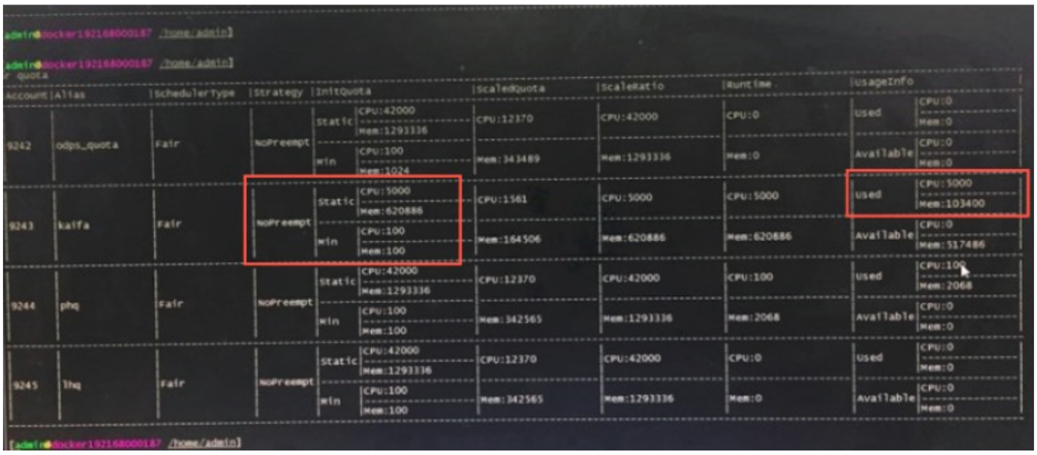
For example, in the following two figures, the first figure shows that a lot of jobs are waiting for resources (in red box). However, a lot of cluster resources are left unused. You can check the quota usage. In the second figure, quota 9243 is only allocated with 5000U, all of which are in use. The CPU quota for 9243 is used up, but there are still pending tasks in 9243. In this case, even if there are unused cluster resources, the tasks under this quota cannot have resources allocated to them.

Jobs waiting for resources



```
dmin@docker192168000187 /home/admin]
 cru|sed 's/,//g' |sort -t '|' -k2 -rn
tal Planned Resource                                    | 9490 | 243314 | {'SInstance': 62 'OdpsSpecialInstance': 6 'OdpsCom
ps/pdata_amc_sit_2018010501210818 0ghnqgn6_SQL_0_1_0_job0 | 5000 | 103400 | {'SInstance': 50}
ps/OdpsServicex                                         | 1400 | 45128  | {'OdpsSpecialInstance': 4 'OdpsCommonInstance': 7}
/sm used resource                                       | 960  |  35568 |  {'SInstance': 26}
ps/HiveServerx                                          | 800  |  35816 |  {'OdpsCommonInstance': 4}
ps/ReplicationServicex                                  | 400  |  4000  |  {'OdpsSpecialInstance': 1}
ps/CGServiceControllerx                                 | 330  |  11110 |  {'SInstance': 10}
ps/MessagerServicex                                     | 300  |  3132  |  {}
ps/QuotaServicex                                        | 100  |  1024  |  {'OdpsSpecialInstance': 1}
ps/martdata_phq_20180105022552648g822yn_SQL_0_1_0_job0  | 100  |  2068  |  {'SInstance': 1}
ps/martdata_lhq_20180105023249573gkbvin6_SQL_0_1_0_job0 | 100  |  2068  |  {'SInstance': 1}
rkItemName                                              | CPU  |  Memory | VirtualResource
ps/pdata_lhq_dev_20180105013711904gatuxn_SQL_0_1_0_job0 | 0    |  0     |  {}
ps/pdata_lhq_dev_20180105013709696g7wqgn6_SQL_0_1_0_job0 | 0   |  0     |  {}
ps/pdata_lhq_dev_20180105013544194gwsuxn_SQL_0_1_0_job0 | 0    |  0     |  {}
ps/pdata_lhq_dev_20180105013401776ggsuxn_SQL_0_1_0_job0 | 0    |  0     |  {}
ps/pdata_lhq_dev_20180105013237183g7ruin6_SQL_0_1_0_job0 | 0   |  0     |  {}
ps/pdata_amc_dev_20180105022335362g812yn_SQL_0_1_0_local1 | 0  |  0     |  {}
ps/odata_lhq_sit_20180105022546325gdefen6_SQL_0_1_0_job0 | 0   |  0     |  {}
ps/odata_lhq_sit_20180105022545896g122yn_SQL_0_1_0_job0 | 0    |  0     |  {}
ps/odata_lhq_sit_20180105022545533g022yn_SQL_0_1_0_job0 | 0    |  0     |  {}
ps/odata_lhq_sit_20180105022544217gcefen6_SQL_0_1_0_job0 | 0   |  0     |  {}
ps/odata_lhq_sit_20180105022537950g79vin6_SQL_0_1_0_job0 | 0   |  0     |  {}
ps/odata_lhq_sit_20180105022535810gv12yn_SQL_0_1_0_job0 | 0    |  0     |  {}
ps/odata_lhq_sit_20180105022535566g59vin6_SQL_0_1_0_job0 | 0   |  0     |  {}
ps/odata_lhq_sit_20180105022535487g49vin6_SQL_0_1_0_job0 | 0   |  0     |  {}
ps/odata_lhq_sit_20180105022534509gt12yn_SQL_0_1_0_job0 | 0    |  0     |  {}
ps/odata_lhq_dev_20180105022351607g68vin6_SQL_0_1_0_job0 | 0   |  0     |  {}
ps/odata_lhq_dev_20180105013544819gpvqgn6_SQL_0_1_0_job0 | 0   |  0     |  {}
ps/odata_ghq_sit_20180105014404120gjvuxn_SQL_0_1_0_job0 | 0    |  0     |  {}
ps/odata_ghq_sit_20180105011745244gskuxn_SQL_0_1_0_job0 | 0    |  0     |  {}
ps/martdata_phq_dev_20180105021429726glafen6_SQL_0_1_0_job0 | 0 | 0     |  {}
ps/martdata_phq_dev_20180105014324311g9yqgn6_SQL_0_1_0_job0 | 0 | 0     |  {}
ps/martdata_lhq_dev_20180105021110917gs6rgn6_SQL_0_1_0_job0 | 0 | 0     |  {}
ps/martdata_lhq_dev_20180105014316771g8yqgn6_SQL_0_1_0_job0 | 0 | 0     |  {}
dmin@docker192168000187 /home/admin]
```

Quota used up



```
admin@docker192168000187 /home/admin]

admin@docker192168000187 /home/admin]
r quota
--------------------------------------------------------------------------------------------------------------------------------
Account|Alias       |SchedulerType |Strategy   |InitQuota                |ScaledQuota   |ScaleRatio    |Runtime      |UsageInfo
--------------------------------------------------------------------------------------------------------------------------------
       |            |              |           |Static|CPU:42000         |CPU:12370     |CPU:42000     |CPU:0        |Used     |CPU:0
       |            |              |           |      |Mem:1293336       |              |              |             |         |Mem:0
9242   |odps_quota  |Fair          |NoPreempt  |------------------------ |------------- |------------- |------------ |---------------
       |            |              |           |Min   |CPU:100           |Mem:343489    |Mem:1293336   |Mem:0        |Available|CPU:0
       |            |              |           |      |Mem:1024          |              |              |             |         |Mem:0
--------------------------------------------------------------------------------------------------------------------------------
       |            |              |           |Static|CPU:5000          |CPU:1561      |CPU:5000      |CPU:5000     |Used     |CPU:5000
       |            |              |           |      |Mem:620886        |              |              |             |         |Mem:103400
9243   |kaifa       |Fair          |NoPreempt  |------------------------ |------------- |------------- |------------ |---------------
       |            |              |           |Min   |CPU:100           |Mem:164506    |Mem:620886    |Mem:620886   |Available|CPU:0
       |            |              |           |      |Mem:100           |              |              |             |         |Mem:517486
--------------------------------------------------------------------------------------------------------------------------------
       |            |              |           |Static|CPU:42000         |CPU:12370     |CPU:42000     |CPU:100      |Used     |CPU:100
       |            |              |           |      |Mem:1293336       |              |              |             |         |Mem:2068
9244   |phq         |Fair          |NoPreempt  |------------------------ |------------- |------------- |------------ |---------------
       |            |              |           |Min   |CPU:100           |Mem:342565    |Mem:1293336   |Mem:2068     |Available|CPU:0
       |            |              |           |      |Mem:100           |              |              |             |         |Mem:0
--------------------------------------------------------------------------------------------------------------------------------
       |            |              |           |Static|CPU:42000         |CPU:12370     |CPU:42000     |CPU:0        |Used     |CPU:0
       |            |              |           |      |Mem:1293336       |              |              |             |         |Mem:0
9245   |lhq         |Fair          |NoPreempt  |------------------------ |------------- |------------- |------------ |---------------
       |            |              |           |Min   |CPU:100           |Mem:342565    |Mem:1293336   |Mem:0        |Available|CPU:0
       |            |              |           |      |Mem:100           |              |              |             |         |Mem:0
--------------------------------------------------------------------------------------------------------------------------------
[admin@docker192168000187 /home/admin]
```

You must divide quota groups based on the following general principles:

- You must plan quota groups in a way that they do not mutually interfere with each other in a large resource pool, and avoid overly fine-grained division of resource groups. For example, some large tasks cannot be scheduled due to quota group limits, or occupy a quota group for an extended period of time, which affects other tasks in the group.
- You must consider the configured MinQuota and MaxQuota when dividing quota groups.
- You can oversell the resources in your cluster, that is, the sum of MaxQuotas of all quota groups can be greater than the total amount of cluster resources. However, the oversell ratio cannot be too high. If the oversell ratio is too high, a quota group with a running project may perpetually occupy a large amount of resources.
- When dividing quota groups, you must consider the priorities of tasks, task execution duration, amount of task data, and characteristics of computing types.

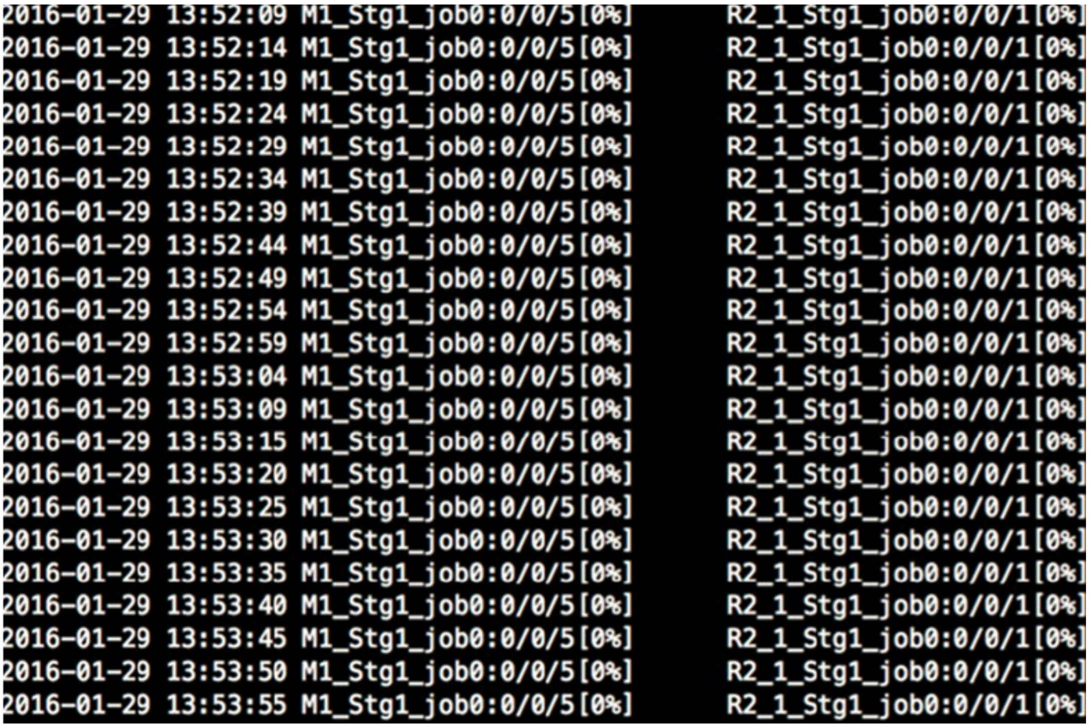
- Properly configure quota groups for peak hours. We recommend that you configure a separate quota group for tasks that are important and time-consuming.
- The division of quota groups and the selection and configuration of projects are conducted based on a resource pre-allocation policy, which needs to be adjusted in a timely manner, based on actual requirements.

11.2.4.2. Common issues and data skew troubleshooting

Scenario 1: how to determine whether a job has stopped running due to insufficient resources

Symptom: The job does not progress as expected.

Symptom

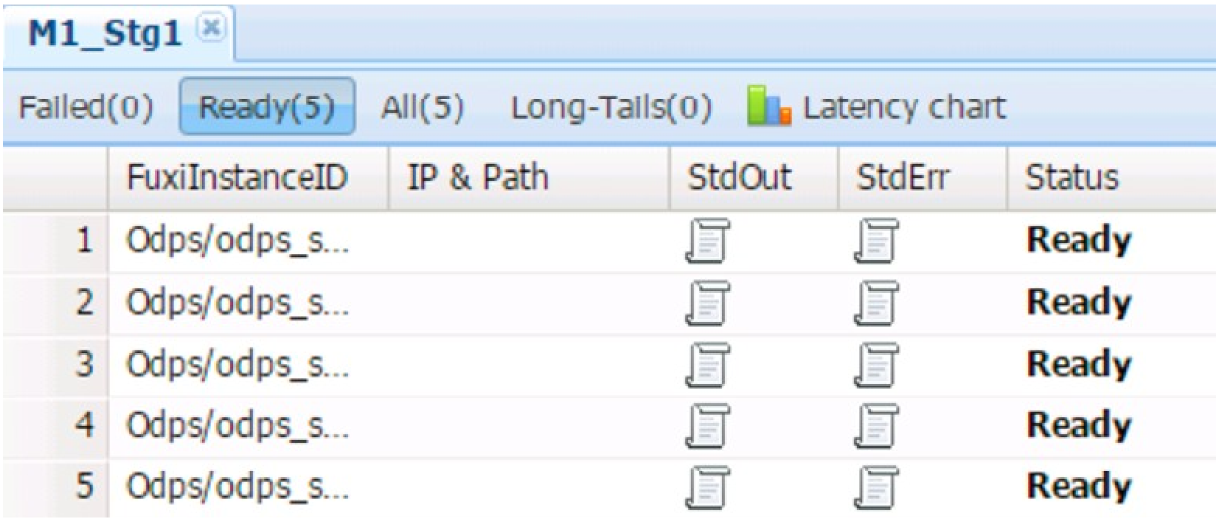


```
2016-01-29 13:52:09 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:14 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:19 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:24 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:29 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:34 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:39 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:44 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:49 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:54 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:52:59 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:04 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:09 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:15 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:20 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:25 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:30 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:35 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:40 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:45 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:50 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
2016-01-29 13:53:55 M1_Stg1_job0:0/0/5[0%]        R2_1_Stg1_job0:0/0/1[0%]
```

Cause: The issue is typically caused by insufficient resources. You can use LogView to determine the status of job resources (task instance status).

- Ready: indicates that instances are waiting for Job Scheduler to allocate resources. Instances can resume operation after they obtain the necessary resources.
- Wait: indicates that instances are waiting for dependent tasks to complete.

The task instances in the Ready state shown in the following figure indicate that there are insufficient resources to run these tasks. After an instance obtains the necessary resources, its status changes to Running.



M1_Stg1

Failed(0) Ready(5) All(5) Long-Tails(0) Latency chart

	FuxiInstanceID	IP & Path	StdOut	StdErr	Status
1	Odps/odps_s...				Ready
2	Odps/odps_s...				Ready
3	Odps/odps_s...				Ready
4	Odps/odps_s...				Ready
5	Odps/odps_s...				Ready

Solution:

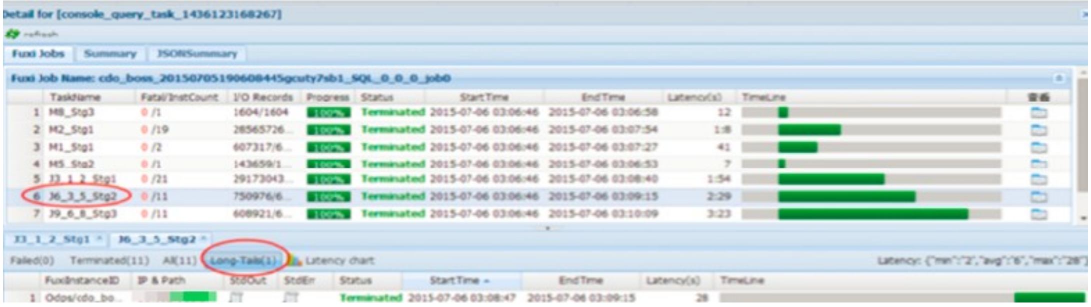
- If there are insufficient resources during peak hours, you can reschedule the tasks to run during off-peak hours.
- If the computing quotas are insufficient, check whether the quota group of the project has sufficient computing resources.
- If computing resources in the cluster are occupied for long periods of time, you can develop a computing quota allocation policy to scale the quota as necessary.
- We recommend that you do not run abnormally large jobs to prevent the jobs from occupying resources for extended periods of time.
- You can enable SQL acceleration, so that you can run small jobs without requesting resources from Job Scheduler.
- You can use the First-In First-Out (FIFO) scheduling policy.

Scenario 2: how to find the root cause of a job that has been running for an extended period of time

Symptom: The MaxCompute job execution progress has remained at 99% for a long period of time.

Cause: The running time of some Fuxi instances in the MaxCompute job is significantly longer than that of other Fuxi instances.

Cause analysis



Detail for [console_query_task_1436123168267]

Fuxi Job Name: cdo_boss_20150705190608445gcuty7sb1_SQL_0_0_0_job0

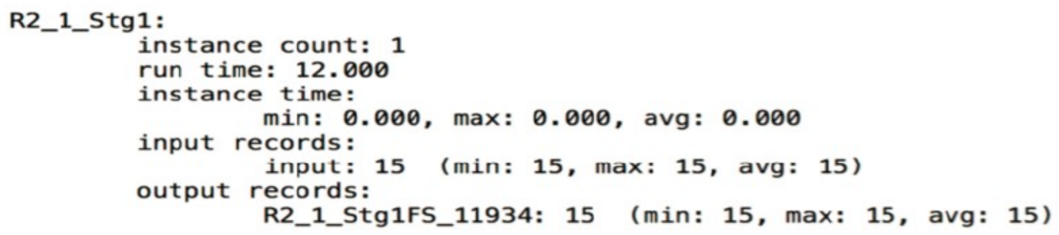
	TaskName	Fatal/InstCount	I/O Records	Progress	Status	StartTime	EndTime	Latency(s)	TimeLine	查看
1	M8_Stg3	0 /1	1604/1604	100%	Terminated	2015-07-06 03:06:46	2015-07-06 03:06:58	12		
2	M2_Stg1	0 /19	28565726...	100%	Terminated	2015-07-06 03:06:46	2015-07-06 03:07:54	1:8		
3	M1_Stg1	0 /2	607317/6...	100%	Terminated	2015-07-06 03:06:46	2015-07-06 03:07:27	41		
4	M5_Stg2	0 /1	143659/1...	100%	Terminated	2015-07-06 03:06:46	2015-07-06 03:06:53	7		
5	J3_1_2_Stg1	0 /21	29173043...	100%	Terminated	2015-07-06 03:06:46	2015-07-06 03:08:40	1:54		
6	J6_3_5_Stg2	0 /11	750976/6...	100%	Terminated	2015-07-06 03:06:46	2015-07-06 03:09:15	2:29		
7	J9_6_8_Stg3	0 /11	608921/6...	100%	Terminated	2015-07-06 03:06:46	2015-07-06 03:10:09	3:23		

Latency: {"min":"2","avg":"6","max":"28"}

	FuxiInstanceID	IP & Path	StdOut	StdErr	Status	StartTime	EndTime	Latency(s)	TimeLine
1	Odps/cdo_bo...				Terminated	2015-07-06 03:08:47	2015-07-06 03:09:15	28	

Further analysis: Analyze the job summary in LogView, and calculate the difference between the max and avg values of input and output records of a slow task. If the max and avg values differ by several orders of magnitude, it can be initially determined that the job data is skewed.

Further analysis



```
R2_1_Stg1:
        instance count: 1
        run time: 12.000
        instance time:
                min: 0.000, max: 0.000, avg: 0.000
        input records:
                input: 15  (min: 15, max: 15, avg: 15)
        output records:
                R2_1_Stg1FS_11934: 15  (min: 15, max: 15, avg: 15)
```

Solution: If there are slow Fuxi instances on a particular machine, check whether a hardware failure has occurred on the machine.

Scenario 3: How to improve the concurrency of MaxCompute jobs

Fault locating: The concurrency of Map tasks depends on the following factors:

- Split size and merge limit.

  Map takes a series of data files as inputs. Larger files are split into partitions based on the odps.sql.mapper.split.size value, which is 256 MB by default. An instance is started for each partition. However, starting an instance requires resources and time. Small files can be merged into a single partition based on the odps.sql.mapper.merge.limit.size value and be processed by a single instance to improve instance utilization. The default value of odps.sql.mapper.merge.limit.size is 64 MB. The total size of small files merged cannot exceed this value.

- Instances cannot process data across multiple partitions.

  A partition is mapped to a folder in Apsara Distributed File System. You must run at least one instance to process data in a partition. Instances cannot process data across multiple partitions. In a partition, you must run instances based on the preceding rule.

Typically, the number of instances for Reduce tasks is 1/4 of that for Map tasks. The number of instances for Join tasks is the same as that for Map tasks, but cannot exceed 1,111.

You can use the following methods to increase the number of concurrent instances for Reduce and Join tasks:

```
set odps.sql.reducer.instances = xxx
```

```
set odps.sql.joiner.instances = xxx
```

Scenarios that require higher concurrency:

- A single record only contains a small amount of data.

  Because a single record contains a small amount of data, there are many records in a file of the same size. If you split data into 256 MB chunks, a single Map instance needs to process a large number of records, reducing concurrency.

- Dump operations occur in the Map, Reduce, and Join stages.

  Based on the preceding job summary analysis, the displayed dump information indicates that the instance does not have sufficient memory to sort data in the Shuffle stage. Improving concurrency can reduce the amount of data processed by a single instance to the amount of data that can be handled by the memory, eliminate disk I/O time consumption, and improve the processing speed.

- Time-consuming UDFs are used.

  The execution of UDFs is time-consuming. If you execute UDFs concurrently, you can reduce the UDF execution time of an instance.

Solution:

- You can decrease the following parameter values to improve the concurrency of Map tasks:

  ```
  odps.sql.mapper.split.size = xxx
  odps.sql.mapper.merge.limit.size = xxx
  ```

- You can increase the following parameter values to improve the concurrency of Reduce and Join tasks:

  ```
  odps.sql.reducer.instances = xxx
  odps.sql.joiner.instances = xxx
  ```

Note: Improving concurrency will result in a greater amount of resources being consumed. We recommend that you take cost into account when improving concurrency. An instance takes an average of 10 minutes to complete after optimization, improving overall resource utilization. We recommend that you optimize jobs in critical paths so that they consume less time.

Scenario 4: how to resolve data skew issues

Different types of data skew issues in SQL are resolved in different ways.

- GROUP BY data skew

  The uneven distribution of GROUP BY keys results in data skew on reducers. You can set the anti-skew parameter before executing SQL tasks.

  ```
  set odps.sql.groupby.skewindata=true
  ```

  After this parameter is set to true, the system automatically adds a random number to each key when running the Shuffle hash algorithm and prevents data skew by introducing a new task.

- DISTRIBUTE BY data skew

  Using constants to execute the DISTRIBUTE BY clause for full sorting of the entire table will result in data skew on reducers. We recommend that you do not perform this operation.

- Data skew in the Join stage

  Data is skewed in the Join stage when the Join keys are unevenly distributed. For example, a key exists in multiple joined tables, resulting in a Cartesian explosion of data in the Join instance. You can use one of the following solutions to resolve data skew in the Join stage:

  - When a large table and a small table are joined, use MapJoin instead of Join to optimize query performance.
  - Use a separate logic to handle a skewed key. For example, when a large number of null values exist in the key, you can filter out the null values or execute a CASE WHEN statement to replace them with random values before the Join operation.
  - If you do not want to modify SQL statements, configure the following parameters to allow MaxCompute to perform automatic optimization:

    ```
    set odps.sql.skewinfo=tab1:(col1,col2)[(v1,v2),(v3,v4),...]
    set odps.sql.skewjoin=true;
    ```

- Data skew caused by multi-distinct

  Multi-distinct syntax aggravates GROUP BY data skew. You can use the GROUP BY clause with the COUNT function instead of multi-distinct to alleviate the data skew issue.

- UDF OOM

  Some jobs report an OOM error during runtime. The error message is as follows: `FAILED: ODPS-0123144 : Fuxi job failed - WorkerRestart errCode:9,errMsg:SigKill(OOM), usually caused by OOM(out of memory)` . You can fix the error by configuring the UDF runtime parameters. Example:

  ```
  odps.sql.mapper.memory=3072;
  set odps.sql.udf.jvm.memory=2048;
  set odps.sql.udf.python.memory=1536;
  ```

The related data skew settings are as follows:

```
set odps.sql.groupby.skewindata=true/false
```

Description: allows you to enable GROUP BY optimization.

```
set odps.sql.skewjoin=true/false
```

Description: allows you to enable Join optimization. It is effective only when odps.sql.skewinfo is set.

```
set odps.sql.skewinfo
```

Description: allows you to set detailed information for Join optimization. The command syntax is as follows:

```
set odps.sql.skewinfo=skewed_src:(skewed_key)[("skewed_value")]
src a join src_skewjoin1 b on a.key = b.key;
```

Example:

```
set odps.sql.skewinfo=src_skewjoin1:(key)[("0")]
-- The output result for a single skewed value of a single field is as follows: explain select a.key c1, a.value c2, b.key c3, b.value c4 from src a join src_skewjoin1 b on a.key = b.key;
```

```
set odps.sql.skewinfo=src_skewjoin1:(key)[("0")("1")]
-- The output result for multiple skewed values of a single field is as follows: explain select a.key c1, a.value c2, b.key c3, b.value c4 from src a join src_skewjoin1 b on a.key = b.key;
```

Scenario 5: how to configure common SQL parameters

Map settings

```
set odps.sql.mapper.cpu=100
```

Description: allows you to set the number of CPUs used by each instance in a Map task. Default value: 100. Valid values: 50 to 800.

```
set odps.sql.mapper.memory=1024
```

Description: allows you to set the memory size of each instance in a Map task. Unit: MB. Default value: 1024. Valid values: 256 to 12288.

```
set odps.sql.mapper.merge.limit.size=64
```

Description: allows you to set the maximum size of control files to be merged. Unit: MB. Default value: 64. You can set this variable to control the inputs of mappers. Valid values: 0 to Integer.MAX_VALUE.

```
set odps.sql.mapper.split.size=256
```

Description: allows you to set the maximum data input volume for a Map task. Unit: MB. Default value: 256. You can set this variable to control the inputs of mappers. Valid values: 1 to Integer.MAX_VALUE.

Join settings

```
set odps.sql.joiner.instances=-1
```

Description: allows you to set the number of instances in a Join task. Default value: -1. Valid values: 0 to 2000.

```
set odps.sql.joiner.cpu=100
```

Description: allows you to set the number of CPUs used by each instance in a Join task. Default value: 100. Valid values: 50 to 800.

```
set odps.sql.joiner.memory=1024
```

Description: allows you to set the memory size of each instance in a Join task. Unit: MB. Default value: 1024. Valid values: 256 to 12288.

Reduce settings

```
set odps.sql.reducer.instances=-1
```

Description: allows you to set the number of instances in a Reduce task. Default value: -1. Valid values: 0 to 2000.

```
set odps.sql.reducer.cpu=100
```

Description: allows you to set the number of CPUs used by each instance in a Reduce task. Default value: 100. Valid values: 50 to 800.

```
set odps.sql.reducer.memory=1024
```

Description: allows you to set the memory size of each instance in a Reduce task. Unit: MB. Default value: 1024. Valid values: 256 to 12288.

UDF settings

```
set odps.sql.udf.jvm.memory=1024
```

Description: allows you to set the maximum memory size used by the UDF JVM heap. Unit: MB. Default value: 1024. Valid values: 256 to 12288.

```
set odps.sql.udf.timeout=600
```

Description: allows you to set the timeout period of a UDF. Unit: seconds. Default value: 600. Valid values: 0 to 3600.

```
set odps.sql.udf.python.memory=256
```

Description: allows you to set the maximum memory size used by the UDF Python API. Unit: MB. Default value: 256. Valid values: 64 to 3072.

```
set odps.sql.udf.optimize.reuse=true/false
```

Description: When this parameter is set to true, each UDF function expression can only be calculated once, improving performance. Default value: true.

```
set odps.sql.udf.strict.mode=false/true
```

Description: allows you to control whether functions return NULL or an error if dirty data is found. If the parameter is set to true, an error is returned. Otherwise, NULL is returned.

MapJoin settings

```
set odps.sql.mapjoin.memory.max=512
```

Description: allows you to set the maximum memory size for a small table when running MapJoin. Unit: MB. Default value: 512. Valid values: 128 to 2048.

```
set odps.sql.reshuffle.dynamicpt=true/false
```

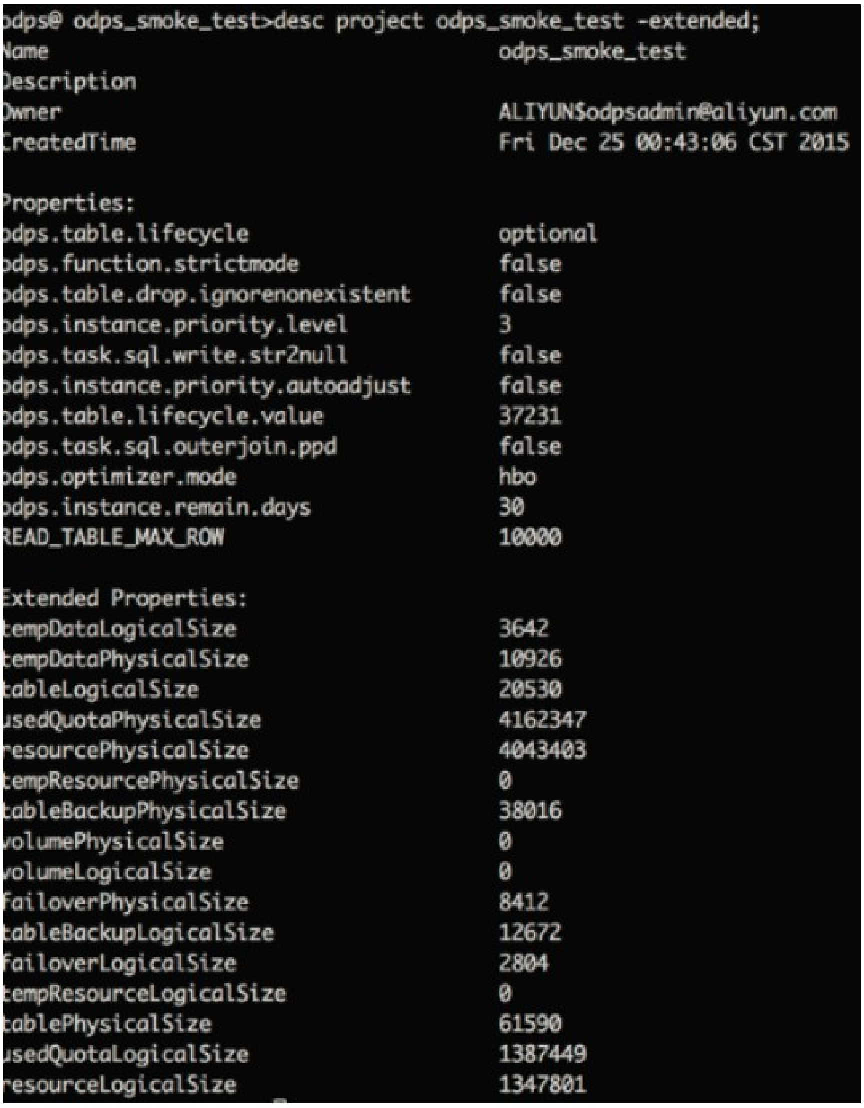
Description:

- Dynamic partitioning scenarios are time-consuming. Disabling dynamic partitioning can accelerate SQL.
- If there are few dynamic partitions, disabling dynamic partitioning can prevent data skew.

Scenario 6: how to check the storage usage of a single project

Launch the MaxCompute console as a project owner and run the `desc project <project_name>-extended;` command to view the following information.

Storage information



```
odps@ odps_smoke_test>desc project odps_smoke_test -extended;
Name                                    odps_smoke_test
Description
Owner                                   ALIYUN$odpsadmin@aliyun.com
CreatedTime                             Fri Dec 25 00:43:06 CST 2015

Properties:
odps.table.lifecycle                    optional
odps.function.strictmode                false
odps.table.drop.ignorenonexistent       false
odps.instance.priority.level            3
odps.task.sql.write.str2null            false
odps.instance.priority.autoadjust       false
odps.table.lifecycle.value              37231
odps.task.sql.outerjoin.ppd             false
odps.optimizer.mode                     hbo
odps.instance.remain.days               30
READ_TABLE_MAX_ROW                      10000

Extended Properties:
tempDataLogicalSize                     3642
tempDataPhysicalSize                    10926
tableLogicalSize                        20530
usedQuotaPhysicalSize                   4162347
resourcePhysicalSize                    4043403
tempResourcePhysicalSize                0
tableBackupPhysicalSize                 38016
volumePhysicalSize                      0
volumeLogicalSize                       0
failoverPhysicalSize                    8412
tableBackupLogicalSize                  12672
failoverLogicalSize                     2804
tempResourceLogicalSize                 0
tablePhysicalSize                       61590
usedQuotaLogicalSize                    1387449
resourceLogicalSize                     1347801
```

The preceding figure shows the capacity-related storage information of the project. The relationship between the physical and logical values of the related metrics is: Physical value of a metric = Logical value of the metric * Number of replicas.

11.2.5. MaxCompute O&M

11.2.5.1. Log on to the ABM console

This topic describes how to log on to the Apsara Big Data Manager (ABM) console.

Prerequisites

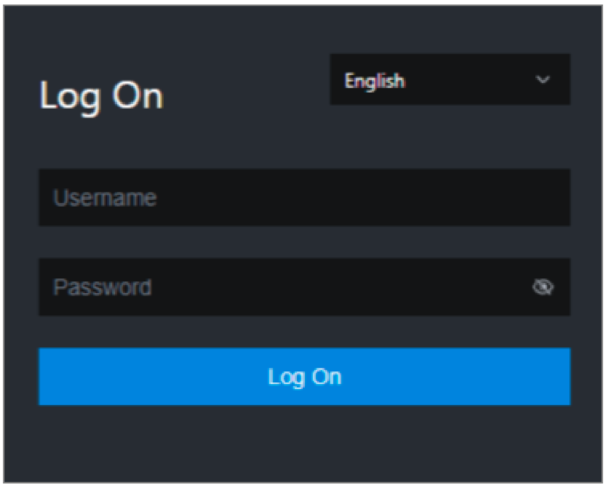
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.



> ? **Note** You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

> ? **Note** Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

For security reasons, your password must meet the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password must be 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Product Management > Products**.
7. In the **Big Data Services** section, choose **General-Purpose O&M > Apsara Big Data Manager**.

11.2.5.2. Business O&M

11.2.5.2.1. O&M overview and entry

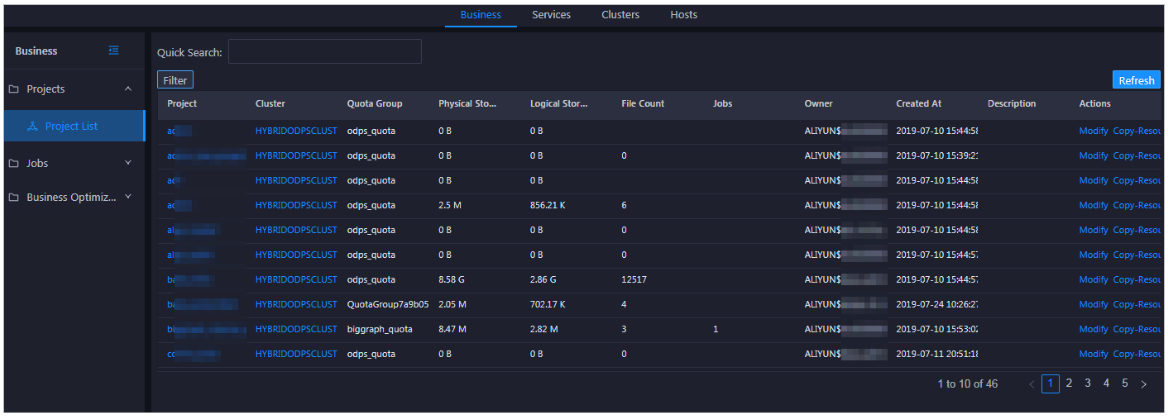
This topic describes the business O&M features and how to go to the business O&M page.

Business O&M features

- Projects:
  - Project List: shows all projects and project details in a MaxCompute cluster. You can search for and filter projects. You can also change the quota group of a project. If zone-disaster recovery is enabled, you can specify resource replication parameters and determine whether to enable resource replication for a project.
  - Authorize Package for Metadata Repository: allows you to authorize members of a project to access the metadata warehouse.
  - Encryption at Rest: allows you to encrypt the data stored in MaxCompute projects.
  - Disaster Recovery: allows you to view the cluster status when zone-disaster recovery is enabled for MaxCompute. You can enable the switchover between the primary and secondary clusters. You can also determine whether to run scheduled tasks to synchronize resources between the primary and secondary clusters.
- Quota Groups: shows the quota groups of all projects in a MaxCompute cluster. It allows you to create and modify quota groups. You can also view details about quota groups and enable period management for quota groups.
- Jobs: shows information about jobs in a MaxCompute cluster. You can search for and filter jobs. You can also view the operational logs, terminate running jobs, and collect job logs.
- Business Optimization:
  - File Merging: allows you to create file merge tasks for clusters and projects. You can also filter merge tasks and view the records of the tasks.
  - File Archiving: allows you to create file archive tasks for clusters and projects. You can also filter archive tasks and view the records of the tasks.
  - Resource Analysis: allows you to view the resource usage of the cluster from different dimensions.

Go to the business O&M page

1. Log on to the Apsara Big Data Manager (ABM) console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Business** tab. In the left-side navigation pane, choose **Projects > Project List**.



Project	Cluster	Quota Group	Physical Sto...	Logical Stor...	File Count	Jobs	Owner	Created At	Description	Actions
ac[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B			ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
ac[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B	0		ALIYUN$[redacted]	2019-07-10 15:39:2		Modify Copy-Resou
ac[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B			ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
ac[redacted]	HYBRIDODPSCLUST	odps_quota	2.5 M	856.21 K	6		ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
al[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B	0		ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
al[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B	0		ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
ba[redacted]	HYBRIDODPSCLUST	odps_quota	8.58 G	2.86 G	12517		ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
ba[redacted]	HYBRIDODPSCLUST	QuotaGroup7a9b05	2.05 M	702.17 K	4		ALIYUN$[redacted]	2019-07-24 10:26:2		Modify Copy-Resou
bi[redacted]	HYBRIDODPSCLUST	biggraph_quota	8.47 M	2.82 M	3	1	ALIYUN$[redacted]	2019-07-10 15:53:0		Modify Copy-Resou
cc[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B	0		ALIYUN$[redacted]	2019-07-11 20:51:1		Modify Copy-Resou

1 to 10 of 46 < 1 2 3 4 5 >

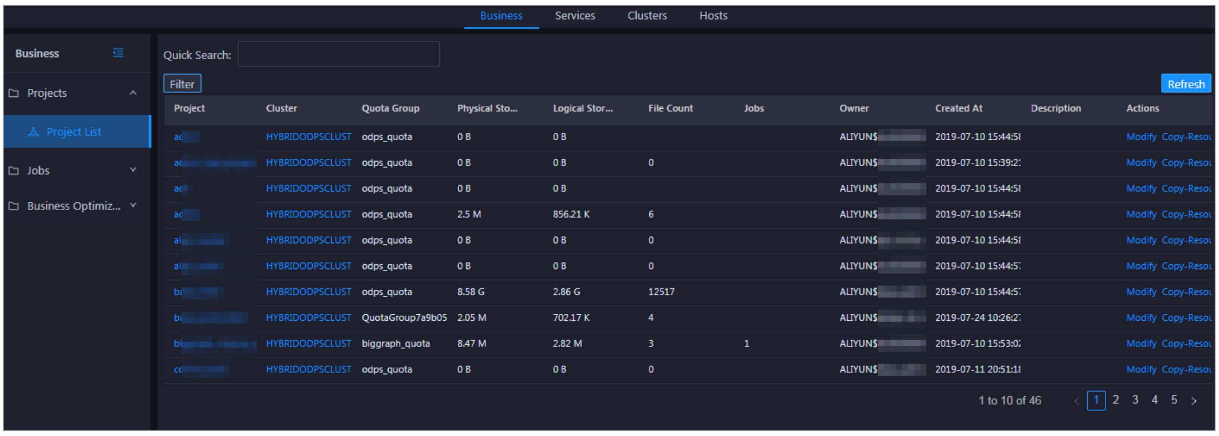
11.2.5.2.2. Project management

11.2.5.2.2.1. Project list

The Project List page shows all projects and project details in a MaxCompute cluster. You can filter, query, and sort projects. You can also change the quota group of a project. If zone-disaster recovery is enabled, you can specify resource replication parameters and determine whether to enable resource replication for a project.

Go to the Project List page

In the left-side navigation pane of the **Business** tab, choose **Projects > Project List** to view projects in a cluster.



Project	Cluster	Quota Group	Physical Sto...	Logical Stor...	File Count	Jobs	Owner	Created At	Description	Actions
ac[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B			ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
ac[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B	0		ALIYUN$[redacted]	2019-07-10 15:39:2		Modify Copy-Resou
ac[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B			ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
ac[redacted]	HYBRIDODPSCLUST	odps_quota	2.5 M	856.21 K	6		ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
al[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B	0		ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
al[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B	0		ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
ba[redacted]	HYBRIDODPSCLUST	odps_quota	8.58 G	2.86 G	12517		ALIYUN$[redacted]	2019-07-10 15:44:5		Modify Copy-Resou
ba[redacted]	HYBRIDODPSCLUST	QuotaGroup7a9b05	2.05 M	702.17 K	4		ALIYUN$[redacted]	2019-07-24 10:26:2		Modify Copy-Resou
bi[redacted]	HYBRIDODPSCLUST	biggraph_quota	8.47 M	2.82 M	3	1	ALIYUN$[redacted]	2019-07-10 15:53:0		Modify Copy-Resou
cc[redacted]	HYBRIDODPSCLUST	odps_quota	0 B	0 B	0		ALIYUN$[redacted]	2019-07-11 20:51:1		Modify Copy-Resou

1 to 10 of 46 ‹ 1 2 3 4 5 ›

The **Project List** page shows the detailed information about all projects in a cluster. You can view the name, cluster, used storage, storage quota, storage usage, number of files, owner, and creation time of a project.

View project details

On the **Project List** page, click the name of a project to view its details. You can view the project overview, jobs, storage, configuration, quota group, and tunnel, as well as information about resource analysis and cross-cluster replication. For more information, see MaxCompute workbench. You can also grant access permissions on the metadata warehouse to project members and encrypt data of the project. For more information, see Grant access permissions on the metadata warehouse and Encrypt data.

Change a quota group

You can change the default quota group of a project.

1. On the **Project List** page, find the target project, click **Actions** in the Actions column, and select **Change Default Quota Group**. In the **Change Default Quota Group** pane, specify the required parameters.

   Parameters:

   - **Region**: the region of the project.
   - **Cluster**: the default cluster of the project. If the project belongs to multiple clusters, select a cluster from the drop-down list to serve as the default cluster.
   - **Quota Group**: the quota group to which the project belongs. To change the quota group, select a quota group from the drop-down list.

2. After you specify the parameters, click **Run**.

Modify the storage quota

You can modify the storage quota of a project.

1. On the **Project List** page, find the target project, click **Actions** in the Actions column, and select **Modify Storage Quota**. In the **Change Storage Quota** pane, specify the required parameters.

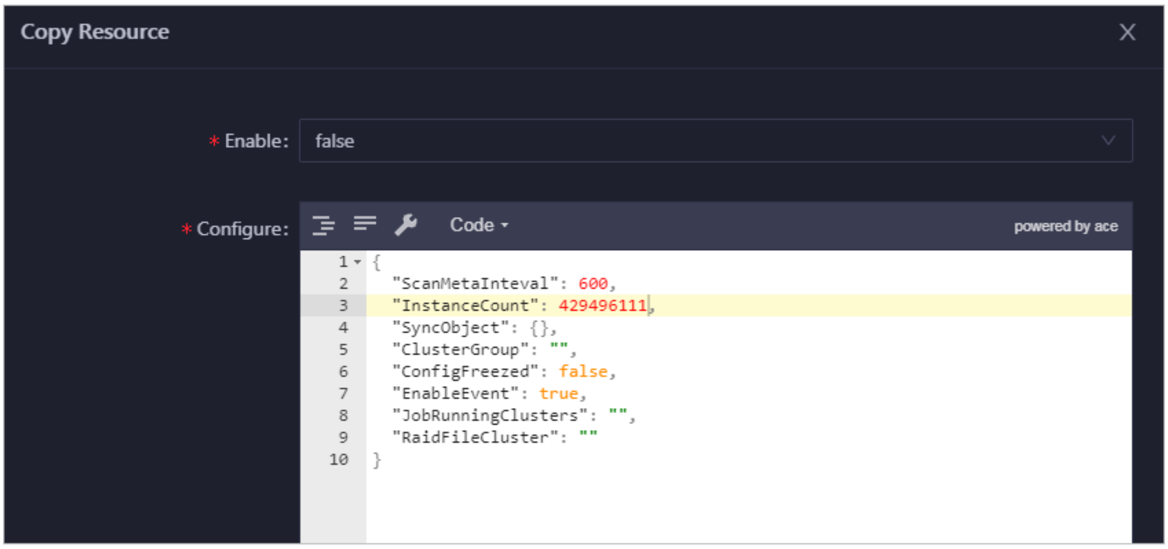
   Parameters:

   - **Region**: the region of the project
   - **Project**: the name of the project for which you want to modify the storage quota
   - **Cluster**: the default cluster of the project
   - **Target Storage Quota (TB)**: the new storage quota
   - **Reason**: the cause for the modification
2. After you specify the parameters, click **Run**.

Configure resource replication

The resource replication feature can be configured only in zone-disaster recovery scenarios. In other scenarios, you can only view the settings. In zone-disaster recovery scenarios, you can determine whether to enable the resource replication feature for a project in the primary cluster. If the resource replication feature is enabled for a project, you can configure data synchronization rules for the project to regularly synchronize data such as table data to a secondary cluster.

1. On the **Project List** page, find the target project, click **Actions** in the Actions column, and select **Resource Replication**. In the **Copy Resource** pane, specify the required parameters.

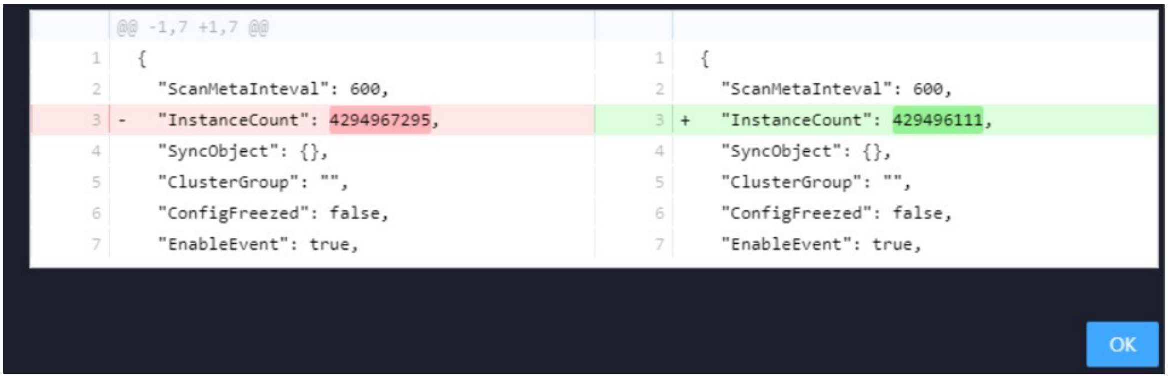
   * Enable: false

   * Configure:

   ```
   {
     "ScanMetaInteval": 600,
     "InstanceCount": 429496111,
     "SyncObject": {},
     "ClusterGroup": "",
     "ConfigFreezed": false,
     "EnableEvent": true,
     "JobRunningClusters": "",
     "RaidFileCluster": ""
   }
   ```

   Parameters:

   - **Enable**: specifies whether to enable the resource replication feature. The value **true** indicates that the resource replication feature is enabled. The value **false** indicates that the resource replication feature is disabled. Default value: **false**.
   - **Configure**: the data synchronization rules of a project. In most cases, the default settings are used. If you want to modify the settings, consult second-line O&M engineers.
2. After you modify code in the **Configure** field, click **Compare Versions** to view the differences, which are highlighted.



```
@@ -1,7 +1,7 @@
 {                                              {
   "ScanMetaInteval": 600,                        "ScanMetaInteval": 600,
-  "InstanceCount": 4294967295,                 + "InstanceCount": 429496111,
   "SyncObject": {},                              "SyncObject": {},
   "ClusterGroup": "",                            "ClusterGroup": "",
   "ConfigFreezed": false,                        "ConfigFreezed": false,
   "EnableEvent": true,                           "EnableEvent": true,
```

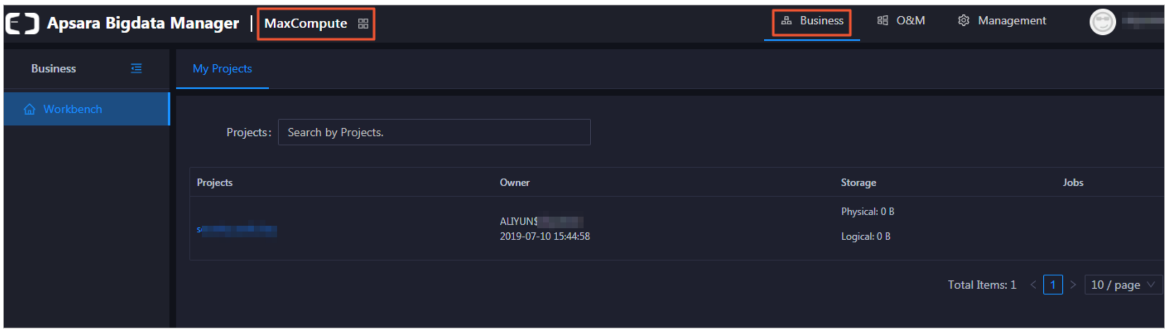
3. Click **Run**.

11.2.5.2.2.2. Project details

The Apsara Big Data Manager (ABM) console shows your MaxCompute projects and project details. You can view the project overview, jobs, storage, configurations, quota groups, and tunnels, as well as information about resource analysis, storage encryption, and cross-cluster replication.

Go to the project details page

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Business** tab. The **Project List** page appears by default. Click the name of a project to view its details.



Projects: Search by Projects.

Projects	Owner	Storage	Jobs
[redacted]	ALIYUN$[redacted] 2019-07-10 15:44:58	Physical: 0 B Logical: 0 B	

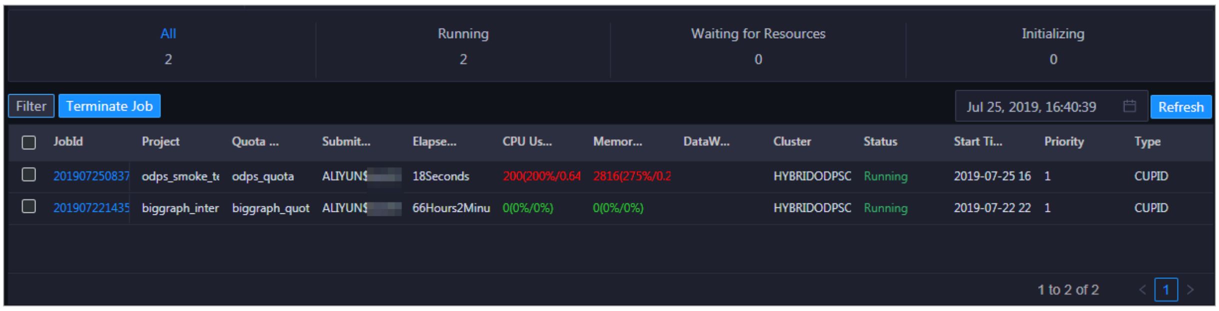
Overview

On the **Overview** tab, you can view the following information about the selected project:

- Basic information, such as the default quota group, creator, creation time, service, and region
- Trend charts that show the trend lines of requested and used CPU and memory resources by minute in different colors
- Trend chart that shows the trend lines of CPU utilization and memory usage by day in different colors

Jobs

On the **Jobs** tab, you can view job snapshots by day over the last week. Detailed information about a job snapshot includes the job ID, project, quota group, submitter, running duration, minimum CPU utilization, maximum CPU utilization, minimum memory usage, maximum memory usage, DataWorks node, running status, start time, priority, and type. You can also view the operational logs of a job to locate its running faults.



All	Running	Waiting for Resources	Initializing
2	2	0	0

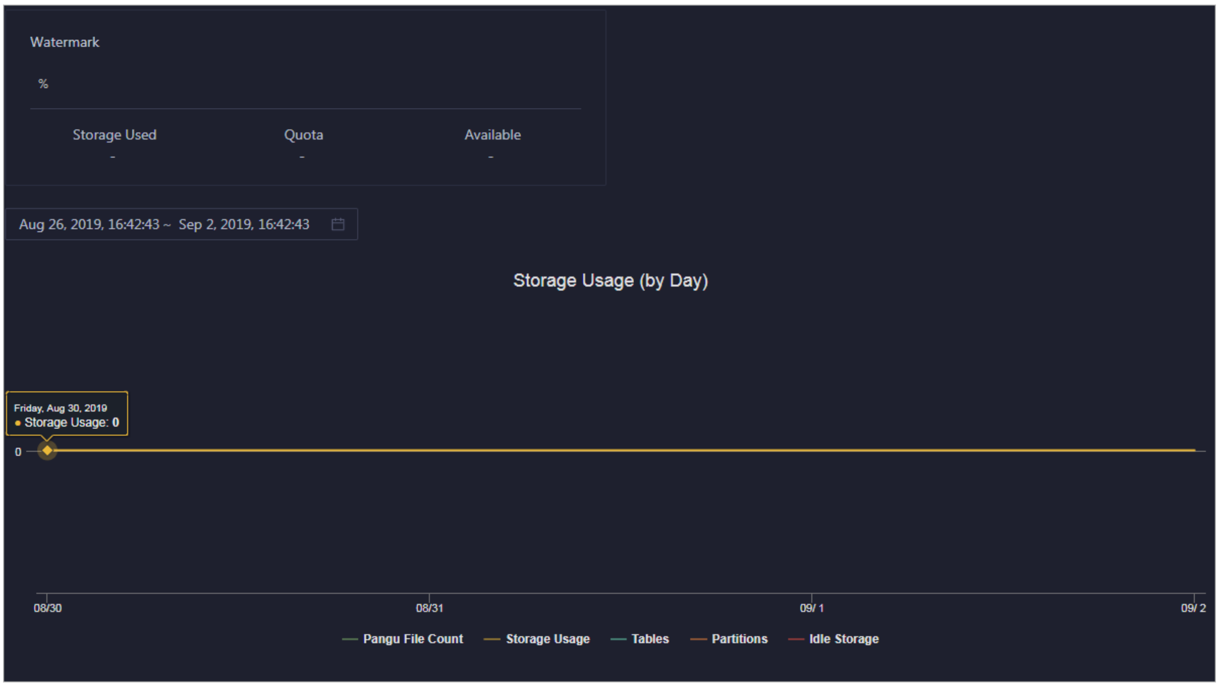
□	JobId	Project	Quota ...	Submit...	Elapse...	CPU Us...	Memor...	DataW...	Cluster	Status	Start Ti...	Priority	Type
□	201907250837	odps_smoke_te	odps_quota	ALIYUN$[redacted]	18Seconds	200(200%/0.64	2816(275%/0.2		HYBRIDODPSC	Running	2019-07-25 16	1	CUPID
□	201907221435	biggraph_inter	biggraph_quot	ALIYUN$[redacted]	66Hours2Minu	0(0%/0%)	0(0%/0%)		HYBRIDODPSC	Running	2019-07-22 22	1	CUPID

You can perform the following operations on the Jobs tab:

- Customize columns or sort job snapshots by column.
- View the operational logs of jobs or terminate jobs.

Storage

On the **Storage** tab, you can view the storage usage, used storage space, storage quota, and available storage space. You can also view a trend chart that shows the trend lines of storage usage, the number of files in Apsara Distributed File System, the number of tables, the number of partitions, and idle storage by day in different colors.



Watermark

%

Storage Used	Quota	Available
-	-	-

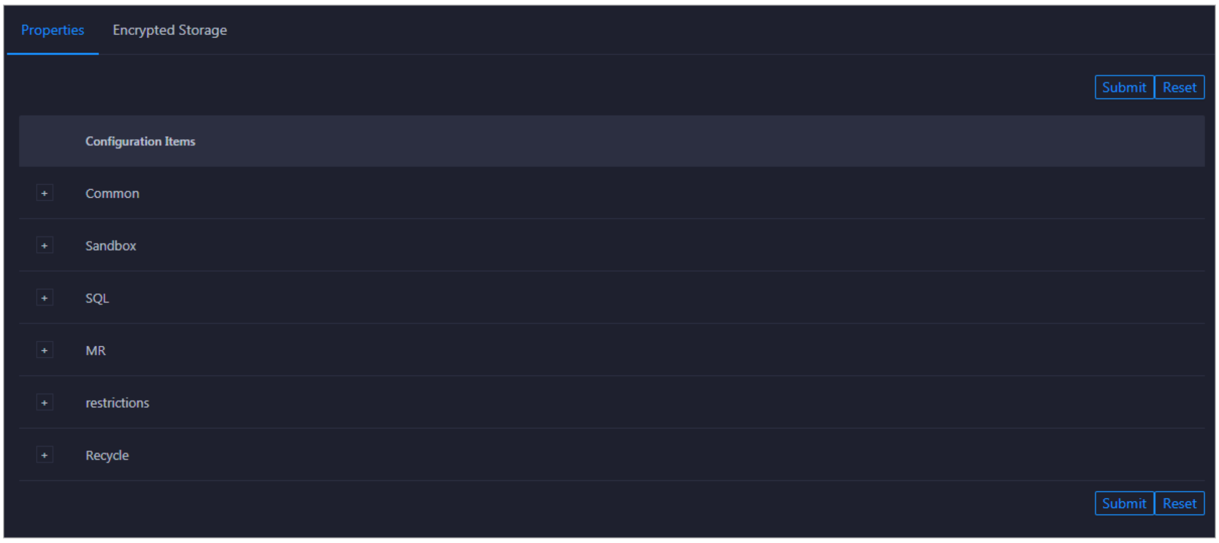
Aug 26, 2019, 16:42:43 ~ Sep 2, 2019, 16:42:43

> **Note** The Storage tab shows only information about storage resources. To query information about computing resources, go to the Quota Groups tab.

Configuration

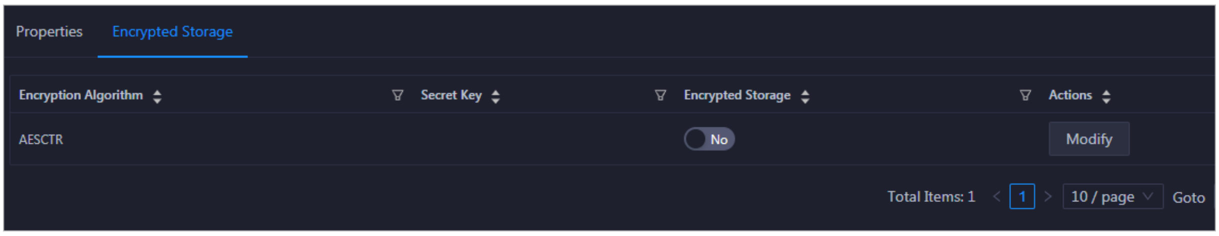
On the **Configuration** tab, you can configure the general, sandbox, SQL, MapReduce, access control, and resource recycling properties of the project. You can configure package-based authorization to allow access to the metadata warehouse.

On the **Properties** tab, you can view and modify each configuration item. Then, click **Submit**. To restore all configuration items to the default settings, click **Reset**.



	Configuration Items
+	Common
+	Sandbox
+	SQL
+	MR
+	restrictions
+	Recycle

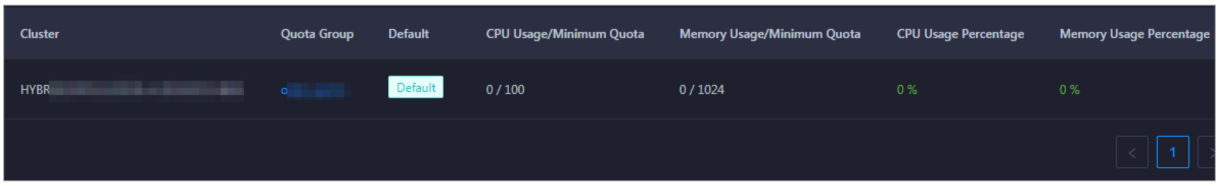
On the **Authorize Package for Metadata Repository** tab, you can install the package and perform package-based authorization.



Encryption Algorithm	Secret Key	Encrypted Storage	Actions
AESCTR		No	Modify

Quota Groups

On the **Quota Groups** tab, you can view the quota groups of a project and the details of each quota group.



Cluster	Quota Group	Default	CPU Usage/Minimum Quota	Memory Usage/Minimum Quota	CPU Usage Percentage	Memory Usage Percentage
HYBR[redacted]	o[redacted]	Default	0 / 100	0 / 1024	0 %	0 %

To view details about a quota group, click the quota group name in the **Quota** column. For more information, see Manage quota groups.

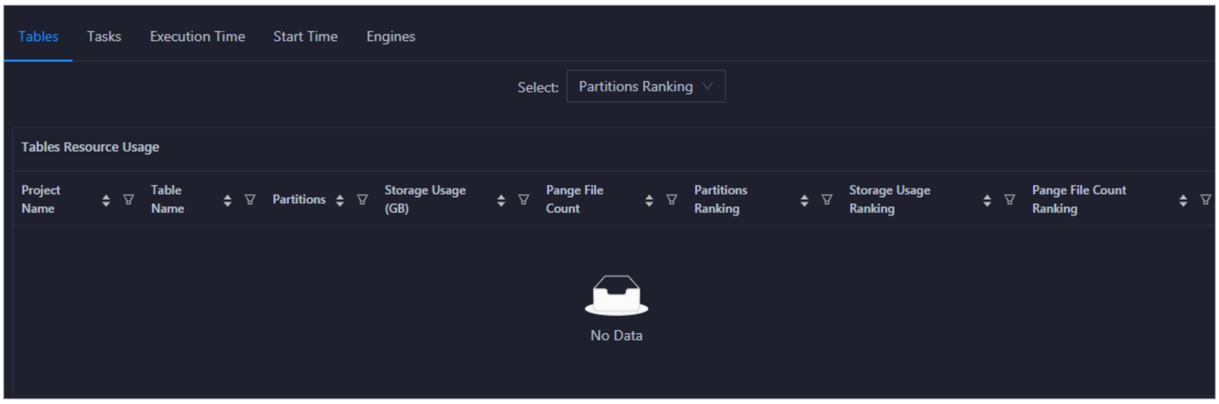
> **Note** The Quota Groups tab shows only information about computing resources. To query information about storage resources, go to the Storage tab.

Tunnel

On the **Tunnel** tab, you can view the tunnel throughput of the project in the unit of bytes per minute. The Tunnel Throughput (Bytes/Min) chart shows the trend lines of inbound and outbound traffic in different colors.

Resource Analysis

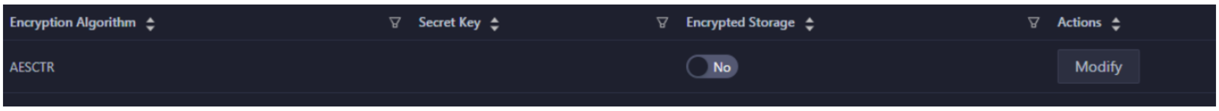
On the **Resource Analysis** tab, you can view the resource usage of the project from different dimensions, including tables, tasks, execution time, start time, and engines.



Project Name	Table Name	Partitions	Storage Usage (GB)	Pange File Count	Partitions Ranking	Storage Usage Ranking	Pange File Count Ranking

Encryption at Rest

On the **Encryption at Rest** tab, you can encrypt data by using the following encryption algorithms: AES-CTR, AES256, RC4, and SM4.



Encryption Algorithm	Secret Key	Encrypted Storage	Actions
AESCTR		No	Modify

Cross-cluster Replication

On the **Cross-cluster Replication** tab, you can view the projects that have the cross-cluster replication feature enabled and the details and status of cross-cluster replication.

When you deploy multiple clusters to use MaxCompute, MaxCompute projects may be mutually dependent. In this case, data may be directly read between projects. MaxCompute regularly scans tables or partitions that are directly read by other tables or partitions. If the duration of direct data reading reaches the specified threshold, MaxCompute adds the tables or partitions to the cross-cluster replication list.

Assume that Project1 in Cluster A depends on Table1 of Project2 in Custer B. In this case, Project1 directly reads data from Table1. If the duration of direct data reading reaches the specified threshold, MaxCompute adds Table1 to the cross-cluster replication list.

The **Cross-cluster Replication** tab consists of the **Replication Details** and **Replication Configuration** sub-tabs.

- Replication Details: shows information about the tables that support cross-cluster replication. The information includes the project name, cluster name, table name, partition, storage space, number of files, and cluster to which the data is synchronized.
- Replication Configuration: shows the configuration of the tables that support cross-cluster replication. The configuration includes the table name, priority, cluster to which the data is synchronized, and lifecycle. You can also view the progress of cross-cluster replication for a table.

11.2.5.2.2.3. Encrypt data

You can specify whether to encrypt the data stored in MaxCompute projects.

Prerequisites

If MaxCompute V3.8.0 or later is deployed, storage encryption is supported by default. If MaxCompute is upgraded to V3.8.0 or later, storage encryption is not supported by default. If you want to enable storage encryption, complete the configuration for your MaxCompute cluster.

Context

After storage encryption is enabled for a project, it cannot be disabled. After storage encryption is enabled, only the data that is newly written to the project is automatically encrypted. To encrypt historical data, you can create rules and configure tasks.

Before you encrypt historical data for a project, make sure that you understand the concepts of rules and tasks in Apsara Big Data Manager (ABM). A rule is used to specify the time period of historical data that you want to encrypt in a specific project. After you create a rule, the system obtains the data in the specified time period every day after the data is exported from the metadata warehouse. You can create only one rule every day. If multiple rules are created on a single day, only the latest rule takes effect. Each rule takes effect only once. You can create a key rotate task to encrypt the selected historical data.

Procedure

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Business** tab. In the left-side navigation pane, choose **Projects > Project List**.
4. On the **Project List** page, click the name of the required project to go to the project details page.
5. On the project details page, click the **Encryption at Rest** tab. The **Encrypt** tab appears.
6. Enable storage encryption.

   After storage encryption is enabled, all data that is newly written to the project is automatically encrypted.

   i. On the **Encrypt** tab, click **Modify** in the Actions column. In the **Configure Encrypted Storage** panel, specify **Encryption Algorithm**, **region**, and **project**.

      > **Note** AES-CTR, AES256, RC4, and SM4 encryption algorithms are supported.

   ii. Click **Run**.

      After storage encryption is enabled, the switch in the **Encrypted Storage** column is turned on.

7. To encrypt historical data or encrypted data, perform the following steps:

i. Create a rule.

On the **Create Rule** tab, click **OK** in the Actions column of a time period in the **Create Rule** section. In the Create Rule message, click **Run**. The new rule appears in the rule list.

The available time periods include **Last Three Months**, **Last Six Months**, **Three Months Ago**, **Six Months Ago**, and **All**.

ii. Create a key rotate task.

On the **Configure Task** tab, click **Add a key rotate task**. In the **Edit Key Rotate Task** panel, specify the required parameters and click **Run**.

Parameter	Description
Region	The region where the project whose data is to be encrypted resides. Select a region from the drop-down list.
Project Name	The name of the project whose data is to be encrypted.
Start Timestamp	The start time of the task.
Ended At	The end time of the task.
Priority	The priority of the task. A small value indicates a high priority.
Enabled	Specifies whether the task is enabled.
Bandwidth Limit	Specifies whether to limit the concurrency of merge tasks for the project. ■ **Yes**: indicates that merge tasks cannot be concurrently run. ■ **No**: indicates that merge tasks can be concurrently run.
Maximum Concurrent Tasks	The maximum number of merge tasks that can be run for the cluster of the selected project at the same time. This parameter is valid only when **Bandwidth Limit** is set to **No**.
Maximum Number of Running Jobs	The maximum number of jobs that can be run for the cluster of the selected project at the same time. This parameter is a global parameter. The jobs refer to all types of jobs in the cluster of the selected project, not only the merge tasks.

Parameter	Description

Merge Parameters	`{`
	`"odps.merge.cross.paths": "true",`
	`"odps.idata.useragent": "odps encrypt key rotate via force mergeTask",`
	`"odps.merge.max.filenumber.per.job": "10000000",`
	`"odps.merge.max.filenumber.per.instance": "10000",`
	`"odps.merge.failure.handling": "any",`
	`"odps.merge.maintain.order.flag": "true",`
	`"odps.merge.smallfile.filesize.threshold": "4096",`
	`"odps.merge.quickmerge.flag": "true",`
	`"odps.merge.maxmerged.filesize.threshold": "4096",`
	`"odps.merge.force.rewrite": "true",`
	`"odps.merge.restructure.action": "hardlink"`
	`}`

8. (Optional)View the history of data encryption in the project.

   On the **Historical Queries** tab, select a date from the **Date** drop-down list. Then, you can view information about storage encryption on the specified date.

11.2.5.2.2.4. Grant access permissions on the metadata warehouse

You can grant access permissions on the metadata warehouse to projects and project members.

Prerequisites

- If MaxCompute V3.8.1 or later is deployed, the package of the metadata warehouse is installed by default. In this case, you can directly use Apsara Big Data Manager (ABM) to grant access permissions on the metadata warehouse. If MaxCompute is upgraded to V3.8.1 or later, the package of the metadata warehouse is not installed by default. Before you grant access permissions on the metadata warehouse, you must manually install the package of the metadata warehouse.
- A project is created in DataWorks.

Context

To allow a project to access the metadata warehouse, grant the required permissions to the project and install the package to the project in the ABM console. When you install the package, ABM retrieves authentication information, such as the AccessKey pair, of the project from DataWorks. If the project is created in MaxCompute, an error message is returned during installation.

Procedure

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Business** tab. The **Project List** page appears by default.
4. Click the name of the required project to go to the project details page.
5. On the project details page, click the **Configuration** tab. Then, click the **Authorize Package for Metadata Repository** tab.
6. Click **Authorize** in the Actions column. In the **Authorize Package** message, click **Run**. A message appears, indicating that the permissions are granted.
7. Click **Install** in the Actions column. In the **Install Package** message, click **Run**. A message appears, indicating that the package is installed. After the package is installed, the switch in the **Authorized** column is turned on.

11.2.5.2.2.5. Perform disaster recovery

When a primary MaxCompute cluster fails, you can perform a primary/secondary switchover in the Apsara Big Data Manager (ABM) console to restore services. This topic describes the prerequisites and procedure of disaster recovery. In this topic, disaster recovery indicates zone-disaster recovery.

Prerequisites

- The resource replication feature is disabled in the ABM console. To disable the feature, perform the following steps:
  i. Log on to the ABM console.
  ii. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
  iii. In the left-side navigation pane of the **Business** tab, choose **Projects > Disaster Recovery**.
  iv. On the page that appears, turn off **Resource Synchronization Status**.
- The domain name of ABM is pointed to the IP address of the secondary ABM cluster. To point the domain name to the IP address, perform the following steps:
  i. Log on to the ABM console.
  ii. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
  iii. On the MaxCompute page, click **Management** in the top navigation bar. In the left-side navigation pane of the page that appears, click **Jobs**. The **Jobs** tab appears by default.
  iv. Find the Change Bcc Dns-Vip Relation For Disaster Recovery job and click **Run** in the Actions column. The **Job Properties** section appears.
  v. Click the ✎ icon next to Group Name to configure the IP address of the Docker container.

  > **Note** NewBccAGIp indicates the IP address of the Docker container under AG# for the bcc-saas service of the secondary ABM cluster. You must configure an IP address at the #Docker# level.

In the dialog box that appears, click the **Servers** tab. Enter the IP address of a server in the field and click **Add Server**. Then, click **OK**. The IP address is configured.

vi. In the upper-right corner, click **Run**. In the message that appears, click **Confirm**.

vii. On the page that appears, click **Start** in the upper-right corner. The switchover starts.

> ⓘ Note If a step fails, click **Retry**. After all the steps are complete, the domain name of ABM is pointed to the IP address of the secondary ABM cluster.

- The secondary ABM cluster page is accessible. If this page is inaccessible, go to the */usr/loca/bigdatak/controllers/bcc/tool/disaster_recovery* directory of the Docker container in bcc-saa.AG# of the secondary ABM cluster. Then, run the `/home/tops/bin/python change_dns_vip.py` script in the directory. If job_success appears, the execution succeeds. Then, run the `/home/tops/bin/python disaster_init.py` script in the current directory. If job_success appears, the execution succeeds. After the scripts are successfully run, you can go to the secondary cluster page.

  > ⓘ Note If an exception occurs when you run the scripts, click **Retry**.

- The Business Continuity Management Center (BCMC) switchover of MaxCompute is complete. The services on which MaxCompute depends are running normally. The services include AAS, Tablestore, and MiniRDS.
- By default, the data synchronization feature is disabled for MaxCompute projects because the computing and storage resources of the primary and secondary data centers are limited. To enable the data synchronization feature, submit a ticket.

Context

Pay attention to the following points for a disaster recovery switchover:

- By default, the logon to Apsara Big Data Manager depends on the Apsara Uni-manager Operations Console. If the Apsara Uni-manager Operations Console has not reached the desired state, single sign-on is not supported. In this case, go to the */usr/loca/bigdatak/controllers/bcc/tool/disaster_recovery* directory of the Docker container in bcc-saa.AG#. Then, run `change_login_by_bcc.sh` to switch the logon mode to the mode that is independent of the Apsara Uni-manager Operations Console. After the Apsara Uni-manager Operations Console has reached the desired state, run `change_login_by_aso.sh` to switch the logon mode back to the mode that depends on the Apsara Uni-manager Operations Console.
- An exception may occur in each step of the switchover process. If an exception occurs, click **Retry**. If the retry succeeds, proceed to the next step. If the exception persists after multiple retries, contact O&M engineers to perform troubleshooting. Then, click **Retry** to complete the step.
- For each switchover, the Apsara distributed operating system of the original primary MaxCompute cluster must be restarted. Otherwise, the admintask service may be faulty after the switchover is complete.
- In the Collect Unsynchronized Data step, an exception shown in the following figure may occur. If this occurs, click **Recollect Unsynchronized Data**.

Procedure

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.

3. In the left-side navigation pane of the **Business** tab, choose **Projects** > **Disaster Recovery**.
4. In the upper-right corner, click **Switchover Process** to start the disaster recovery process.
5. Wait for resource replication to automatically stop.

   Wait for resource replication to automatically stop. After **Next** becomes blue, click **Next**.

   > ? **Note** If an error occurs, click **Retry**. If the retry is invalid, contact O&M engineers to perform troubleshooting and try again.

6. Switch control clusters.
   1. Wait for the primary/secondary switchover to complete for control clusters.

      > ? **Note** After the original primary cluster becomes the secondary cluster, the switchover is complete.

   2. Click **Restart Standby Cluster**.

      > ? **Note** The MaxCompute clusters become abnormal.

   3. After the MaxCompute clusters become normal, click **Restart Frontend Server** and wait until the restart result is returned.
   4. After the restart succeeds, click **Test adminTask**.

      > ? **Note** If an exception occurs, click **Retry** and then **Test adminTask**. Alternatively, repeat from Step 6.b.

   5. After **Next** becomes blue, click **Next**.

      > ? **Note** The Switching message remains displayed until the test succeeds.

7. Switch computing clusters.

   The computing cluster switchover automatically starts for the projects that have two computing clusters. The switchover cannot be performed for the projects that have only one computing cluster. After the switchovers are complete for all the projects, click **Next**.

   > ? **Note** If the computing clusters of a project fail to be switched, contact O&M engineers to identify the cause of the exception. If the exception can be fixed, fix it and click **Retry** to continue the switchover. If the project is damaged or does not need a cluster switchover, click **Next** after you confirm that computing clusters of other projects are switched.

8. Switch the replication service to the secondary clusters.

   The script is automatically run at the background. When a success message appears, click **Next**.

9. Collect unsynchronized data.

i. Wait for the system to collect statistics on projects that contain unsynchronized data.

> **Note** This step requires a long time to complete. The specific time depends on the data volume.

ii. After the collection is complete, click **Download Unsynchronized Data of Selected Projects** to download the unsynchronized data to your computer.

> **Note** The unsynchronized data that is obtained from this step is required for the Manually Fill in Missing Data step. The projects that are obtained from this step must be the same as those for the Repair Metadata and Manually Fill in Missing Data steps.

iii. After the unsynchronized data is downloaded, verify the data and click **Next**. If all data is synchronized, click **Next**.

> **Note** If the unsynchronized data is abnormal, you can click **Recollect Unsynchronized Data**.

10. Repair metadata.

    Select all projects, click **Repair Metadata of Selected Projects**, and then wait for results. If the metadata of some projects fails to be repaired, click **Download Last Execution Log** and send the logs to O&M engineers. The logs can be used to identify and analyze the cause of the exception. After the exception is fixed, repair the metadata of the projects again. If you do not need to repair the metadata of all projects, click **Next** after the metadata of required projects is repaired.

11. Manually supplement missing data.

    Use DataWorks or the odpscmd client to manually supplement the missing data based on the unsynchronized data that you downloaded. After you supplement the missing data, select all projects and click **Confirm Data Repair Complete**. Then, click **Next**.

12. Repair unsynchronized resources.

    i. Wait for the system to collect statistics on projects that contain unsynchronized resources.

    > **Note** This step requires a long time to complete. The specific time depends on the data volume.

    ii. Use DataWorks or the odpscmd client to manually supplement the missing resources based on the unsynchronized resources that you collected. If an exception occurs, send exception information to O&M engineers to perform troubleshooting. After all the project resources are repaired, click **Complete and Next**.

13. Wait for resource replication to automatically start.

    Wait for resource replication to automatically start. After **Next** becomes blue, click **Next**.

14. Exit the configuration wizard.

    After the switchover is complete, click **Back** to exit the wizard.

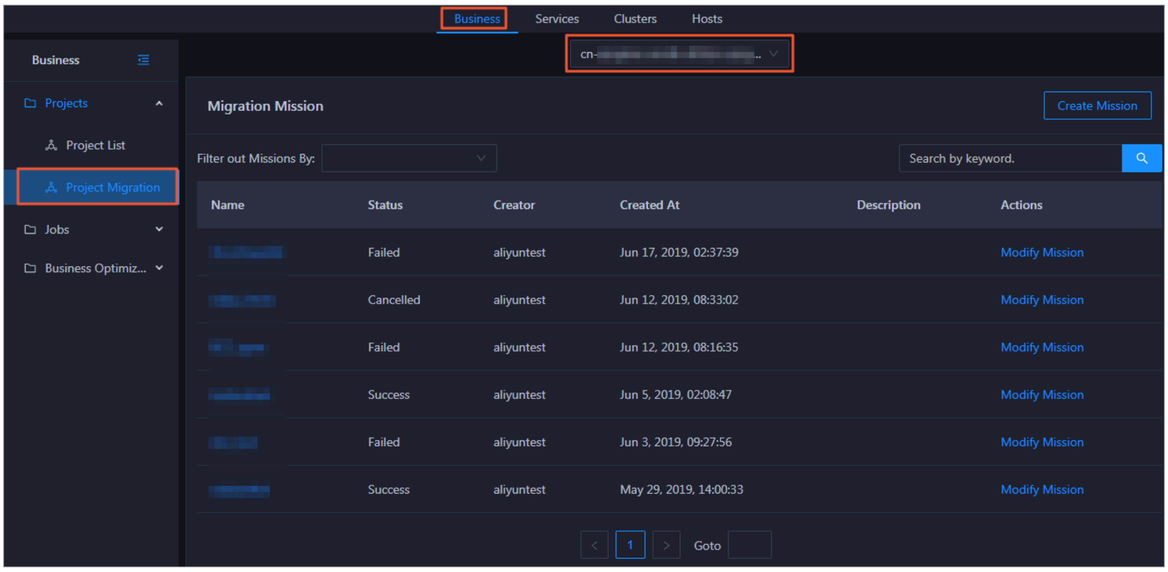
11.2.5.2.2.6. Migrate projects

Apsara Big Data Manager (ABM) allows you to migrate MaxCompute projects across regions from one cluster to another. This allows you to balance the computing and storage resources of each cluster.

> **Note** The project migration feature is supported only when the clusters are deployed in multi-region mode.

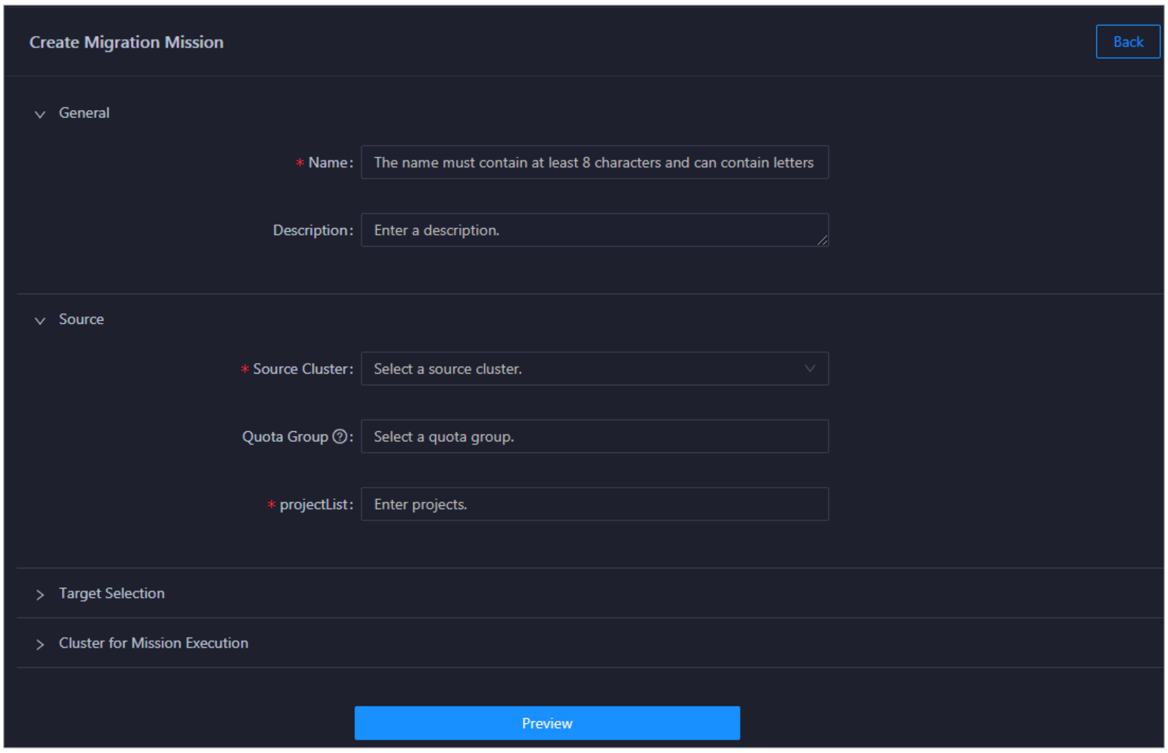
Create a project migration task

1. In the left-side navigation pane of the **Business** tab, choose **Projects > Project Migration**.
2. In the upper part of the **Migration Mission** page, select the region where the project resides.



Name	Status	Creator	Created At	Description	Actions
[redacted]	Failed	aliyuntest	Jun 17, 2019, 02:37:39		Modify Mission
[redacted]	Cancelled	aliyuntest	Jun 12, 2019, 08:33:02		Modify Mission
[redacted]	Failed	aliyuntest	Jun 12, 2019, 08:16:35		Modify Mission
[redacted]	Success	aliyuntest	Jun 5, 2019, 02:08:47		Modify Mission
[redacted]	Failed	aliyuntest	Jun 3, 2019, 09:27:56		Modify Mission
[redacted]	Success	aliyuntest	May 29, 2019, 14:00:33		Modify Mission

3. In the upper-right corner, click **Create Mission**. On the page that appears, specify the parameters in the **General**, **Source**, **Target Selection**, and **Cluster for Mission Execution** sections as prompted.



Create Migration Mission

Back

General

* Name: The name must contain at least 8 characters and can contain letters

Description: Enter a description.

Source

* Source Cluster: Select a source cluster.

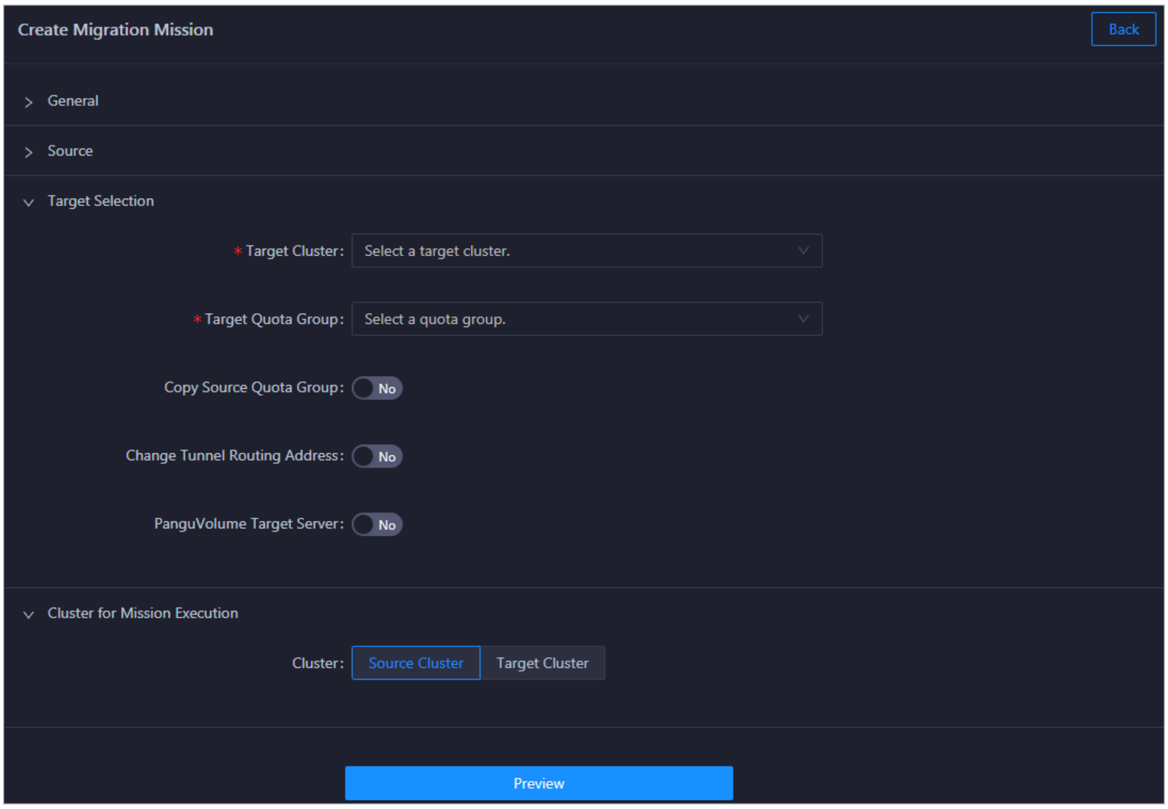
Quota Group ⓘ: Select a quota group.

* projectList: Enter projects.

Target Selection

Cluster for Mission Execution

Preview



Create Migration Mission

Back

General

Source

Target Selection

* Target Cluster: Select a target cluster.

* Target Quota Group: Select a quota group.

Copy Source Quota Group: No

Change Tunnel Routing Address: No

PanguVolume Target Server: No

Cluster for Mission Execution

Cluster: Source Cluster | Target Cluster

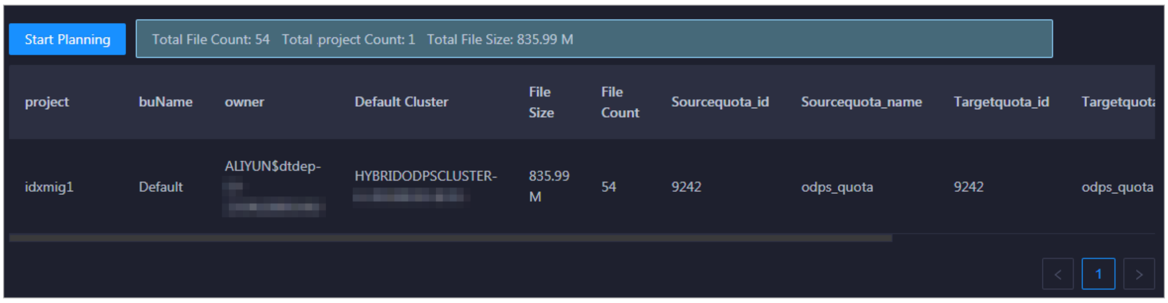
Preview

The following table describes the required parameters.

Section	Parameter	Description
	Source Cluster	The name of the source cluster. Select a cluster from the drop-down list.

Section	Parameter	Description
Source	**Quota Group**	The quota group of the source cluster. Select a quota group from the drop-down list.
	projectList	The projects that you want to migrate. After **Quota Group** is specified, all the projects in the quota group are automatically loaded. You can migrate these projects at a time. If some projects in the quota group do not need to be migrated, you can remove the projects.
Target Selection	**Copy Source Quota Group**	Specifies whether the destination cluster uses the same quota group as the source cluster. If you enable this feature, the **Target Quota Group** parameter cannot be specified.
	Change Tunnel Routing Address	Specifies whether to use a new Tunnel route. Tunnel provides highly concurrent upload and download services for offline data. Each project has a default Tunnel route. If you want to use a new Tunnel route after a project is migrated to a new cluster, enable **Change Tunnel Routing Address** and specify the new Tunnel route.
	PanguVolume Target Server	Specifies whether the destination Apsara Distributed File System volume can be specified. Cross-volume project migration is not supported. Set this parameter to **No**.
Cluster for Mission Execution	**Cluster**	○ **Source Cluster**: indicates that the source cluster pushes the project to the destination cluster. ○ **Target Cluster**: indicates that the destination cluster pulls the project from the source cluster.

4. Click **Preview** to preview project migration details.

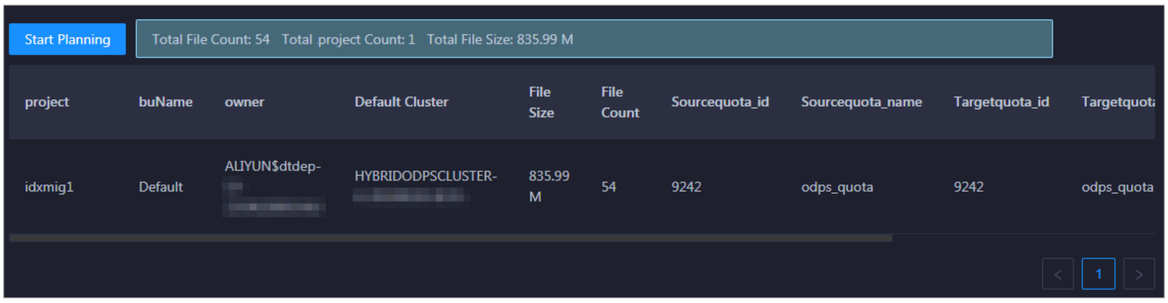


Total File Count: 54 Total project Count: 1 Total File Size: 835.99 M

project	buName	owner	Default Cluster	File Size	File Count	Sourcequota_id	Sourcequota_name	Targetquota_id	Targetquot:
idxmig1	Default	ALIYUN$dtdep-[redacted]	HYBRIDODPSCLUSTER-[redacted]	835.99 M	54	9242	odps_quota	9242	odps_quota

5. After you confirm the configuration, click **Start Planning** in the upper-left corner. A project migration task is generated. The migration details appear.

   It requires some time to generate the task.



Total File Count: 54 Total .project Count: 1 Total File Size: 835.99 M

project	buName	owner	Default Cluster	File Size	File Count	Sourcequota_id	Sourcequota_name	Targetquota_id	Targetquot
idxmig1	Default	ALIYUN$dtdep-[redacted]	HYBRIDODPSCLUSTER-[redacted]	835.99 M	54	9242	odps_quota	9242	odps_quota

A standard project migration task generally includes five steps:

i. **Add Target Cluster**: Add the destination cluster to the cluster list of the project that you want to migrate.

ii. **Start to Replicate**: Replicate the project from the source cluster to the destination cluster.

iii. **Switch Default Cluster**: Change the default cluster of the project to the destination cluster. After the default cluster is changed, generated data is written to the destination cluster.

iv. **Clear Replication**: Clear the data replication list. During project migration, the migrated project in the source cluster and the corresponding project in the destination cluster synchronize data based on the data replication list. This ensures data consistency between the two projects. Data is continuously synchronized until the data replication list is cleared.

v. **Remove Source Cluster**: Delete the migrated project from the source cluster.

For more information about how to modify a task after it is generated, see Modify a project migration task.

Run the project migration task

After the project migration task is created, you can run the task on the **Migration Details** page.

1. Click the task name in the task list to go to the **Migration Details** page.
2. On the **Migration Details** page, click **Submit for Execution**.

   After the project migration task starts, the system automatically runs the **Add Target Cluster** and **Start to Replicate** steps in sequence.

   If you migrate multiple projects at a time, the process requires many steps to complete. Therefore, we recommend that you sort the steps by project to view the migration steps for each project. If the status of a step is **Success**, the step is complete. If the status of a step is **Failed**, the step fails.

   In the migration process, some steps can be run only after you click **OK**. If you do not need to run a step, click **Skip**. To confirm or skip multiple steps at a time, select the steps and click **OK** or **Skip** in the upper-left corner.

   You can also click the status of a migration step for a project. In the dialog box that appears, click **Yes** to skip the remaining steps.
3. When the **Start to Replicate** step is complete, check the difference in data volumes between the migrated project in the source cluster and the corresponding project in the destination cluster.

   > Notice We recommend that you run the next step only when the difference in data volumes does not exceed 5%.

To check the data volume of a project, log on to the admingateway host in the cluster where the project resides and run the **pu dirmeta /product/aliyun/odps/${project_name}/** command.

4. If the difference in data volumes does not exceed 5%, perform one of the following operations:
   - Change the default cluster: Click **OK** in the Actions column of the **Switch Default Cluster** step. After this operation, the destination cluster becomes the default cluster of the migrated project. The default cluster is changed in this example.
   - Do not change the default cluster: Click **Skip** in the Actions column of the **Switch Default Cluster** step. After this operation, the source cluster is still used as the default cluster of the project.

   After the default cluster is changed, generated data is written to the destination cluster.

   > **Warning** During project migration, the migrated project in the source cluster and the corresponding project in the destination cluster synchronize data based on the data replication list to ensure data consistency. It requires some time for data synchronization to complete. Therefore, after the default cluster is changed, we recommend that you wait for about one week before you proceed to the next step.

5. Wait for about one week and check whether the data volume of the migrated project in the source cluster is the same as that of the corresponding project in the destination cluster.

   To check the data volume of a project, log on to the admingateway host in the cluster where the project resides and run the **pu dirmeta /product/aliyun/odps/${project_name}/** command.

   > **Warning** Before you proceed to the next step, make sure that the data volume of the migrated project in the source cluster is the same as that of the corresponding project in the destination cluster. Otherwise, data may be lost.

6. To retain the migrated project in the source cluster, click **Skip** in the Actions column of the **Remove Source Cluster** step before you perform the **Clear Replication** step.
7. After the data volume of the migrated project in the source cluster becomes the same as that of the project in the destination cluster, click **OK** in the Actions column of the **Clear Replication** step to clear the data replication list.

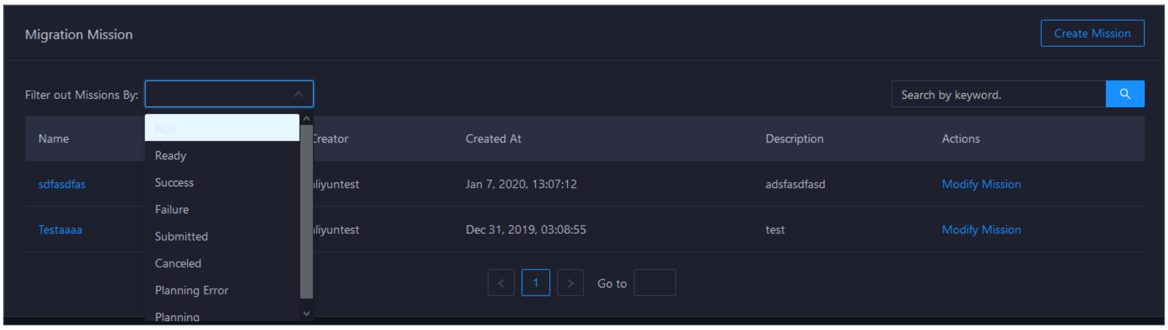
   After the data replication list is cleared, data is no longer synchronized between the migrated project in the source cluster and the corresponding project in the destination cluster.

   The system automatically runs the **Remove Source Cluster** step to delete all migrated projects from the source cluster. This releases storage and computing resources.

View migration details

You can view the details of a project migration task, including the steps, results, and debugging information.

1. If multiple migration tasks exist, search for a task or filter tasks on the **Migration Mission** page.
   - Filter tasks: Select a task state from the **Filter out Mission By** drop-down list. All tasks in this state are automatically filtered from the migration task list.
   - Search for a task: Enter the name of a migration task in the search box in the upper-right corner and click the search icon to search for the task.



Migration Mission

Create Mission

Filter out Missions By:

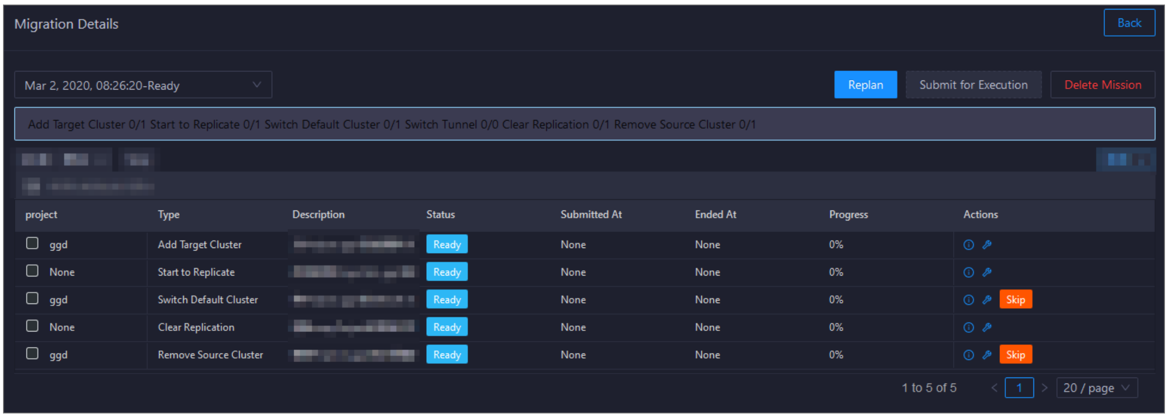
Null
Ready
Success
Failure
Submitted
Canceled
Planning Error
Planning

Search by keyword.

Name	Creator	Created At	Description	Actions
sdfasdfas	aliyuntest	Jan 7, 2020, 13:07:12	adsfasdfasd	Modify Mission
Testaaaa	aliyuntest	Dec 31, 2019, 03:08:55	test	Modify Mission

1 Go to

2. Click the name of a task. On the **Migration Details** page, view the details of the task.



Migration Details

Back

Mar 2, 2020, 08:26:20-Ready

Replan Submit for Execution Delete Mission

Add Target Cluster 0/1 Start to Replicate 0/1 Switch Default Cluster 0/1 Switch Tunnel 0/0 Clear Replication 0/1 Remove Source Cluster 0/1

[redacted]

project	Type	Description	Status	Submitted At	Ended At	Progress	Actions
□ ggd	Add Target Cluster	[redacted]	Ready	None	None	0%	
□ None	Start to Replicate	[redacted]	Ready	None	None	0%	
□ ggd	Switch Default Cluster	[redacted]	Ready	None	None	0%	Skip
□ None	Clear Replication	[redacted]	Ready	None	None	0%	
□ ggd	Remove Source Cluster	[redacted]	Ready	None	None	0%	Skip

1 to 5 of 5 1 20 / page

3. If a step fails, click the **Details** or **Debugging** icon in the Actions column to view the details or debugging information of the step. This allows you to identify the cause of the failure.
4. Perform other required operations.

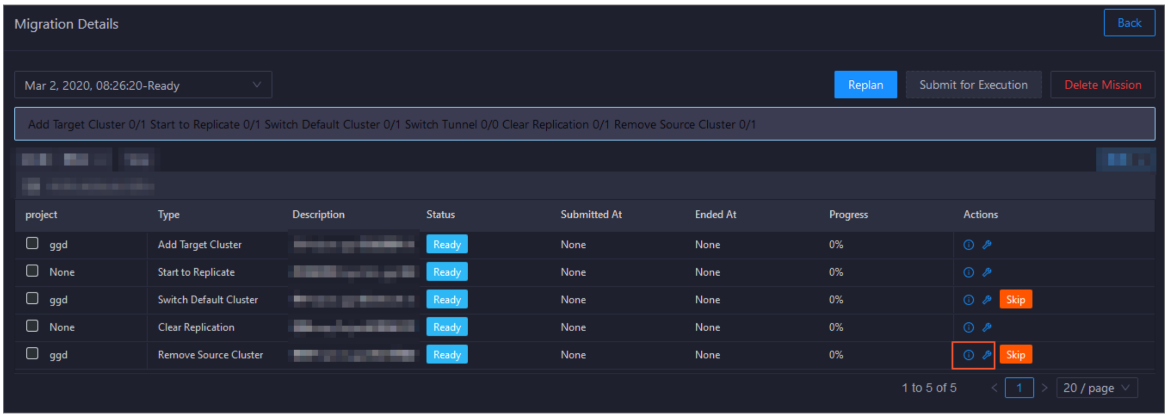
   Click **Menu** in the upper-right corner. You can export the step list, change the column width to automatically fit the content, or customize whether to show or hide a column.

   You can also right-click a cell in the step list and copy the cell content.

View step details and debugging information

If a step fails, you can view the step details and debugging information to identify the cause of the failure.

1. Find the step that fails to run during the migration of a project.



Migration Details

Back

Mar 2, 2020, 08:26:20-Ready

Replan Submit for Execution Delete Mission

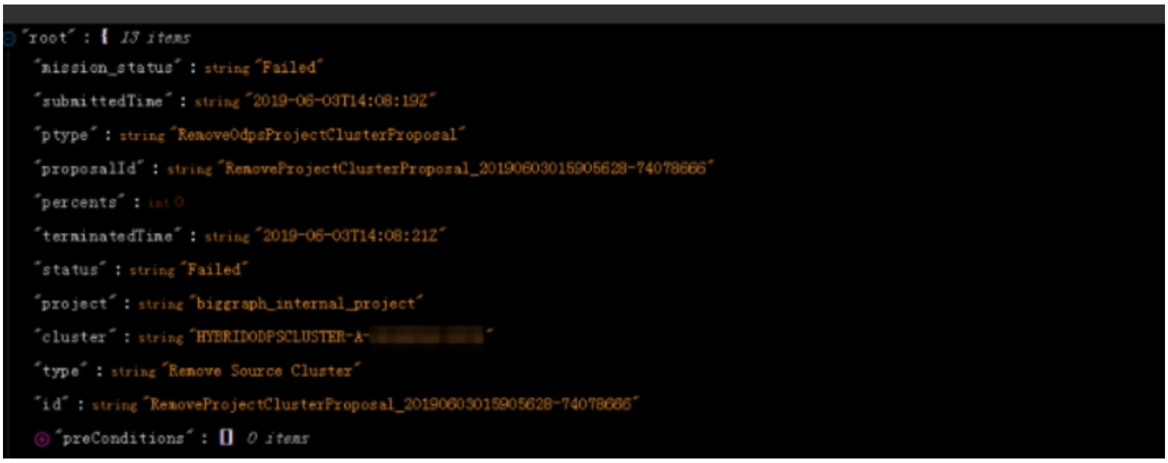
Add Target Cluster 0/1 Start to Replicate 0/1 Switch Default Cluster 0/1 Switch Tunnel 0/0 Clear Replication 0/1 Remove Source Cluster 0/1

[redacted]

project	Type	Description	Status	Submitted At	Ended At	Progress	Actions
□ ggd	Add Target Cluster	[redacted]	Ready	None	None	0%	
□ None	Start to Replicate	[redacted]	Ready	None	None	0%	
□ ggd	Switch Default Cluster	[redacted]	Ready	None	None	0%	Skip
□ None	Clear Replication	[redacted]	Ready	None	None	0%	
□ ggd	Remove Source Cluster	[redacted]	Ready	None	None	0%	Skip

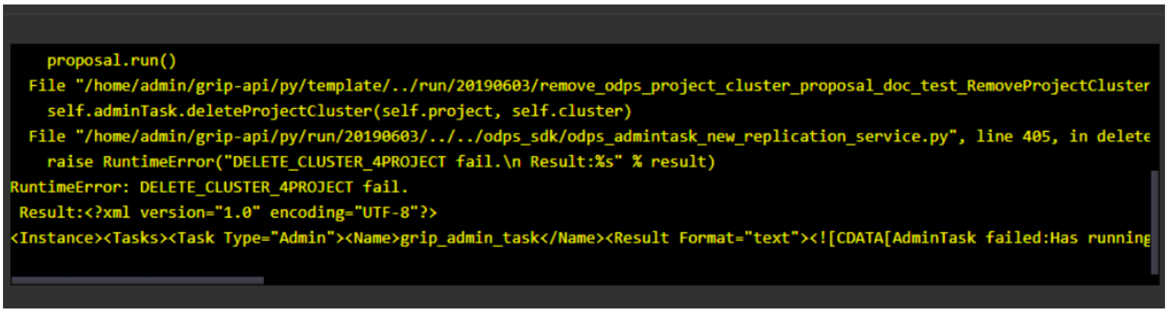
1 to 5 of 5 1 20 / page

2. Click the **Details** icon in the Actions column to view the details of the step.



```
"root" : { 13 items
  "mission_status" : string "Failed"
  "submittedTime" : string "2019-06-03T14:08:19Z"
  "ptype" : string "RemoveOdpsProjectClusterProposal"
  "proposalId" : string "RemoveProjectClusterProposal_20190603015905628-74078666"
  "percents" : int 0
  "terminatedTime" : string "2019-06-03T14:08:21Z"
  "status" : string "Failed"
  "project" : string "biggraph_internal_project"
  "cluster" : string "HYBRIDODPSCLUSTER-A-[redacted]"
  "type" : string "Remove Source Cluster"
  "id" : string "RemoveProjectClusterProposal_20190603015905628-74078666"
  "preConditions" : [] 0 items
```

3. Click the **Debugging** icon in the Actions column to view the debugging information of the step.



```
    proposal.run()
  File "/home/admin/grip-api/py/template/../run/20190603/remove_odps_project_cluster_proposal_doc_test_RemoveProjectCluster
    self.adminTask.deleteProjectCluster(self.project, self.cluster)
  File "/home/admin/grip-api/py/run/20190603/../../odps_sdk/odps_admintask_new_replication_service.py", line 405, in delete
    raise RuntimeError("DELETE_CLUSTER_4PROJECT fail.\n Result:%s" % result)
RuntimeError: DELETE_CLUSTER_4PROJECT fail.
 Result:<?xml version="1.0" encoding="UTF-8"?>
<Instance><Tasks><Task Type="Admin"><Name>grip_admin_task</Name><Result Format="text"><![CDATA[AdminTask failed:Has running
```

Modify a project migration task

After a project migration task is created, you can modify the task if the task does not meet your requirements.

To modify the task, find the required task, click **Modify Mission** in the Actions column, or click **Replan** on the **Migration Details** page.

11.2.5.2.3. Manage quota groups

Apsara Big Data Manager (ABM) shows the quota groups of all projects in a MaxCompute cluster. It allows you to create and modify quota groups. You can also view details about quota groups and enable period management for quota groups.

Go to the Quota Groups page

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Business** tab. In the left-side navigation pane of the tab that appears, click **Quota Groups**. Then, click **Quota Groups** or **Periods** as required.

Create a quota group

In the upper-right corner of the **Quota Groups** page, click **Create Quota Group**. In the panel that appears, configure the parameters and click **Run**.

Parameter	Description
Cluster	The cluster of the quota group that you want to create.
Quota Group	The name of the quota group that you want to create.
Preemption Policy	The preemption policy of the quota group. Valid values: No Preemption and Preemption. Default value: No Preemption.
Scheduling Type	The type of resource scheduling. Valid values: First In, First Out and Average. Default value: First In, First Out.
Minimum CUs	The minimum number of compute units (CUs) that are provided by the quota group.
Maximum CUs	The maximum number of CUs that are provided by the quota group.
CPU-to-Memory Ratio	The ratio of CPUs to memory of hosts in the quota group.

Modify a quota group

On the **Quota Groups** page, find the quota group that you want to modify and click **Modify** in the Actions column. In the panel that appears, modify the settings and click **Run**.

> ? **Note** If period management has been enabled for the quota group you want to modify, first modify the period management configuration.

View details about a quota group

On the **Quota Groups** page, find the quota group whose details you want to view and click **Details** in the Actions column. Then, you can view information about the resource usage, resource analysis, and period management of the quota group.

Enable period management for a quota group

1. On the **Periods** page, find the quota group for which you want to enable period management and click **Period Management** in the Actions column.
2. On the **Period Management** tab, click **Set Periods**. In the dialog box that appears, set Period and click **Enable Period Management**.

   > ? **Note**
   >
   > - You can click **Add** to specify more than one period and **Delete** to delete a period.
   > - For the quota group that has period management enabled, click **Edit** in the Actions column. In the **Modify Period Configuration** panel, you can modify the parameters of the quota group within the specified period.

3. To disable period management for a quota group, click **Set Periods** again. In the dialog box that appears, click **Disable Period Management**.

11.2.5.2.4. Job management

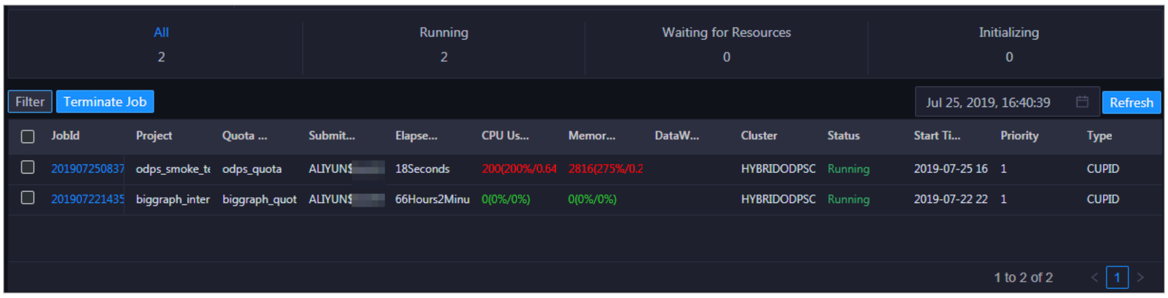
11.2.5.2.4.1. Job snapshots

The job snapshots feature allows you to manage the tasks that are created in MaxCompute and the merge tasks that are created in Apsara Big Data Manager (ABM). You can also view Logview information about jobs, terminate jobs, and collect job logs.

View job snapshots

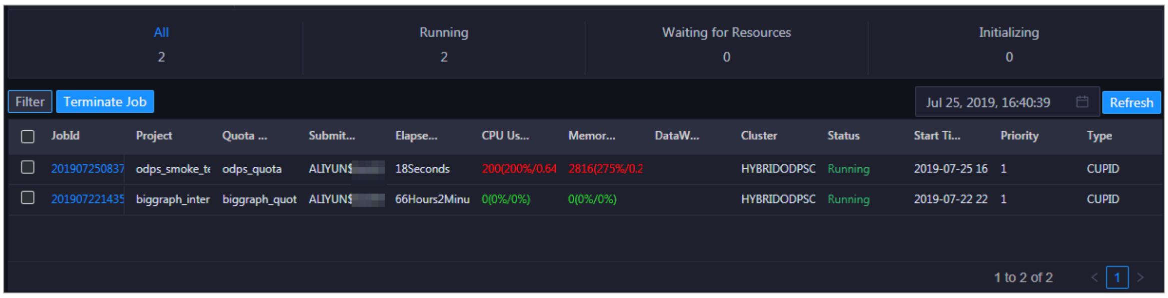
You can view job snapshots by day in the last week. The information about a job snapshot includes the job ID, project, quota group, submitter, running duration, minimum CPU utilization, and maximum CPU utilization. It also includes the minimum memory usage, maximum memory usage, DataWorks node, running status, start time, priority, and type. You can also view the operational logs of a job to identify job failures.

1. In the left-side navigation pane of the **Business** tab, choose **Jobs > Job Snapshots**. The **Job Snapshots** page appears.



□	JobId	Project	Quota ...	Submit...	Elapse...	CPU Us...	Memor...	DataW...	Cluster	Status	Start Ti...	Priority	Type
□	201907250837	odps_smoke_t	odps_quota	ALIYUN$[redacted]	18Seconds	200(200%/0.64	2816(275%/0.2		HYBRIDODPSC	Running	2019-07-25 16	1	CUPID
□	201907221435	biggraph_inter	biggraph_quot	ALIYUN$[redacted]	66Hours2Minu	0(0%/0%)	0(0%/0%)		HYBRIDODPSC	Running	2019-07-22 22	1	CUPID

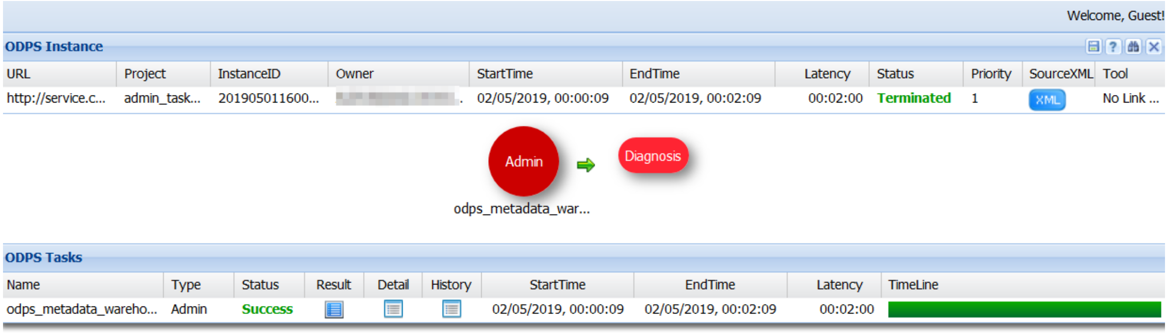
2. In the upper-right corner, select the date and time to view job snapshots by day.



□	JobId	Project	Quota ...	Submit...	Elapse...	CPU Us...	Memor...	DataW...	Cluster	Status	Start Ti...	Priority	Type
□	201907250837	odps_smoke_t	odps_quota	ALIYUN$[redacted]	18Seconds	200(200%/0.64	2816(275%/0.2		HYBRIDODPSC	Running	2019-07-25 16	1	CUPID
□	201907221435	biggraph_inter	biggraph_quot	ALIYUN$[redacted]	66Hours2Minu	0(0%/0%)	0(0%/0%)		HYBRIDODPSC	Running	2019-07-22 22	1	CUPID

3. Click **All**, **Running**, **Waiting for Resources**, or **Initializing** to view job snapshots on the specified date.

4. Find the required snapshot and click **Logview** in the Actions column. In the dialog box that appears, click **Run** to view Logview information about the job.



Welcome, Guest!

ODPS Instance

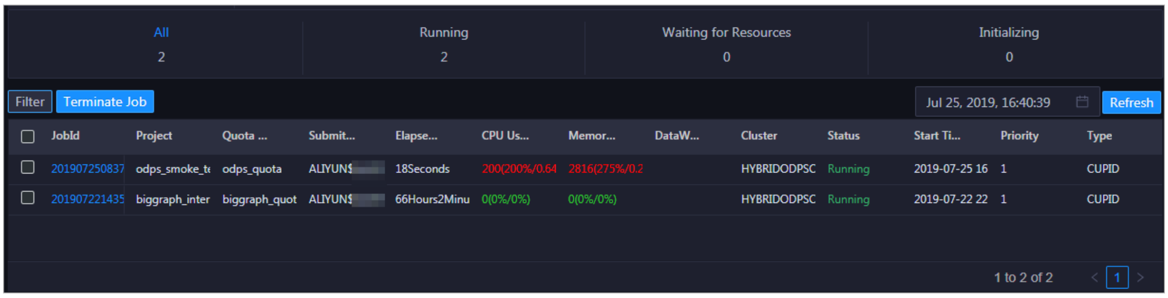
URL	Project	InstanceID	Owner	StartTime	EndTime	Latency	Status	Priority	SourceXML	Tool
http://service.c...	admin_task...	201905011600...	[redacted]	02/05/2019, 00:00:09	02/05/2019, 00:02:09	00:02:00	Terminated	1	XML	No Link ...

ODPS Tasks

Name	Type	Status	Result	Detail	History	StartTime	EndTime	Latency	TimeLine
odps_metadata_wareho...	Admin	Success	▤	▤	▤	02/05/2019, 00:00:09	02/05/2019, 00:02:09	00:02:00	🟩

Terminate jobs

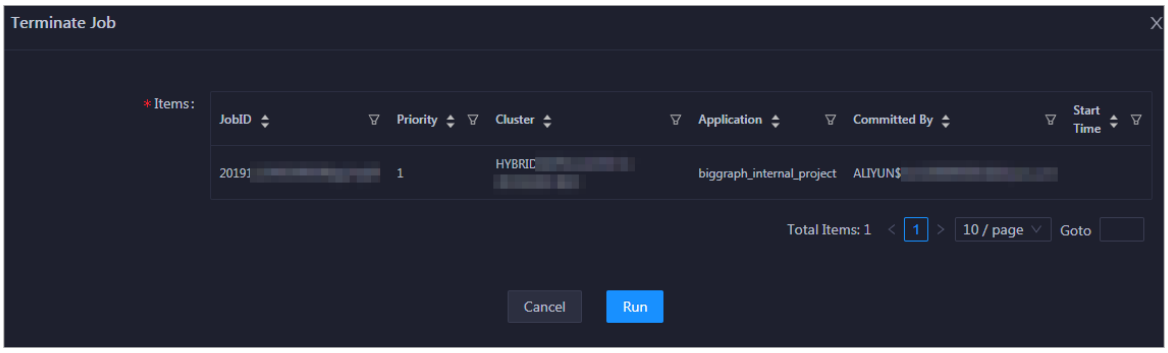
1. In the left-side navigation pane of the **Business** tab, choose **Jobs** > **Job Snapshots**. The **Job Snapshots** page appears.



All	Running	Waiting for Resources	Initializing
2	2	0	0

□	JobId	Project	Quota ...	Submit...	Elapse...	CPU Us...	Memor...	DataW...	Cluster	Status	Start Ti...	Priority	Type
□	201907250837	odps_smoke_te	odps_quota	ALIYUN$[redacted]	18Seconds	200(200%/0.64	2816(275%/0.2		HYBRIDODPSC	Running	2019-07-25 16	1	CUPID
□	201907221435	biggraph_inter	biggraph_quot	ALIYUN$[redacted]	66Hours2Minu	0(0%/0%)	0(0%/0%)		HYBRIDODPSC	Running	2019-07-22 22	1	CUPID

2. Select one or more jobs and click **Terminate Job** above the snapshot list. In the panel that appears, view information about the job or jobs that you want to terminate.

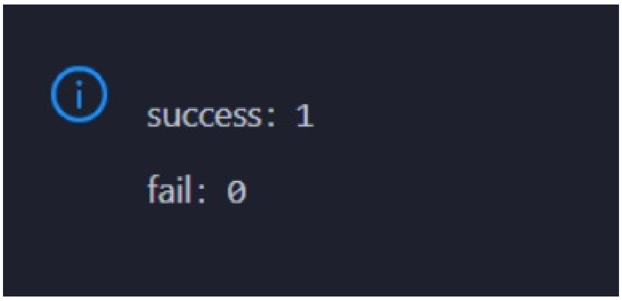


Terminate Job

* Items:

JobID	Priority	Cluster	Application	Committed By	Start Time
20191[redacted]	1	HYBRID[redacted]	biggraph_internal_project	ALIYUN$[redacted]	

3. Click **Run**. A message appears, indicating the running result.



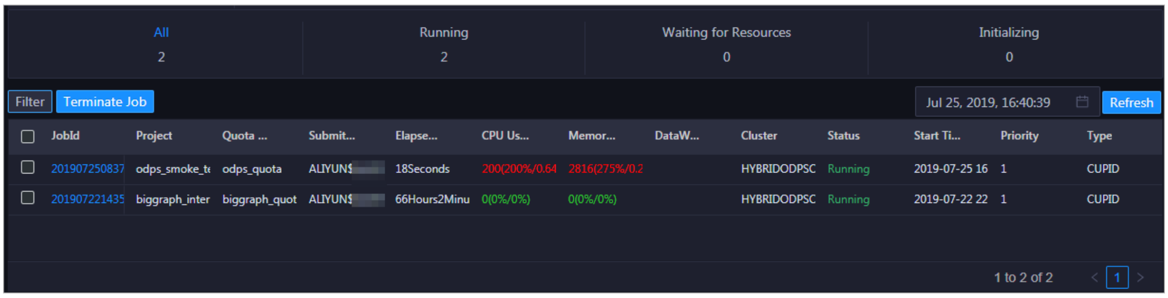
```
success: 1
fail: 0
```

Collect job logs

If an exception occurs during job running, you can collect job logs to identify and analyze the exception.

1. In the left-side navigation pane of the **Business** tab, choose **Jobs** > **Job Snapshots**. The **Job**

Snapshots page appears.



All	Running	Waiting for Resources	Initializing
2	2	0	0

□	JobId	Project	Quota ...	Submit...	Elapse...	CPU Us...	Memor...	DataW...	Cluster	Status	Start Ti...	Priority	Type
□	201907250837	odps_smoke_t	odps_quota	ALIYUN$[redacted]	18Seconds	200(200%/0.64	2816(275%/0.2		HYBRIDODPSC	Running	2019-07-25 16	1	CUPID
□	201907221435	biggraph_inter	biggraph_quot	ALIYUN$[redacted]	66Hours2Minu	0(0%/0%)	0(0%/0%)		HYBRIDODPSC	Running	2019-07-22 22	1	CUPID

2. In the upper-right corner of the **Job Snapshots** page, choose **Actions > Collect Job Logs**.
3. In the **Collect Job Logs** panel, configure the parameters.

   The following table describes the parameters.

Parameter	Description
Target Service	The service from which you want to collect job logs.
instanceid	Optional. The ID of the job instance.
requestid	Optional. The request ID returned when the job fails. If the value you specify is not a request ID, job logs that contain the specified value are collected.
Time Period	The time period to collect job logs.
Time Interval	Optional. The time interval to collect job logs. Unit: hours.
Degree of Concurrency	The maximum number of nodes from which you can collect job logs at the same time.

4. Click **Run** to start job log collection.
5. View the execution status and progress of job log collection.

   In the upper-right corner of the **Job Snapshots** page, click **Actions** and select **Execution History** next to **Collect Job Logs**. In the **Execution History** panel, view the execution status and history of job log collection.

   RUNNING indicates that the execution is in progress. SUCCESS indicates that the execution succeeds. FAILED indicates that the execution fails. If the status is RUNNING, click **Details** in the Actions column of a task to view the execution progress.
6. View the path to store job logs.

   In the **Execution History** panel, click **Details** in the Details column of an execution record to view the details. In the Steps section, view the path to store the job logs.

11.2.5.2.5. Business optimization

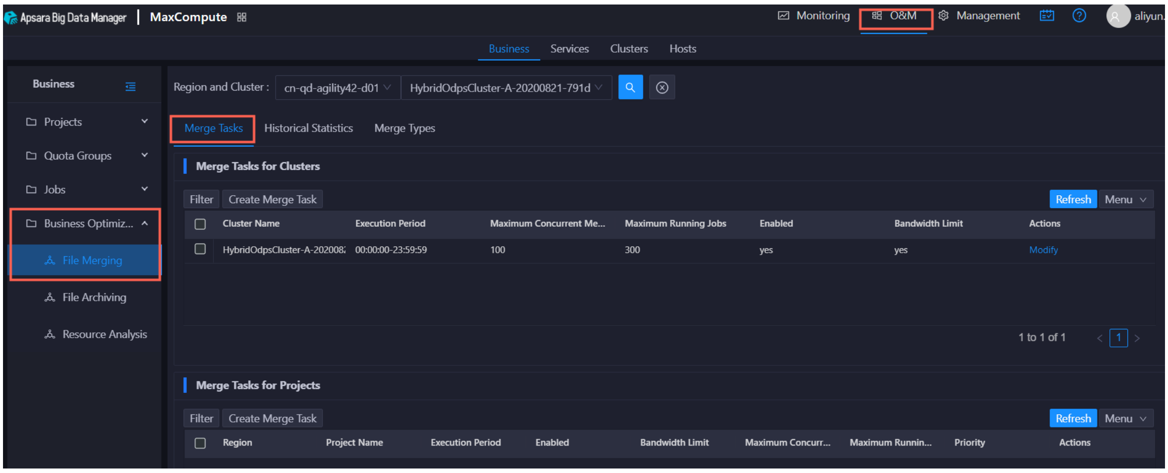
11.2.5.2.5.1. Merge small files

Excessive small files in a MaxCompute cluster occupy a lot of memory resources. Apsara Big Data Manager (ABM) allows you to merge multiple small files in clusters and projects to free up memory occupied by the files.

Create a file merge task for a cluster

If multiple small files exist in most projects of a MaxCompute cluster, you can create a task to merge these files in a centralized manner.

1. In the left-side navigation pane of the **Business** tab, choose **Business Optimization > File Merging**. The **Merge Tasks** tab appears.



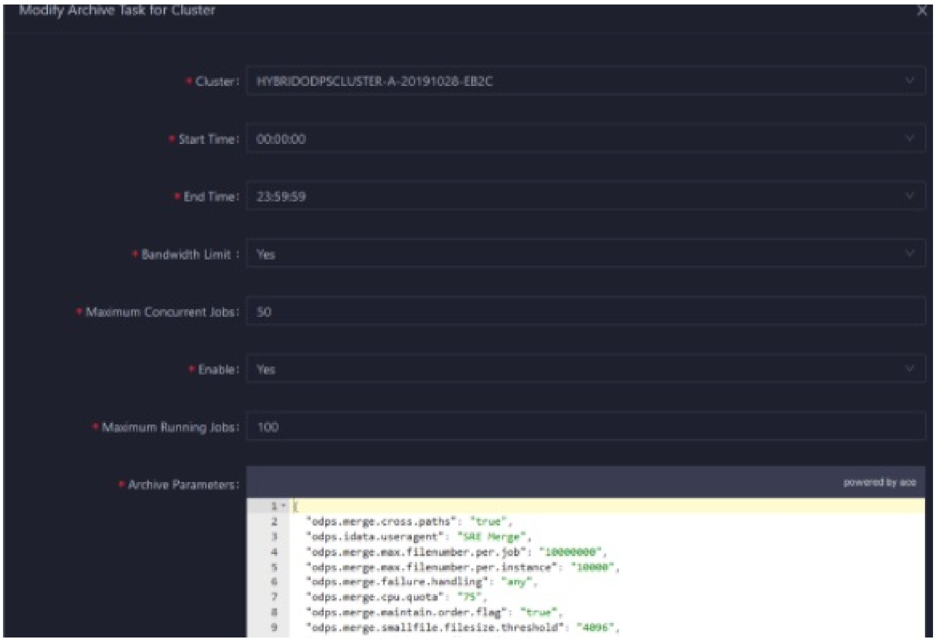
Merge Tasks for Clusters

Cluster Name	Execution Period	Maximum Concurrent Me...	Maximum Running Jobs	Enabled	Bandwidth Limit	Actions
HybridOdpsCluster-A-202008	00:00:00-23:59:59	100	300	yes	yes	Modify

Merge Tasks for Projects

Region	Project Name	Execution Period	Enabled	Bandwidth Limit	Maximum Concurr...	Maximum Runnin...	Priority	Actions

2. In the **Merge Tasks for Clusters** section, click **Create Merge Task**. In the Modify Merge Task for Cluster panel, specify the required parameters.


Modify Archive Task for Cluster

* Cluster: HYBRIDODPSCLUSTER-A-20191028-EB2C
* Start Time: 00:00:00
* End Time: 23:59:59
* Bandwidth Limit : Yes
* Maximum Concurrent Jobs: 50
* Enable: Yes
* Maximum Running Jobs: 100
* Archive Parameters:

```
{
  "odps.merge.cross.paths": "true",
  "odps.idata.useragent": "SRE Merge",
  "odps.merge.max.filenumber.per.job": "10000000",
  "odps.merge.max.filenumber.per.instance": "10000",
  "odps.merge.failure.handling": "any",
  "odps.merge.cpu.quota": "75",
  "odps.merge.maintain.order.flag": "true",
  "odps.merge.smallfile.filesize.threshold": "4096",
```

The following table describes the parameters.

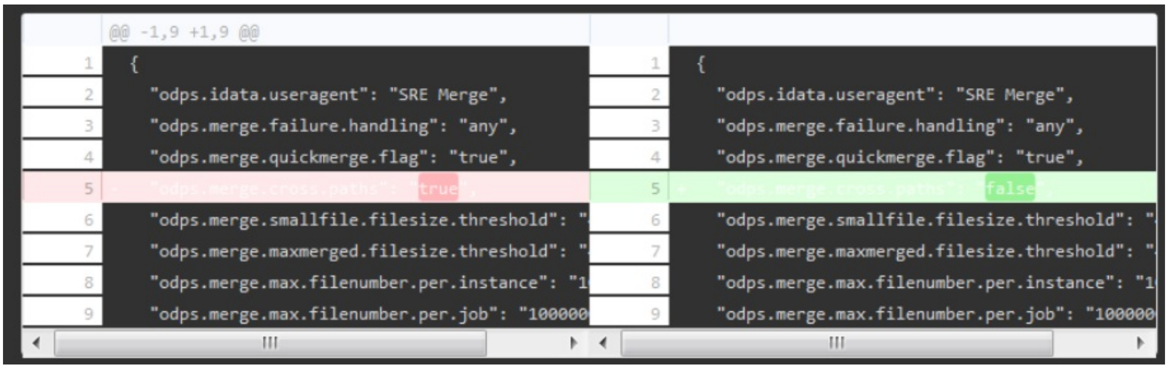
Parameter	Description
Cluster	The cluster for which you want to run the merge task. Select a cluster from the drop-down list.

Parameter	Description
Start Time	The start time of the task.
End Time	The end time of the task.
Bandwidth Limit	Specifies whether to limit the concurrency of merge tasks for the cluster. ○ **Yes**: indicates that merge tasks cannot be concurrently run. ○ **No**: indicates that merge tasks can be concurrently run.
Maximum Concurrent Tasks	The maximum number of merge tasks that can be run for the selected cluster at the same time. This parameter is valid only when **Bandwidth Limit** is set to **No**.
Enabled	Specifies whether the task is enabled.

Merge Parameters	The parameter configuration for the merge task. You can use the following default configuration:
	{
	"odps.idata.useragent": "SRE Merge",
	"odps.merge.cpu.quota": "75",
	"odps.merge.quickmerge.flag": "true",
	"odps.merge.cross.paths": "true",
	"odps.merge.smallfile.filesize.threshold": "4096",
	"odps.merge.maxmerged.filesize.threshold": "4096",
	"odps.merge.max.filenumber.per.instance": "10000",
	"odps.merge.max.filenumber.per.job": "10000000",
	"odps.merge.maintain.order.flag": "true",
	"odps.merge.failure.handling": "any"
	}

Maximum Running Jobs	The maximum number of jobs that can be run for the selected cluster at the same time. This parameter is a global parameter. The jobs refer to all types of jobs in the selected cluster, not only merge tasks.

3. Click **Compare Versions** below Merge Parameters to view the differences between the original and modified values.



```
@@ -1,9 +1,9 @@
{
  "odps.idata.useragent": "SRE Merge",
  "odps.merge.failure.handling": "any",
  "odps.merge.quickmerge.flag": "true",
- "odps.merge.cross.paths": "true",
  "odps.merge.smallfile.filesize.threshold": "
  "odps.merge.maxmerged.filesize.threshold": "
  "odps.merge.max.filenumber.per.instance": "1
  "odps.merge.max.filenumber.per.job": "100000
```

```
{
  "odps.idata.useragent": "SRE Merge",
  "odps.merge.failure.handling": "any",
  "odps.merge.quickmerge.flag": "true",
+ "odps.merge.cross.paths": "false",
  "odps.merge.smallfile.filesize.threshold": "
  "odps.merge.maxmerged.filesize.threshold": "
  "odps.merge.max.filenumber.per.instance": "1
  "odps.merge.max.filenumber.per.job": "100000
```

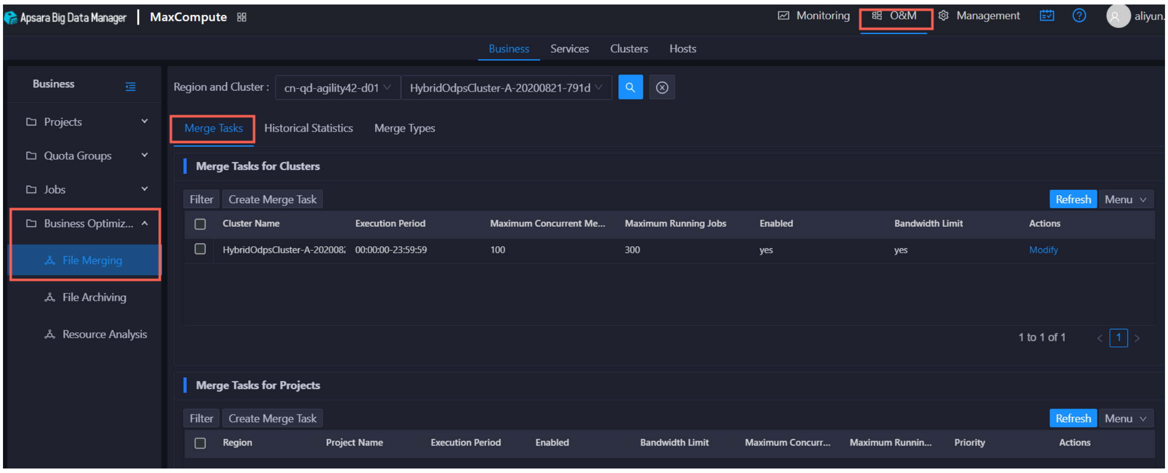
4. Click **Run**.

The newly created merge task appears in the list of merge tasks for clusters.

Create a merge task for a project

If excessive small files exist in only a few projects of a MaxCompute cluster, you can create a merge task to merge the small files in a specific project.

1. In the left-side navigation pane of the **Business** tab, choose **Business Optimization > File Merging**. The **Merge Tasks** tab appears.



Region and Cluster : cn-qd-agility42-d01 HybridOdpsCluster-A-20200821-791d

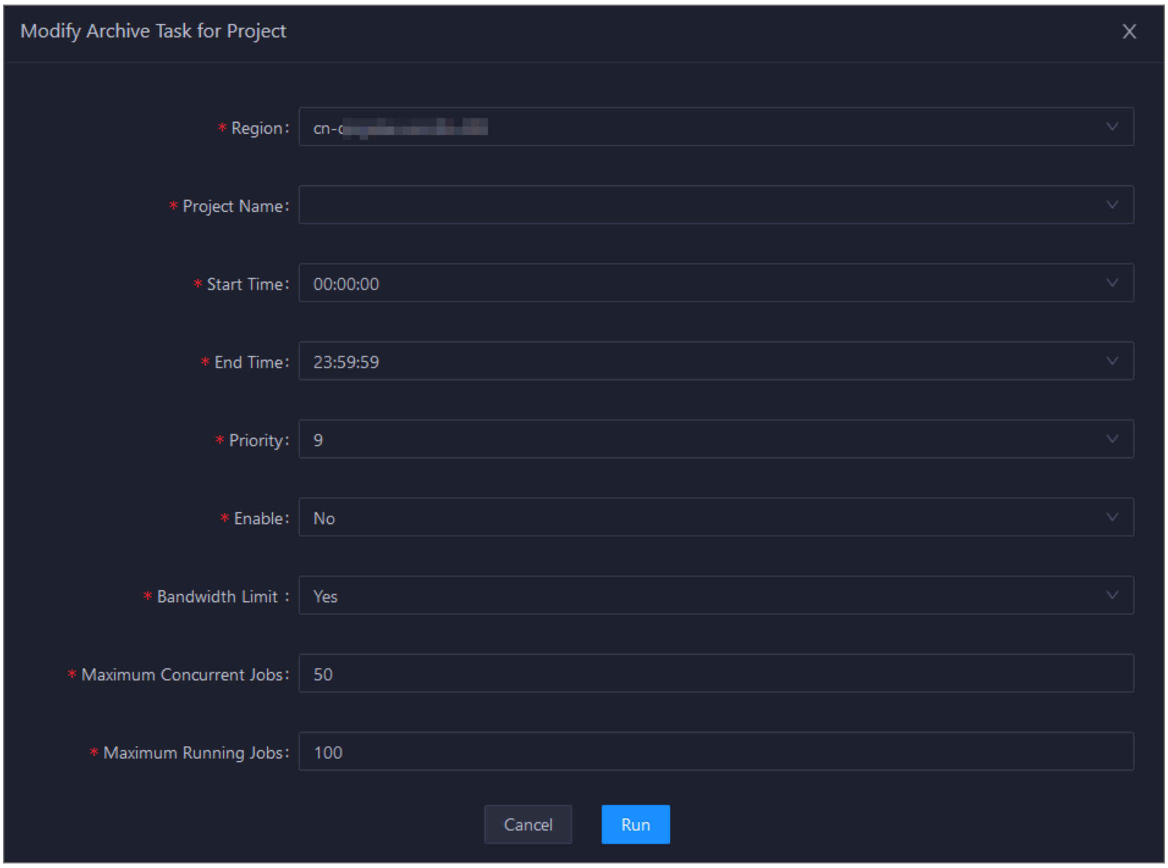
Merge Tasks for Clusters

□	Cluster Name	Execution Period	Maximum Concurrent Me...	Maximum Running Jobs	Enabled	Bandwidth Limit	Actions
□	HybridOdpsCluster-A-202008:	00:00:00-23:59:59	100	300	yes	yes	Modify

Merge Tasks for Projects

□	Region	Project Name	Execution Period	Enabled	Bandwidth Limit	Maximum Concurr...	Maximum Runnin...	Priority	Actions

2. In the **Merge Tasks for Projects** section, click **Create Merge Task**. In the Modify Merge Task for Project panel, specify the required parameters.



Modify Archive Task for Project

* Region: cn-c[redacted]

* Project Name:

* Start Time: 00:00:00

* End Time: 23:59:59

* Priority: 9

* Enable: No

* Bandwidth Limit : Yes

* Maximum Concurrent Jobs: 50

* Maximum Running Jobs: 100

The following table describes the parameters.

Parameter	Description
Region	The region where the selected project resides. Select a region from the drop-down list.
Project Name	The name of the project for which you want to run the merge task. Select a project from the drop-down list.
Start Time	The start time of the task.
Priority	The priority of the task. A small value indicates a high priority.
End Time	The end time of the task.
Enabled	Specifies whether the task is enabled.
Bandwidth Limit	Specifies whether to limit the concurrency of merge tasks for the project. ○ **Yes**: indicates that merge tasks cannot be concurrently run. ○ **No**: indicates that merge tasks can be concurrently run.
Maximum Concurrent Tasks	The maximum number of merge tasks that can be run for the cluster where the selected project resides at the same time. This parameter is valid only when **Bandwidth Limit** is set to **No**.
Maximum Running Jobs	The maximum number of jobs that can be run for the cluster where the selected project resides at the same time. This parameter is a global parameter. The jobs refer to all types of jobs in the cluster where the selected project resides, not only merge tasks.

3. Click **Run**.

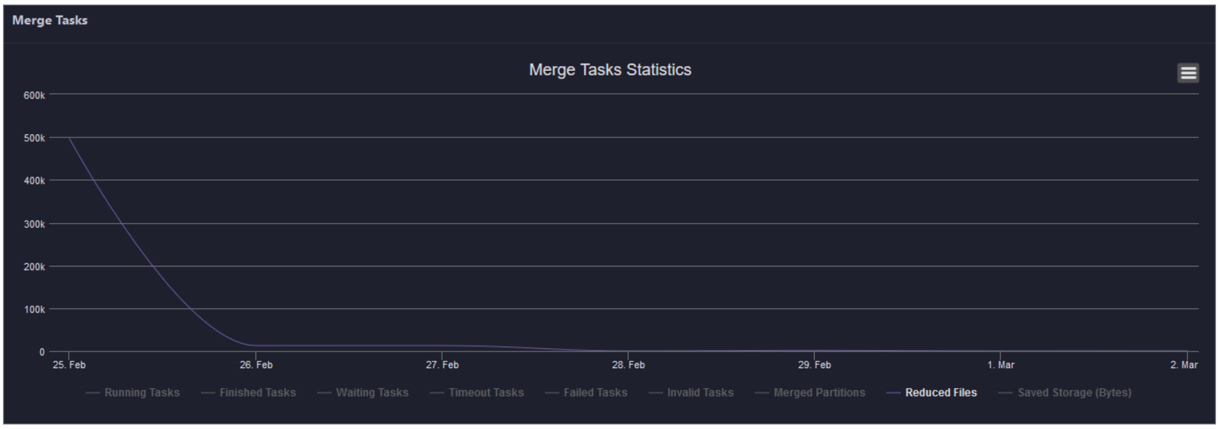
   The newly created merge task appears in the list of merge tasks for projects.

View merge task statistics

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > File Merging**. Then, click the **Historical Statistics** tab to view the historical statistics of merge tasks for clusters and projects.

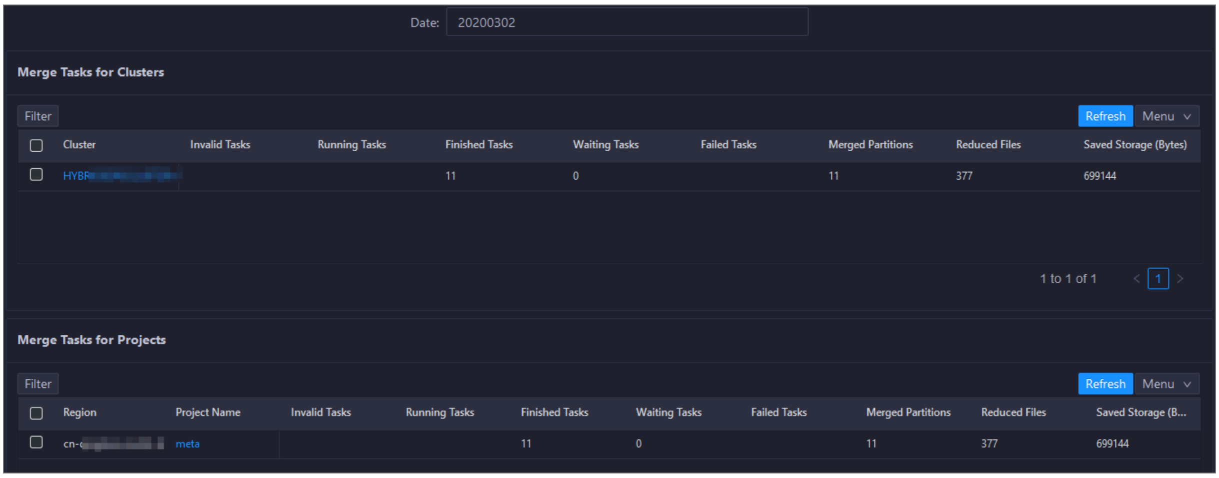
Merge Task Statistics

The trend chart for merge tasks shows statistics on the execution of all merge tasks for each day in the last month. It shows the numbers of running tasks, finished tasks, waiting tasks, timeout tasks, failed tasks, invalid tasks, merged partitions, and reduced files. It also shows the reduced data volume on physical storage, in bytes.



Merge Tasks for Clusters and Merge Tasks for Projects

The two tables show statistics on the execution of merge tasks for clusters and projects on a specific day in the last month. The tables show the numbers of running tasks, finished tasks, waiting tasks, timeout tasks, failed tasks, invalid tasks, merged partitions, and reduced files. The tables also show the reduced data volume on physical storage, in bytes.



Date: 20200302

Merge Tasks for Clusters

Cluster	Invalid Tasks	Running Tasks	Finished Tasks	Waiting Tasks	Failed Tasks	Merged Partitions	Reduced Files	Saved Storage (Bytes)
HYBR[redacted]			11	0		11	377	699144

1 to 1 of 1

Merge Tasks for Projects

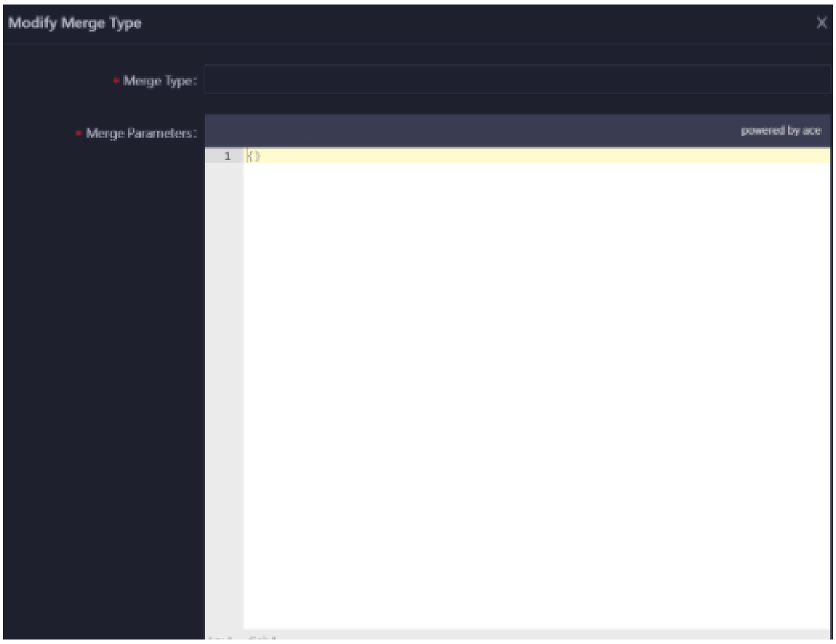
Region	Project Name	Invalid Tasks	Running Tasks	Finished Tasks	Waiting Tasks	Failed Tasks	Merged Partitions	Reduced Files	Saved Storage (B...
cn-[redacted]	meta			11	0		11	377	699144

Manage merge types

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > File Merging**. Then, click the **Merge Types** tab to view the existing merge types and merge parameters.

Create Merge Type

1. In the **Merge Tasks** section, click **Create Merge Type**. In the Modify Merge Type panel, specify the required parameters.



Modify Merge Type

* Merge Type:

* Merge Parameters:

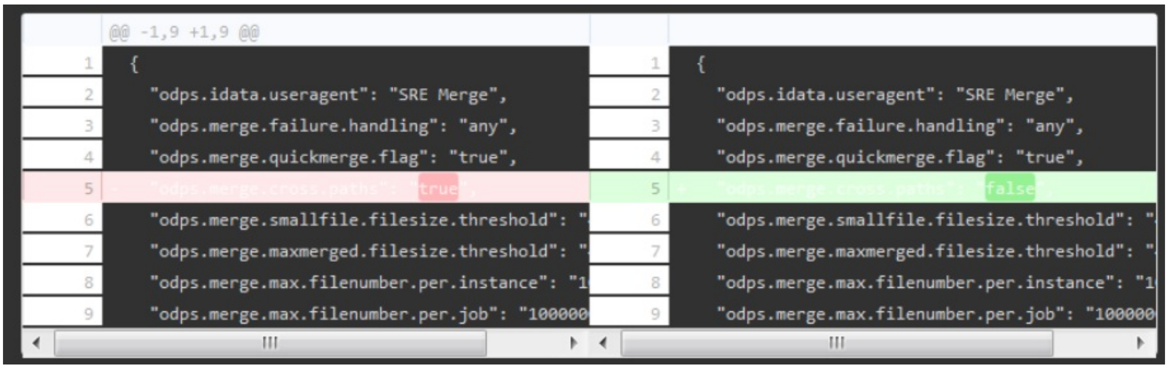
powered by ace

```
{}
```

The following table describes the parameters.

Parameter	Description
Merge Type	The name of the merge type.
Merge Parameters	The merge parameters of the merge type.

2. Click **Compare Versions** below Merge Parameters to view the differences between the original and modified values.



```
@@ -1,9 +1,9 @@
{
    "odps.idata.useragent": "SRE Merge",
    "odps.merge.failure.handling": "any",
    "odps.merge.quickmerge.flag": "true",
-   "odps.merge.cross.paths": "true",
    "odps.merge.smallfile.filesize.threshold": "
    "odps.merge.maxmerged.filesize.threshold": "
    "odps.merge.max.filenumber.per.instance": "1
    "odps.merge.max.filenumber.per.job": "100000
```

```
{
    "odps.idata.useragent": "SRE Merge",
    "odps.merge.failure.handling": "any",
    "odps.merge.quickmerge.flag": "true",
+   "odps.merge.cross.paths": "false",
    "odps.merge.smallfile.filesize.threshold": "
    "odps.merge.maxmerged.filesize.threshold": "
    "odps.merge.max.filenumber.per.instance": "1
    "odps.merge.max.filenumber.per.job": "100000
```

3. Click **Run**.

   The newly created merge type appears in the list of merge types.

11.2.5.2.5.2. Compress idle files

Apsara Big Data Manager (ABM) allows you to create archive tasks to compress idle files in MaxCompute clusters and projects. This saves storage space for the clusters.

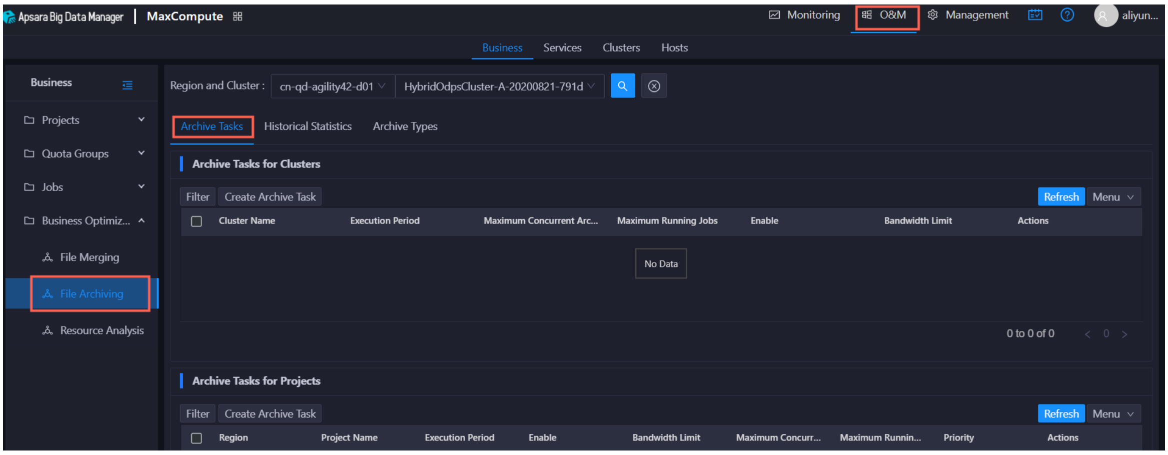
Definition

In a cluster, ABM sorts the tables or partitions created more than 90 days ago by storage space. Then, it compresses the first 100,000 tables or partitions.

Create an archive task for a cluster

If excessive idle files exist in most projects of a MaxCompute cluster, you can create an archive task to compress the idle files in the cluster in a centralized manner.

1. In the left-side navigation pane of the **Business** tab, choose **Business optimization > File Archiving**. The **Archive Tasks** tab appears.



2. In the **Archive Tasks for Clusters** section, click **Create Archive Task**. In the Modify Archive Task for Cluster panel, specify the required parameters.

   The following table describes the parameters.

Parameter	Description
Cluster	The cluster for which you want to run the archive task. Select a cluster from the drop-down list.
Start Time	The start time of the task.
End Time	The end time of the task.
Bandwidth Limit	Specifies whether to limit the concurrency of archive tasks for the cluster. ○ **Yes**: indicates that archive tasks cannot be concurrently run. ○ **No**: indicates that archive tasks can be concurrently run.
Maximum Concurrent Jobs	The maximum number of archive tasks that can be run for the selected cluster at the same time. This parameter is valid only when **Bandwidth Limit** is set to **No**.
Enable	Specifies whether the task is enabled.
Maximum Running Jobs	The maximum number of jobs that can be run for the selected cluster at the same time. This parameter is a global parameter. The jobs refer to all types of jobs in the selected cluster, not only archive tasks.

Parameter	Description

Archive Parameters	The parameter configuration for the archive task. You can use the following default configuration:
	{
	"odps.idata.useragent": "SRE Archive",
	"odps.oversold.resources.ratio": "100",
	"odps.merge.quickmerge.flag": "true",
	"odps.merge.cross.paths": "true",
	"odps.merge.smallfile.filesize.threshold": "4096",
	"odps.merge.maxmerged.filesize.threshold": "4096",
	"odps.merge.max.filenumber.per.instance": "10000",
	"odps.merge.max.filenumber.per.job": "10000000",
	"odps.merge.maintain.order.flag": "true",
	"odps.sql.hive.compatible": "true",
	"odps.merge.compression.strategy": "normal",
	"odps.compression.strategy.normal.compressor": "zstd",
	"odps.merge.failure.handling": "any",
	"odps.merge.archive.flag": "true"
	}

3. Click **Compare Versions** below Archive Parameters to view the differences between the original and modified values.
4. Click **Run**.

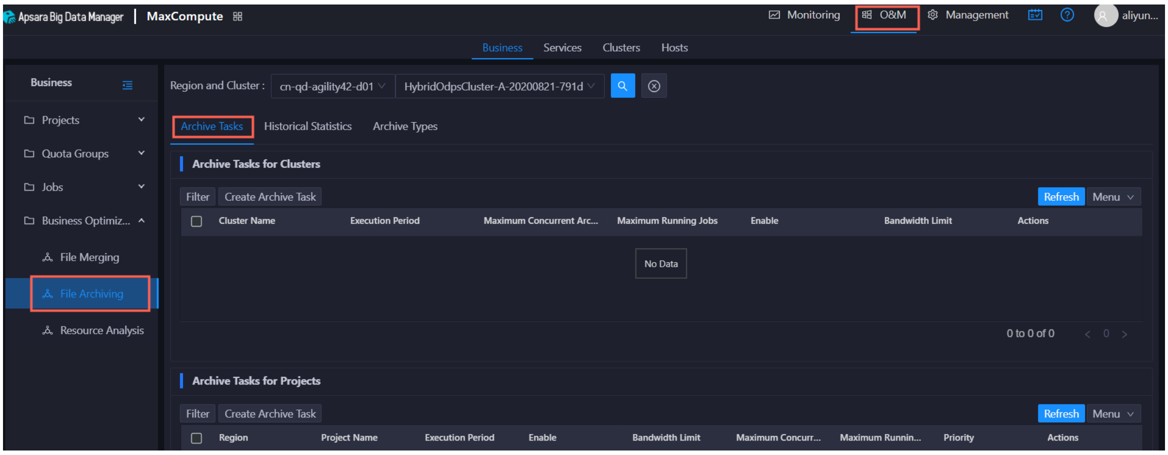
   The newly created archive task appears in the list of archive tasks for clusters.

Create an archive task for a project

If excessive idle files exist in only a few projects of a MaxCompute cluster, you can create an archive task to compress the idle files in a specific project.

> **Note** If the tables or partitions of a project are not ranked top 100,000 in the cluster of the project, the archive task cannot compress the idle files in the project.

1. In the left-side navigation pane of the **Business** tab, choose **Business Optimization > File Archiving**. The **Archive Tasks** tab appears.



2. In the **Archive Tasks for Projects** section, click **Create Archive Task**. In the Modify Archive Task for Project panel, specify the required parameters.

   The following table describes the parameters.

Parameter	Description
Region	The region where the selected project resides. Select a region from the drop-down list.
Project Name	The name of the project for which you want to run the archive task. Select a project from the drop-down list.
Start Time	The start time of the task.
Priority	The priority of the task. A small value indicates a high priority.
End Time	The end time of the task.
Bandwidth Limit	Specifies whether to limit the concurrency of archive tasks for the project. ○ **Yes**: indicates that archive tasks cannot be concurrently run. ○ **No**: indicates that archive tasks can be concurrently run.
Maximum Concurrent Jobs	The maximum number of archive tasks that can be run for the cluster where the selected project resides at the same time. This parameter is valid only when **Bandwidth Limit** is set to **No**.
Enable	Specifies whether the task is enabled.
Maximum Running Jobs	The maximum number of jobs that can be run for the cluster where the selected project resides at the same time. This parameter is a global parameter. The jobs refer to all types of jobs in the cluster where the selected project resides, not only archive tasks.

3. Click **Run**.

   The newly created archive task appears in the list of archive tasks for projects.

View archive task statistics

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > File Archiving**. Then, click the **Historical Statistics** tab to view the historical statistics of archive tasks for clusters and projects.

Archive Tasks

The trend chart for archive tasks shows statistics on the execution of all archive tasks for each day in the last month. It shows the numbers of running tasks, finished tasks, waiting tasks, timeout tasks, failed tasks, invalid tasks, merged partitions, and reduced files. It also shows the reduced data volume on physical storage, in bytes.

Statistics by Cluster and Statistics by Project

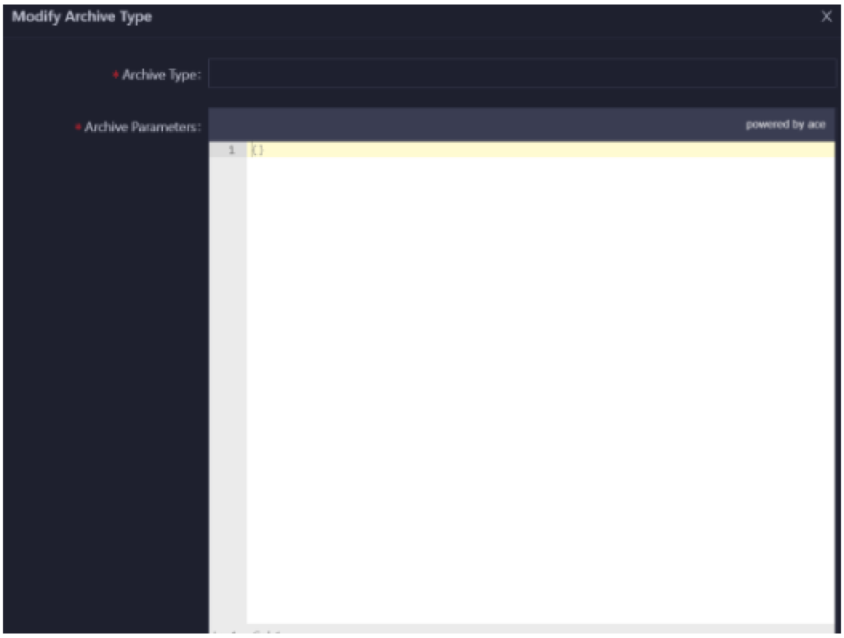
The two tables show statistics on the execution of archive tasks for clusters and projects on a specific day in the last month. The tables show the numbers of running tasks, finished tasks, waiting tasks, timeout tasks, failed tasks, invalid tasks, merged partitions, and reduced files. The tables also show the reduced data volume on physical storage, in bytes.

Manage archive types

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > File Archiving**. Then, click the **Archive Types** tab to view the existing archive types and archive parameters.

Create Archive Type

1. In the **Archive Tasks** section, click **Create Archive Type**. In the Modify Archive Type panel, specify the required parameters.



The following table describes the parameters.

Parameter	Description
Archive Type	The name of the archive type.
Archive Parameters	The archive parameters of the archive type.

2. Click **Compare Versions** below Archive Parameters to view the differences between the original and modified values.
3. Click **Run**.

   The newly created archive type appears in the list of archive types.

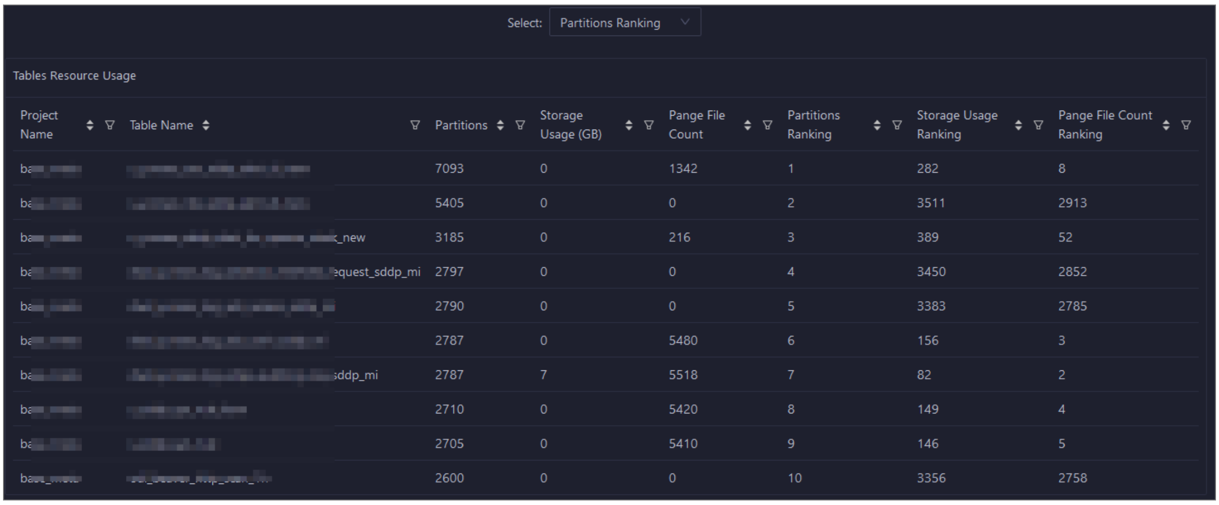
11.2.5.2.5.3. Analyze resources

Apsara Big Data Manager (ABM) allows you to analyze the resources for MaxCompute clusters on different tabs in the ABM console. This way, you can better understand the data storage in MaxCompute. The tabs include Tables, Projects, Tasks, Execution Time, Start Time, and Engines.

Tables

On the Tables tab, you can view the detailed information about all tables in each project, including Partitions, Storage Usage (GB), Pangu File Count, Partitions Ranking, Storage Usage Ranking, and Pangu File Count Ranking. You can sort tables by partition quantity, physical storage usage, and file quantity of Apsara Distributed File System.

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > Resource Analysis**. The **Tables** tab appears.



Select: Partitions Ranking

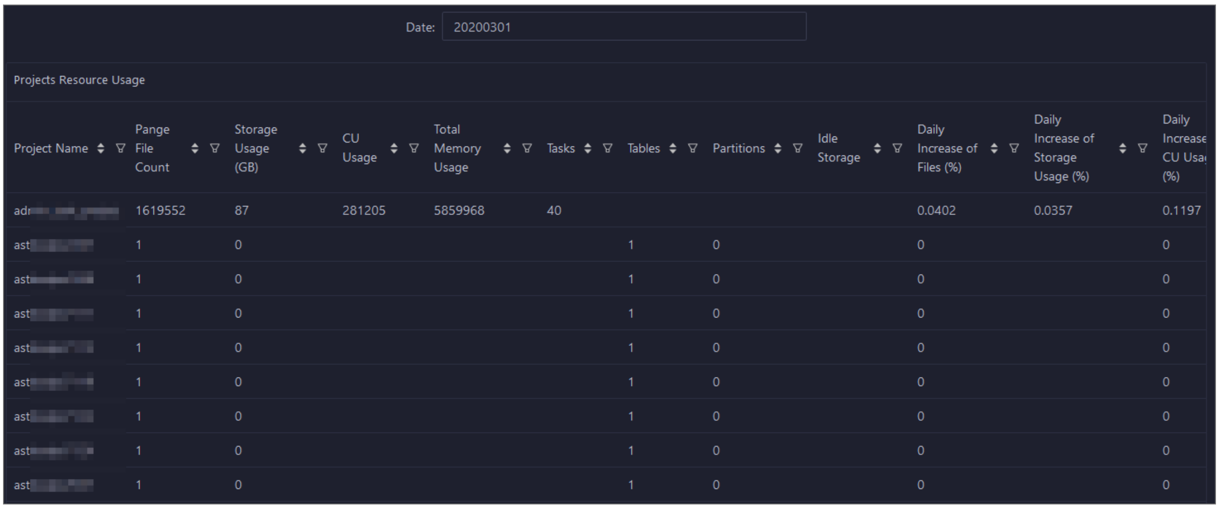
Tables Resource Usage

Project Name	Table Name	Partitions	Storage Usage (GB)	Pange File Count	Partitions Ranking	Storage Usage Ranking	Pange File Count Ranking
[redacted]	[redacted]	7093	0	1342	1	282	8
[redacted]	[redacted]	5405	0	0	2	3511	2913
[redacted]	[redacted]	3185	0	216	3	389	52
[redacted]	[redacted]	2797	0	0	4	3450	2852
[redacted]	[redacted]	2790	0	0	5	3383	2785
[redacted]	[redacted]	2787	0	5480	6	156	3
[redacted]	[redacted]	2787	7	5518	7	82	2
[redacted]	[redacted]	2710	0	5420	8	149	4
[redacted]	[redacted]	2705	0	5410	9	146	5
[redacted]	[redacted]	2600	0	0	10	3356	2758

Projects

On the Projects tab, you can view the detailed information about storage for each project, including Pangu File Count, Storage Usage (GB), CU Usage, Total Memory Usage, Tasks, Tables, Idle Storage, and daily and weekly increases in percentage of these items.

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > Resource Analysis**. Click the **Projects** tab.



Date: 20200301

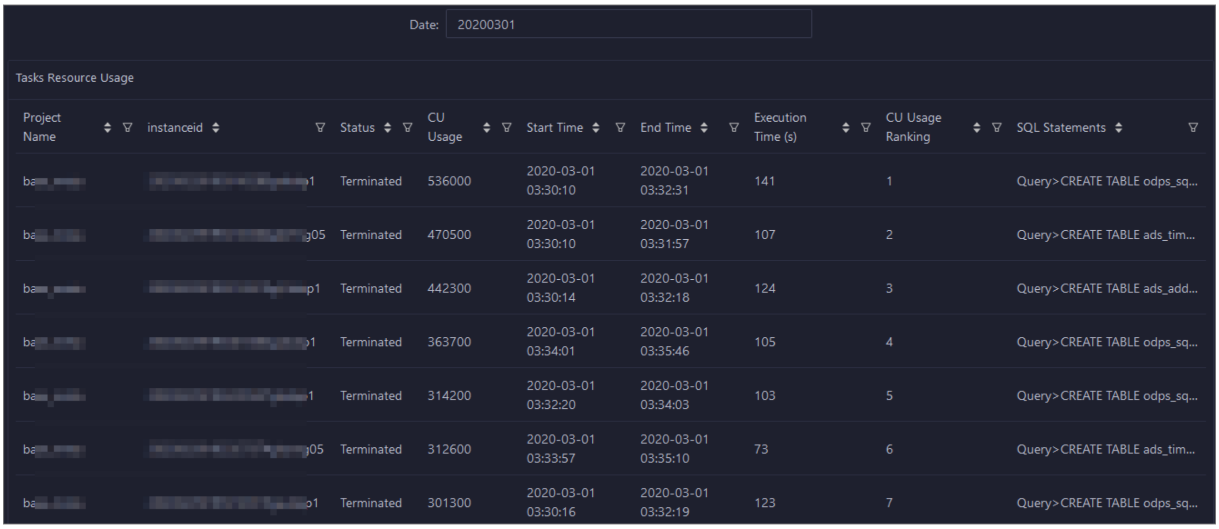
Projects Resource Usage

Project Name	Pange File Count	Storage Usage (GB)	CU Usage	Total Memory Usage	Tasks	Tables	Partitions	Idle Storage	Daily Increase of Files (%)	Daily Increase of Storage Usage (%)	Daily Increase CU Usa (%)
adr[redacted]	1619552	87	281205	5859968	40				0.0402	0.0357	0.1197
ast[redacted]	1	0				1	0		0		0
ast[redacted]	1	0				1	0		0		0
ast[redacted]	1	0				1	0		0		0
ast[redacted]	1	0				1	0		0		0
ast[redacted]	1	0				1	0		0		0
ast[redacted]	1	0				1	0		0		0
ast[redacted]	1	0				1	0		0		0
ast[redacted]	1	0				1	0		0		0

Tasks

On the Tasks tab, you can view the detailed information about all tasks in each project, including instanceid, Status, CU Usage, Start Time, End Time, Execution Time (s), CU Usage Ranking, and SQL Statements.

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > Resource Analysis**. Click the **Tasks** tab.



Date: 20200301

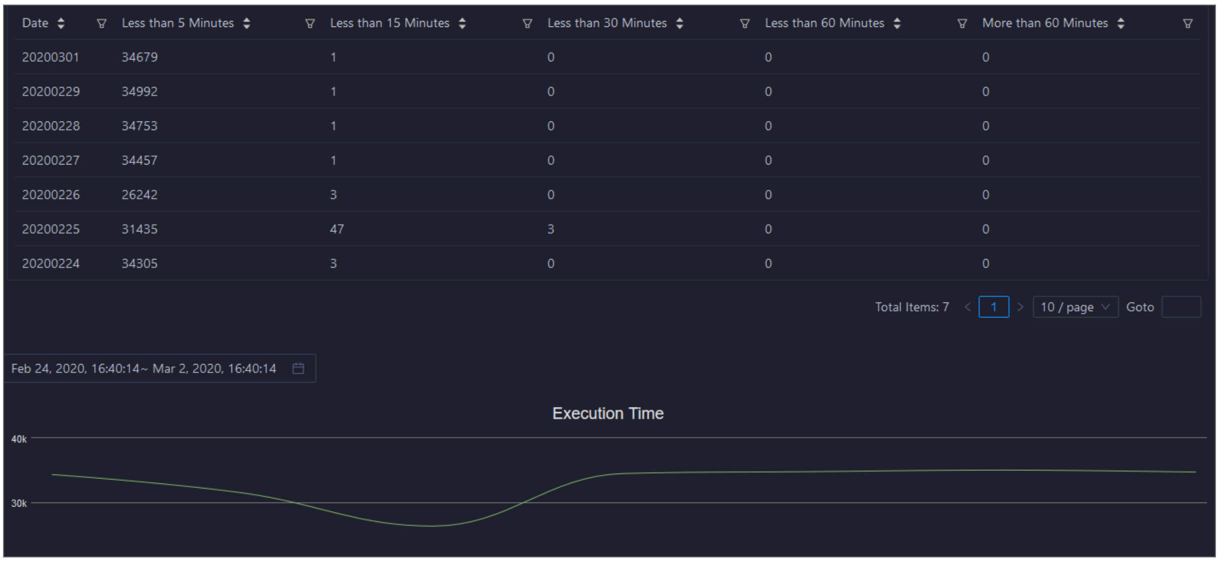
Tasks Resource Usage

Project Name	instanceid	Status	CU Usage	Start Time	End Time	Execution Time (s)	CU Usage Ranking	SQL Statements
ba[redacted]	[redacted]1	Terminated	536000	2020-03-01 03:30:10	2020-03-01 03:32:31	141	1	Query>CREATE TABLE odps_sq...
ba[redacted]	[redacted]g05	Terminated	470500	2020-03-01 03:30:10	2020-03-01 03:31:57	107	2	Query>CREATE TABLE ads_tim...
ba[redacted]	[redacted]p1	Terminated	442300	2020-03-01 03:30:14	2020-03-01 03:32:18	124	3	Query>CREATE TABLE ads_add...
ba[redacted]	[redacted]1	Terminated	363700	2020-03-01 03:34:01	2020-03-01 03:35:46	105	4	Query>CREATE TABLE odps_sq...
ba[redacted]	[redacted]1	Terminated	314200	2020-03-01 03:32:20	2020-03-01 03:34:03	103	5	Query>CREATE TABLE odps_sq...
ba[redacted]	[redacted]g05	Terminated	312600	2020-03-01 03:33:57	2020-03-01 03:35:10	73	6	Query>CREATE TABLE ads_tim...
ba[redacted]	[redacted]1	Terminated	301300	2020-03-01 03:30:16	2020-03-01 03:32:19	123	7	Query>CREATE TABLE odps_sq...

Execution Time

On the Execution Time tab, you can view the numbers of tasks whose execution time is within different time ranges in each project. The metrics include Less than 5 Minutes, Less than 15 Minutes, Less than 30 Minutes, Less than 60 Minutes, and More than 60 Minutes. The Execution Time chart displays the trend lines of task quantity in different colors by day.

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > Resource Analysis**. Click the **Execution Time** tab.



Date	Less than 5 Minutes	Less than 15 Minutes	Less than 30 Minutes	Less than 60 Minutes	More than 60 Minutes
20200301	34679	1	0	0	0
20200229	34992	1	0	0	0
20200228	34753	1	0	0	0
20200227	34457	1	0	0	0
20200226	26242	3	0	0	0
20200225	31435	47	3	0	0
20200224	34305	3	0	0	0

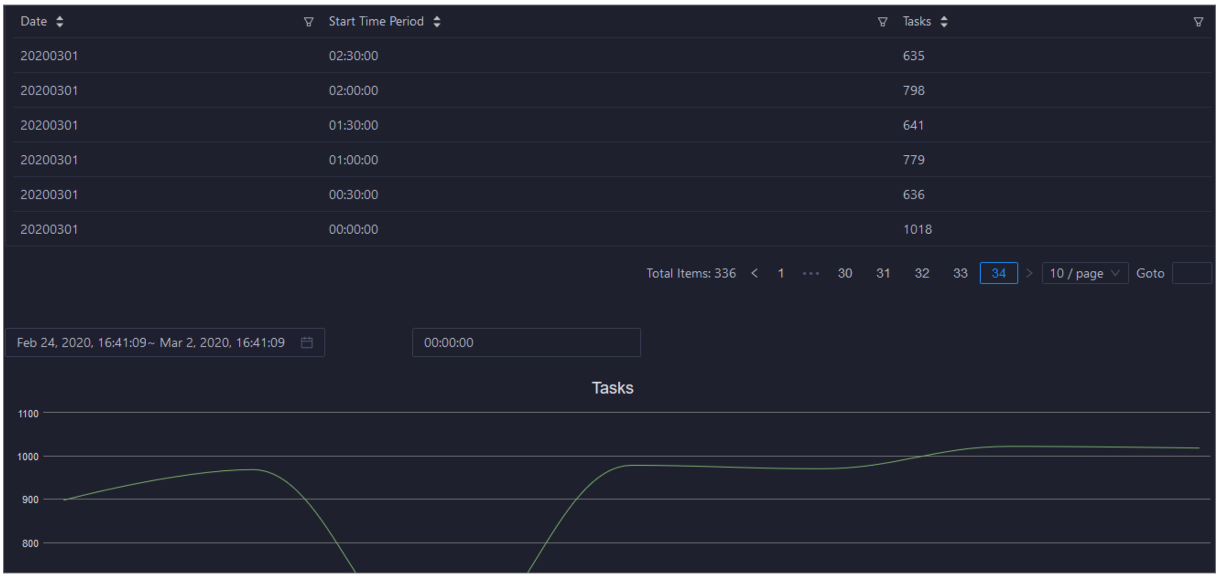
Total Items: 7 < 1 > 10 / page Goto

Feb 24, 2020, 16:40:14~ Mar 2, 2020, 16:40:14

Start Time

On the Start Time tab, you can view the numbers of tasks started in different time periods for each project. The time interval is 30 minutes. The Tasks chart displays the trend line of the number of tasks started in a specified time period by day.

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > Resource Analysis**. Click the **Start Time** tab.



Date	Start Time Period	Tasks
20200301	02:30:00	635
20200301	02:00:00	798
20200301	01:30:00	641
20200301	01:00:00	779
20200301	00:30:00	636
20200301	00:00:00	1018

Total Items: 336 < 1 ••• 30 31 32 33 34 > 10 / page Goto

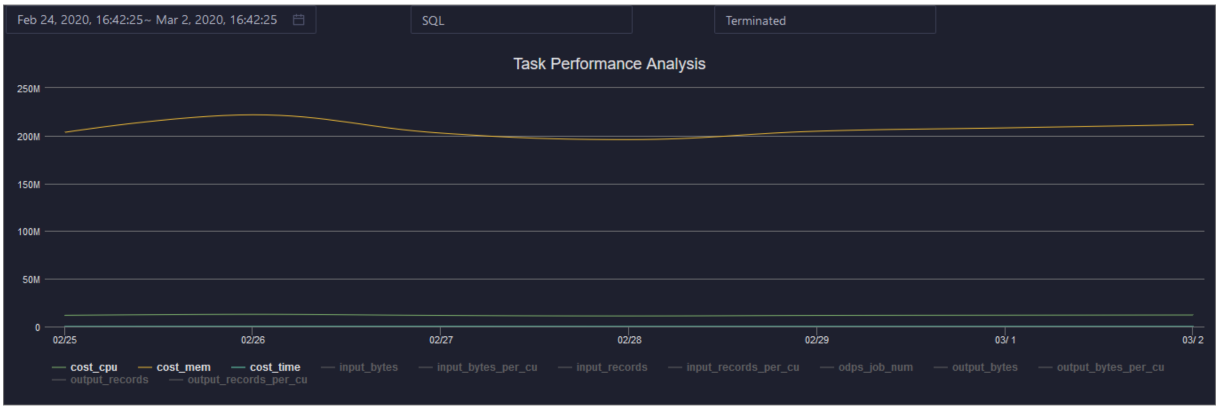
Feb 24, 2020, 16:41:09~ Mar 2, 2020, 16:41:09

00:00:00

Engines

On the Engines tab, you can view the trend lines of performance statistics of tasks in each project in the Task Performance Analysis chart. The performance metrics include cost_cpu, cost_mem, cost_time, input_bytes, input_bytes_per_cu, input_records, input_records_per_cu, output_bytes, output_bytes_per_cu, output_records, and output_records_per_cu.

In the left-side navigation pane of the **Business** tab, choose **Business Optimization > Resource Analysis**. Click the **Engines** tab.



Feb 24, 2020, 16:42:25~ Mar 2, 2020, 16:42:25

SQL

Terminated

11.2.5.3. Service O&M

11.2.5.3.1. Control service O&M

11.2.5.3.1.1. O&M features and entry

This topic describes control service O&M features and how to go to the control service O&M page.

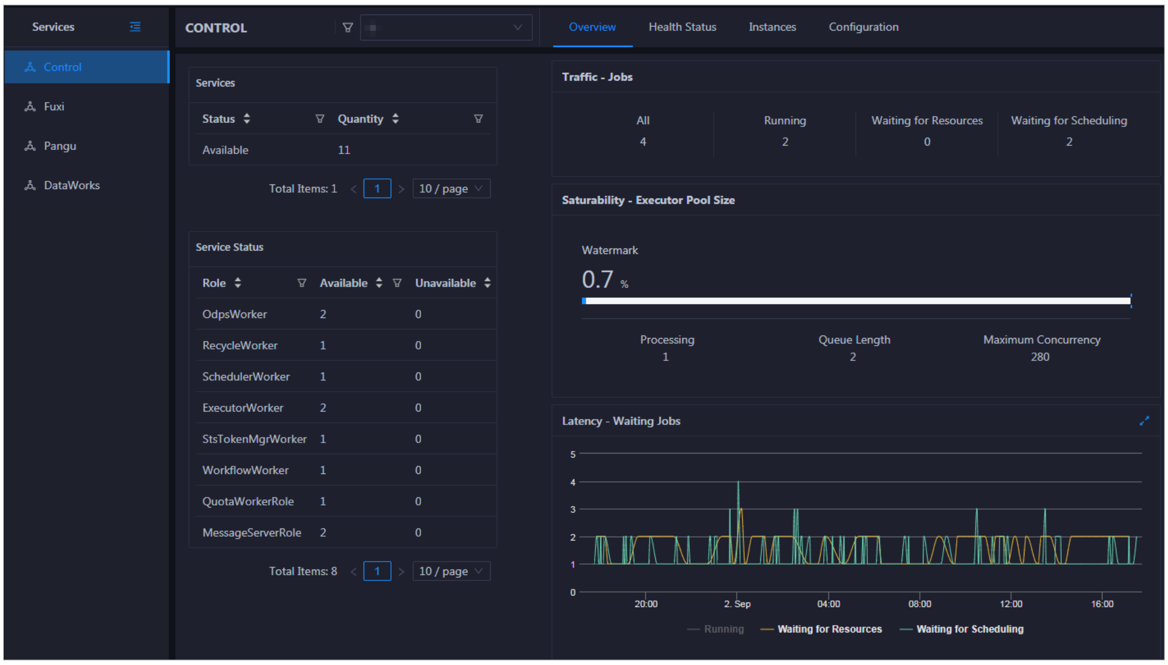
Control service O&M features

- Overview: shows the overall running information about the control service. You can view the service overview, service status, job running, executor pool size, and job status.
- Health Status: shows all checkers for the control service. You can query checker details, check results for hosts in a cluster, and schemes to clear alerts (if any exists). You can also log on to a host and perform manual checks on the host.
- Instances: shows information about the server roles of the control service. You can view the host, status, requested CPU resources, and requested memory of each server role.
- Configuration: provides the access entry to configure global computing, cluster-level computing, computing scheduling, and cluster endpoints.
- Metadata Repository: allows you to view the completion time and status of the output tasks of the metadata warehouse and the trend chart of the consumed time for running tasks in MaxCompute.
- Start Service Role or Stop Service Role: allows you to start or stop the server roles of the MaxCompute control service and view the execution history. If you fail to start or stop the server roles, you can identify the cause of the failure.
- Start Admin Console: allows you to start AdminConsole.
- Collect Service Logs: allows you to collect service logs for the specified time period. This enables you to identify the cause of a failure.

Go to the control service O&M page

1. Log on to the Apsara Big Data Manager (ABM) console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.

4. In the left-side navigation pane of the **Services** tab, click **Control**. The **Overview** tab for the control service appears.



Services

Status	Quantity
Available	11

Total Items: 1 < 1 > 10 / page

Service Status

Role	Available	Unavailable
OdpsWorker	2	0
RecycleWorker	1	0
SchedulerWorker	1	0
ExecutorWorker	2	0
StsTokenMgrWorker	1	0
WorkflowWorker	1	0
QuotaWorkerRole	1	0
MessageServerRole	2	0

Total Items: 8 < 1 > 10 / page

Traffic - Jobs

All	Running	Waiting for Resources	Waiting for Scheduling
4	2	0	2

Saturability - Executor Pool Size

Watermark
0.7 %

Processing	Queue Length	Maximum Concurrency
1	2	280

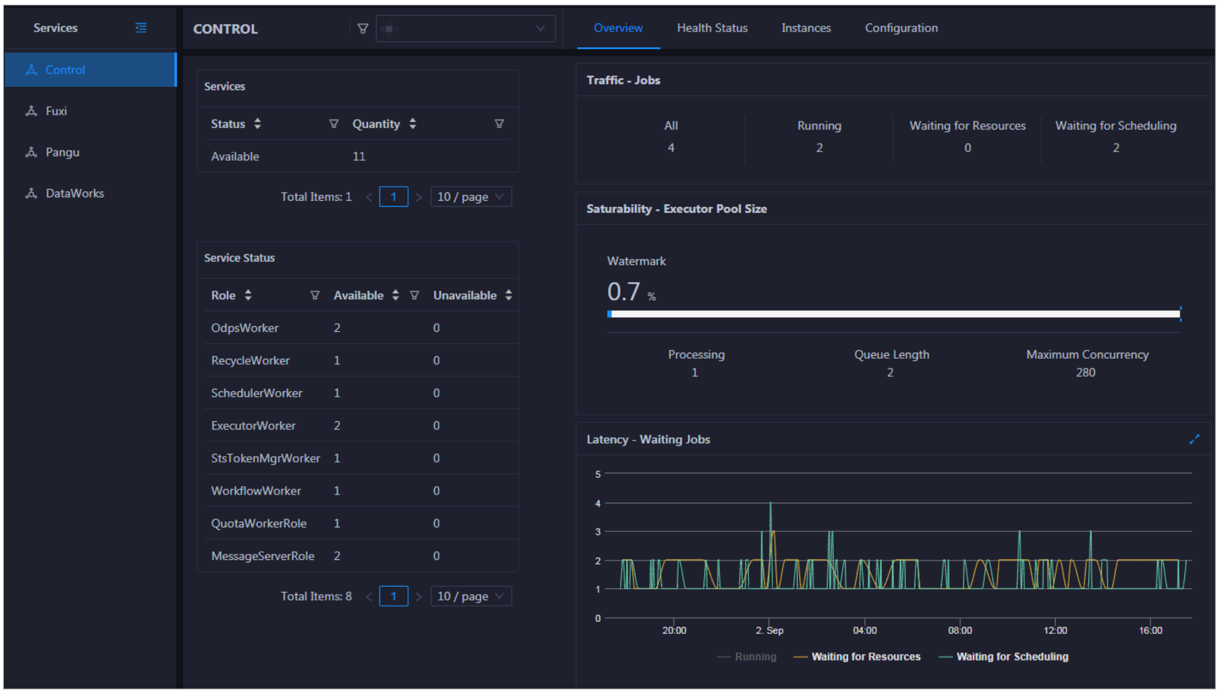
Latency - Waiting Jobs

11.2.5.3.1.2. Control service overview

The Overview page displays the overall running information about the control service, including the service summary, service status, job summary, executor pool summary, and job status.

Entry

On the **Services** page, click **Control** in the left-side navigation pane. The **Overview** page for the control service appears.


Services
Control
Fuxi
Pangu
DataWorks
CONTROL
Overview
Health Status
Instances
Configuration

Services

Status	Quantity
Available	11

Total Items: 1 < 1 > 10 / page

Service Status

Role	Available	Unavailable
OdpsWorker	2	0
RecycleWorker	1	0
SchedulerWorker	1	0
ExecutorWorker	2	0
StsTokenMgrWorker	1	0
WorkflowWorker	1	0
QuotaWorkerRole	1	0
MessageServerRole	2	0

Total Items: 8 < 1 > 10 / page

Traffic - Jobs

All	Running	Waiting for Resources	Waiting for Scheduling
4	2	0	2

Saturability - Executor Pool Size

Watermark
0.7 %

Processing	Queue Length	Maximum Concurrency
1	2	280

Latency - Waiting Jobs

5
4
3
2
1
0
20:00
2. Sep
04:00
08:00
12:00
16:00
Running
Waiting for Resources
Waiting for Scheduling

On the **Overview** page, you can view the overall running information about the control service, including the service summary, service status, job summary, executor pool summary, and job status.

Services

This section displays the numbers of available services and unavailable services respectively.

Service Status

This section displays all control service roles. You can also view the numbers of available and unavailable services respectively for each service role.

Traffic - Jobs

This section displays the total number of jobs in the cluster, and the numbers of running jobs, jobs waiting for resources, and jobs waiting for scheduling respectively.

Saturability - Executor Pool Size

The section displays information about the thread pool, including the resource usage, number of jobs being processed, queue length, and maximum concurrency.

Latency - Waiting Jobs

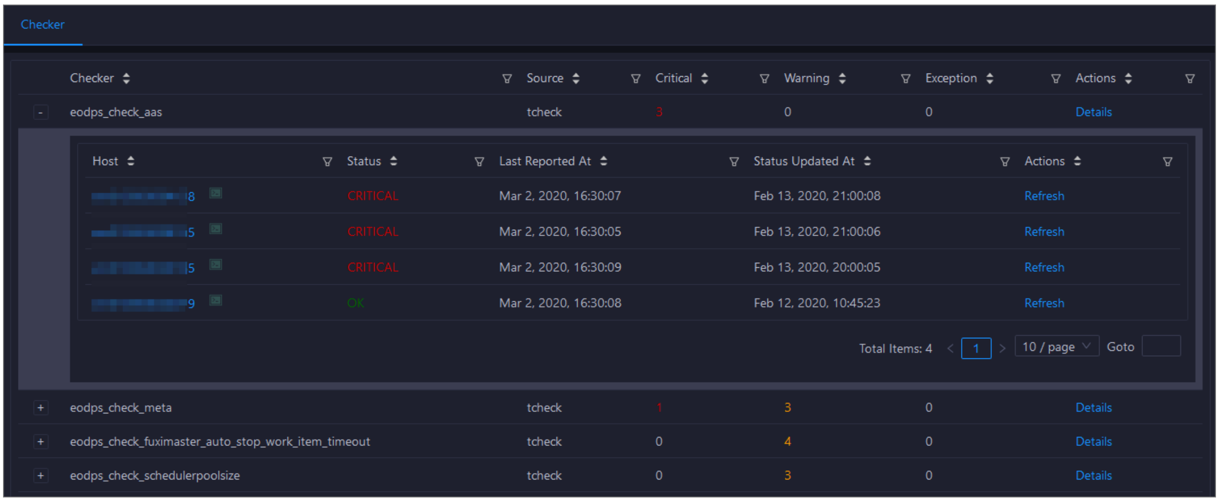
This section displays the trend chart of jobs. The chart displays the trend lines of the numbers of running jobs, jobs waiting for resources, and jobs waiting for scheduling in different colors.

11.2.5.3.1.3. Control service health

On the Health Status page for the control service, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Entry

On the **Services** page, click **Control** in the left-side navigation pane, and then click the **Health Status** tab.



Checker

	Checker	Source	Critical	Warning	Exception	Actions
-	eodps_check_aas	tcheck	3	0	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
[redacted]	CRITICAL	Mar 2, 2020, 16:30:07	Feb 13, 2020, 21:00:08	Refresh
[redacted]	CRITICAL	Mar 2, 2020, 16:30:05	Feb 13, 2020, 21:00:06	Refresh
[redacted]	CRITICAL	Mar 2, 2020, 16:30:09	Feb 13, 2020, 20:00:05	Refresh
[redacted]	OK	Mar 2, 2020, 16:30:08	Feb 12, 2020, 10:45:23	Refresh

Total Items: 4 < 1 > 10 / page Goto

	Checker	Source	Critical	Warning	Exception	Actions
+	eodps_check_meta	tcheck	1	3	0	Details
+	eodps_check_fuximaster_auto_stop_work_item_timeout	tcheck	0	4	0	Details
+	eodps_check_schedulerpoolsize	tcheck	0	3	0	Details

On the **Health Status** page, you can view all checkers of the cluster and the check results for the hosts in the cluster. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

Supported operations

On the Health Status page, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host. For more information, see Cluster health.

11.2.5.3.1.4. Instances

The Instances tab shows information about server roles, which includes the host, status, requested CPU resources, and requested memory of each server role.

Go to the Instances tab

In the left-side navigation pane of the **Services** tab, click **Control**. Then, click the **Instances** tab.

The Instances tab shows information about server roles, which includes the host, status, requested CPU resources, and requested memory of each server role.

11.2.5.3.1.5. Control service configuration

The Configuration page under Control is the access to configuring global computing, cluster-level computing, computing scheduling, and cluster endpoints. If you need to modify the configurations of the control service, submit a ticket to apply for technical support, and then modify the configurations carefully under the guidance of technical support engineers.

On the **Services** page, click **Control** in the left-side navigation pane, and then click the **Configuration** tab.

The **Configuration** page consists of the following tabs:

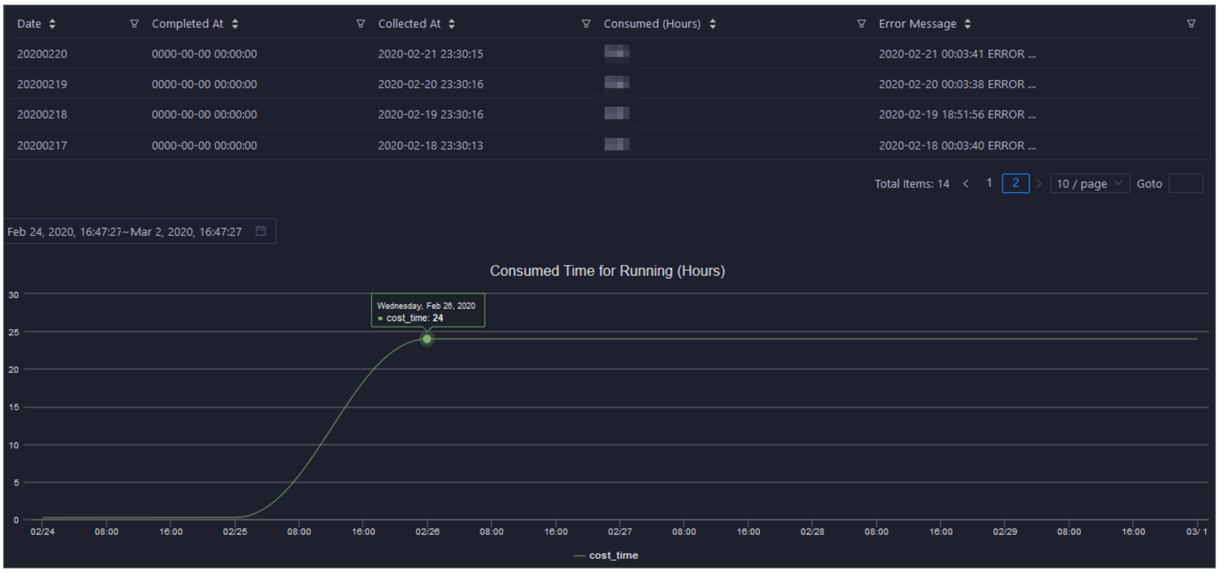
- Computing: provides the global computing configuration, cluster-level computing configuration, and compute scheduling configuration features.
- Tunnel Routing Address: provides the cluster endpoint configuration feature.

11.2.5.3.1.6. Metadata warehouse for the control service

This topic describes how to view the completion time and status of the output tasks of the metadata warehouse and the trend chart of the consumed time for running tasks in MaxCompute.

The metadata warehouse in MaxCompute regularly runs output tasks every day. Apsara Big Data Manager (ABM) obtains the status of output tasks every 30 minutes. If an output task of the metadata warehouse is not complete within 24 hours, the output task is regarded as a failure.

In the left-side navigation pane of the **Services** tab, click **Control**. On the page that appears, click the **Metadata Repository** tab.



Date	Completed At	Collected At	Consumed (Hours)	Error Message
20200220	0000-00-00 00:00:00	2020-02-21 23:30:15	[redacted]	2020-02-21 00:03:41 ERROR ...
20200219	0000-00-00 00:00:00	2020-02-20 23:30:16	[redacted]	2020-02-20 00:03:38 ERROR ...
20200218	0000-00-00 00:00:00	2020-02-19 23:30:16	[redacted]	2020-02-19 18:51:56 ERROR ...
20200217	0000-00-00 00:00:00	2020-02-18 23:30:13	[redacted]	2020-02-18 00:03:40 ERROR ...

Total Items: 14 < 1 2 > 10 / page Goto

Feb 24, 2020, 16:47:27~Mar 2, 2020, 16:47:27

The **Metadata Repository** tab displays the completion time of the output tasks of the metadata warehouse and the trend chart of the consumed time for running tasks. The time displayed in the **Completed At** column indicates the time when an output task is complete. The time displayed in the **Collected At** column indicates the last time at which ABM obtains the status of output tasks.

11.2.5.3.1.7. Stop or start a server role

Apsara Big Data Manager (ABM) allows you to start or stop the server roles of the MaxCompute control service and view the execution history. If you fail to start or stop the server roles, you can identify the failure.

Stop a server role

1. Log on to the ABM console.
2. In the upper-left corner, click the ▦ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Control**. In the upper-right corner of the tab that appears, choose **Actions** > **Stop Service Role**.
5. In the Stop Service Role panel, select a server role that you want to stop and click **Run**.
6. In the upper-right corner, click **Actions** and select **Execution History** next to **Stop Service Role** to check whether the action is successful in the execution history.

   The Execution History panel shows the current status, submission time, start time, end time, and operator of each action.
7. Click **Details** in the Details column to view the execution details.

   On the execution details page, you can view the job name, execution status, execution steps, script, and parameter settings. You can also download the execution details to your computer.

Start a server role

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Control**. In the upper-right corner of the tab that appears, choose **Actions** > **Start Service Role**.
5. In the Start Service Role panel, select a server role that you want to start and click **Run**.
6. In the upper-right corner, click **Actions** and select **Execution History** next to **Start Service Role** to check whether the action is successful in the execution history.

   The Execution History panel shows the current status, submission time, start time, end time, and operator of each action.
7. Click **Details** in the Details column to view the execution details.

   On the execution details page, you can view the job name, execution status, execution steps, script, and parameter settings. You can also download the execution details to your computer.

Identify the cause of a failure

This section describes how to identify the cause of the failure to start a server role.

1. In the Execution History panel, click **Details** in the Details column of the task to view the details.
2. In the Start Service Role panel, click **View Details** for a failed step to identify the cause of the failure.

   You can view the parameter settings, outputs, error messages, script, and runtime parameters to identify the cause of the failure.

11.2.5.3.1.8. Start AdminConsole

AdminConsole is a management platform of MaxCompute. It is disabled by default. Apsara Big Data Manager (ABM) allows you to quickly start AdminConsole to better manage MaxCompute clusters.

Prerequisites

Your ABM account is granted the required permissions to perform O&M operations on MaxCompute.

Step 1: Start AdminConsole

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Control**.
5. In the upper-right corner of the page that appears, choose **Actions** > **Start Admin Console**.
6. In the **Start Admin Console** panel, click **Run**.

Step 2: View the execution status or progress

1. On any tab of the **CONTROL** page, click **Actions** and select **Execution History** next to **Start Admin Console** in the upper-right corner to view the execution history.

RUNNING indicates that the execution is in progress. **SUCCESS** indicates that the execution succeeds. **FAILED** indicates that the execution fails.

2. If the status is **RUNNING**, click **Details** in the Details column to view the execution progress.

Step 3: (Optional) Identify the cause of a failure

If the status is **FAILED**, you can view the execution logs to identify the cause of the failure.

1. On any tab of the **CONTROL** page, click **Actions** and select **Execution History** next to **Start Admin Console** in the upper-right corner to view the execution history.
2. In the Execution History panel, click **Details** in the Details column of the task to view the details.
3. On the **Servers** tab of the failed step, click **View Details** in the Actions column of a failed server. The **Execution Output** tab appears in the Execution Details section. You can view the output to identify the cause of the failure.

11.2.5.3.1.9. Collect service logs

Apsara Big Data Manager (ABM) allows you to collect service logs for the specified time period. This enables you to identify the cause of a failure.

Prerequisites

Your ABM account is granted the required permissions to perform O&M operations on MaxCompute.

Step 1: Collect service logs

1. Log on to the ABM console.
2. In the upper-left corner, click the ▦ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Control**.
5. In the upper-right corner of the page that appears, choose **Actions > Collect Service Logs**.
6. In the **Collect Service Logs** panel, specify the required parameters.

   The following table describes the parameters.

Parameter	Description
Target Service	The service from which you want to collect service logs. Select a service from the drop-down list. You can select multiple services.
Time Period	The time period in which the logs that you want to collect are generated.
Degree of Concurrency	The maximum number of nodes from which you can collect service logs at the same time.
Hostname	The name of the host. Separate multiple hostnames with commas (,).

7. Click **Run**.

Step 2: View the execution status or progress

1. On any tab of the **CONTROL** page, click **Actions** and select **Execution History** next to **Collect Service Logs** in the upper-right corner to view the execution history.

   RUNNING indicates that the execution is in progress. **SUCCESS** indicates that the execution succeeds. **FAILED** indicates that the execution fails.

2. If the status is **RUNNING**, click **Details** in the Details column to view the execution progress.

Step 3: (Optional) Identify the cause of a failure

If the status is **FAILED**, you can view the execution logs to identify the cause of the failure.

1. On any tab of the **CONTROL** page, click **Actions** and select **Execution History** next to **Collect Service Logs** in the upper-right corner to view the execution history.
2. In the Execution History panel, click **Details** in the Details column of the task to view the details.
3. On the **Servers** tab of the failed step, click **View Details** in the Actions column of a failed server. The **Execution Output** tab appears in the Execution Details section. You can view the output to identify the cause of the failure.

11.2.5.3.2. Job Scheduler O&M

11.2.5.3.2.1. O&M features and entry

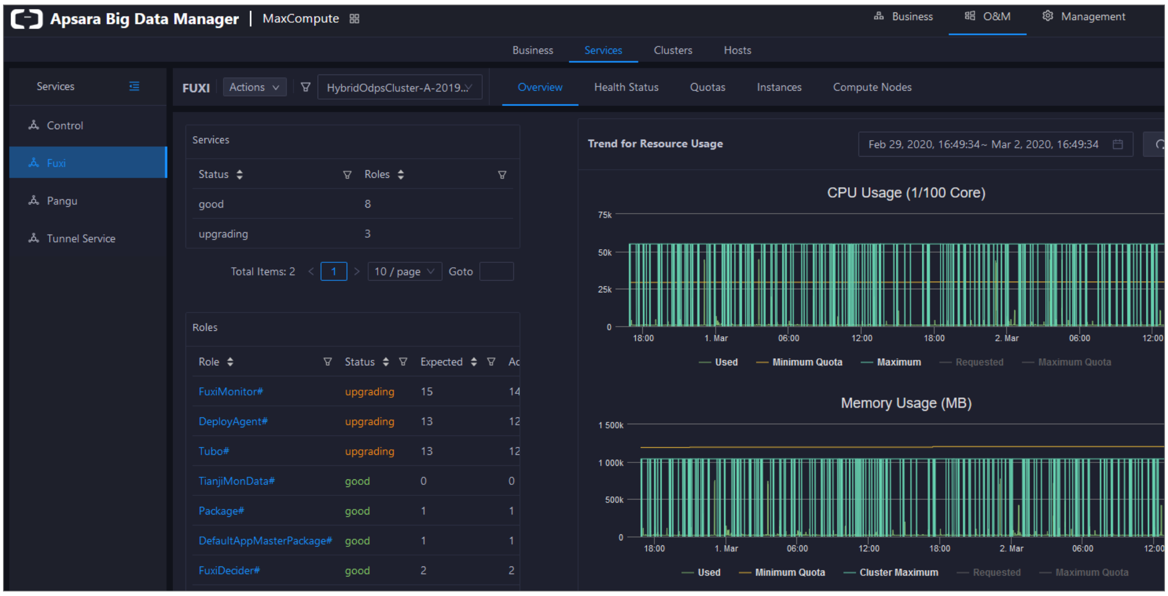
This topic describes Job Scheduler O&M features. It also provides more information about how to go to the Job Scheduler O&M page.

Job Scheduler O&M features

- Overview: displays the key operating information of Job Scheduler. The information includes the service overview, service status, resource usage, compute node overview, and the trend charts of CPU utilization and memory usage.
- Health Status: displays all checkers for Job Scheduler. You can query checker details, check results for hosts in a cluster, and schemes to clear alerts (if any exists). You can also log on to a host and perform manual checks on the host.
- Quotas: allows you to view, create, or modify the quota groups in Job Scheduler.
- Instances: displays information about the master nodes and server roles of Job Scheduler and allows you to restart the master nodes.
- Compute Nodes: displays all compute nodes in Job Scheduler and allows you to add compute nodes to or remove compute nodes from a blacklist or read-only list.
- Enable SQL Acceleration or Disable SQL Acceleration: allows you to enable or disable SQL acceleration for Job Scheduler.
- Restart Fuxi Master Node: allows you to restart the primary and secondary master nodes for Job Scheduler.

Go to the Job Scheduler O&M page

1. Log on to the Apsara Big Data Manager (ABM) console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Fuxi**. The **Overview** tab appears.



Apsara Big Data Manager | MaxCompute

Services

Status	Roles
good	8
upgrading	3

Total Items: 2 < 1 > 10 / page Goto

Roles

Role	Status	Expected	Ac
FuxiMonitor#	upgrading	15	14
DeployAgent#	upgrading	13	12
Tubo#	upgrading	13	12
TianjiMonData#	good	0	0
Package#	good	1	1
DefaultAppMasterPackage#	good	1	1
FuxiDecider#	good	2	2

Trend for Resource Usage

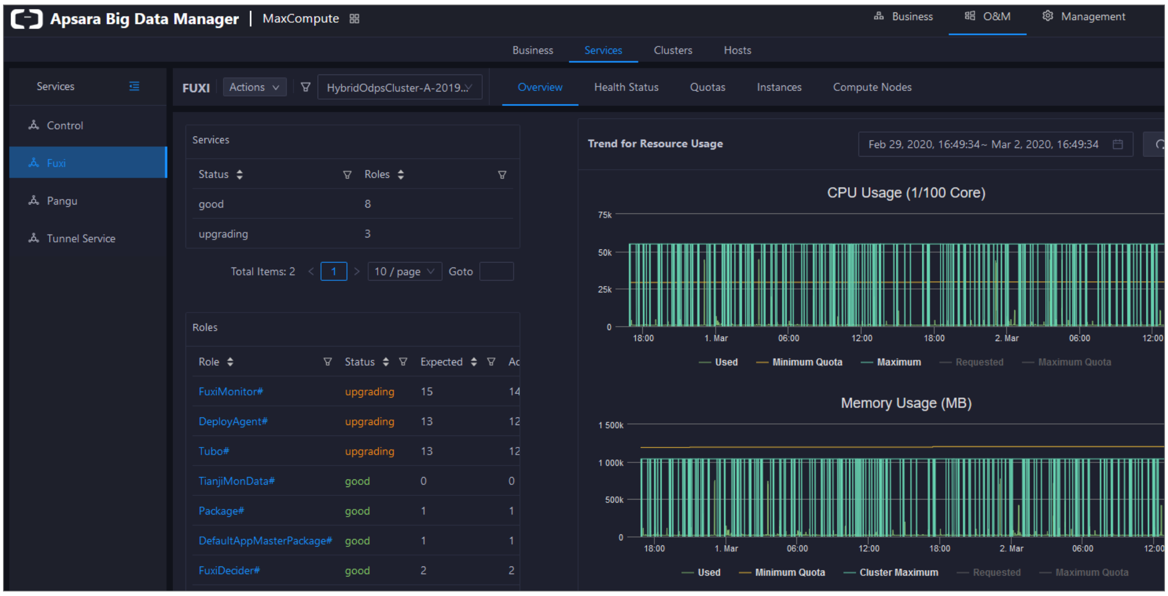
Feb 29, 2020, 16:49:34~ Mar 2, 2020, 16:49:34

11.2.5.3.2.2. Overview

The Overview tab shows the key operating information of Job Scheduler. The information includes the service overview, service status, resource usage, compute node overview, and the trend charts of CPU utilization and memory usage.

Go to the Overview tab

1. In the left-side navigation pane of the **Services** tab, click **Fuxi**.
2. Select a cluster and click the **Overview** tab. The **Overview** tab for the selected cluster appears.



Apsara Big Data Manager | MaxCompute

Services

Status	Roles
good	8
upgrading	3

Total Items: 2 < 1 > 10 / page Goto

Roles

Role	Status	Expected	Ac
FuxiMonitor#	upgrading	15	14
DeployAgent#	upgrading	13	12
Tubo#	upgrading	13	12
TianjiMonData#	good	0	0
Package#	good	1	1
DefaultAppMasterPackage#	good	1	1
FuxiDecider#	good	2	2

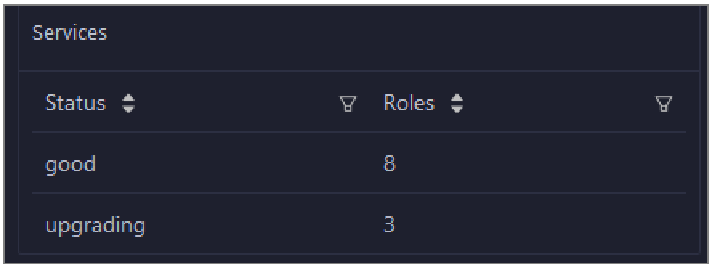
Trend for Resource Usage

Feb 29, 2020, 16:49:34~ Mar 2, 2020, 16:49:34

The **Overview** tab shows the key operating information of Job Scheduler. The information includes the service overview, service status, resource usage, compute node overview, and the trend charts of CPU utilization and memory usage.

Services

This section shows the numbers of available services, unavailable services, and services that are being updated.

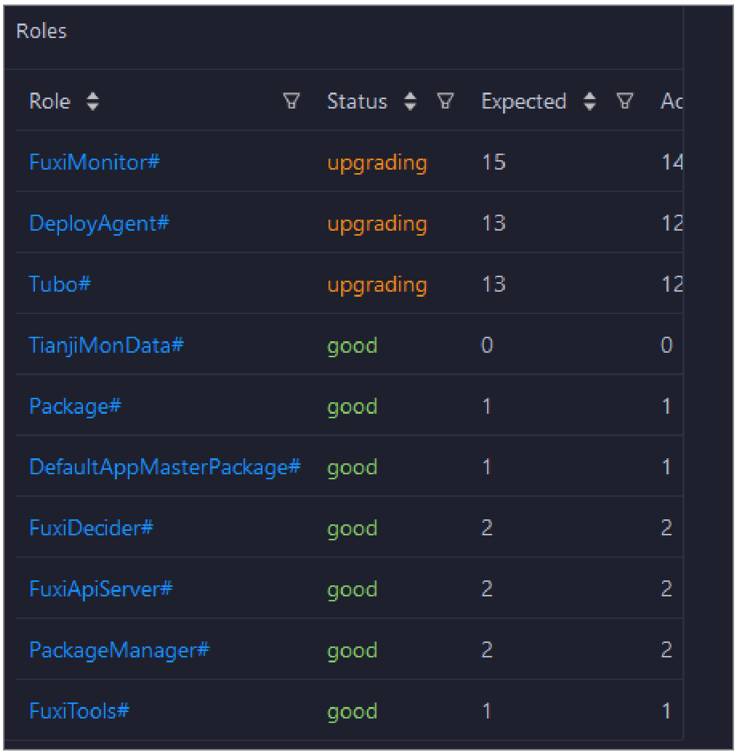


Services

Status	Roles
good	8
upgrading	3

Roles

This section shows all Job Scheduler server roles and their states. You can also view the expected and actual numbers of machines for each server role.



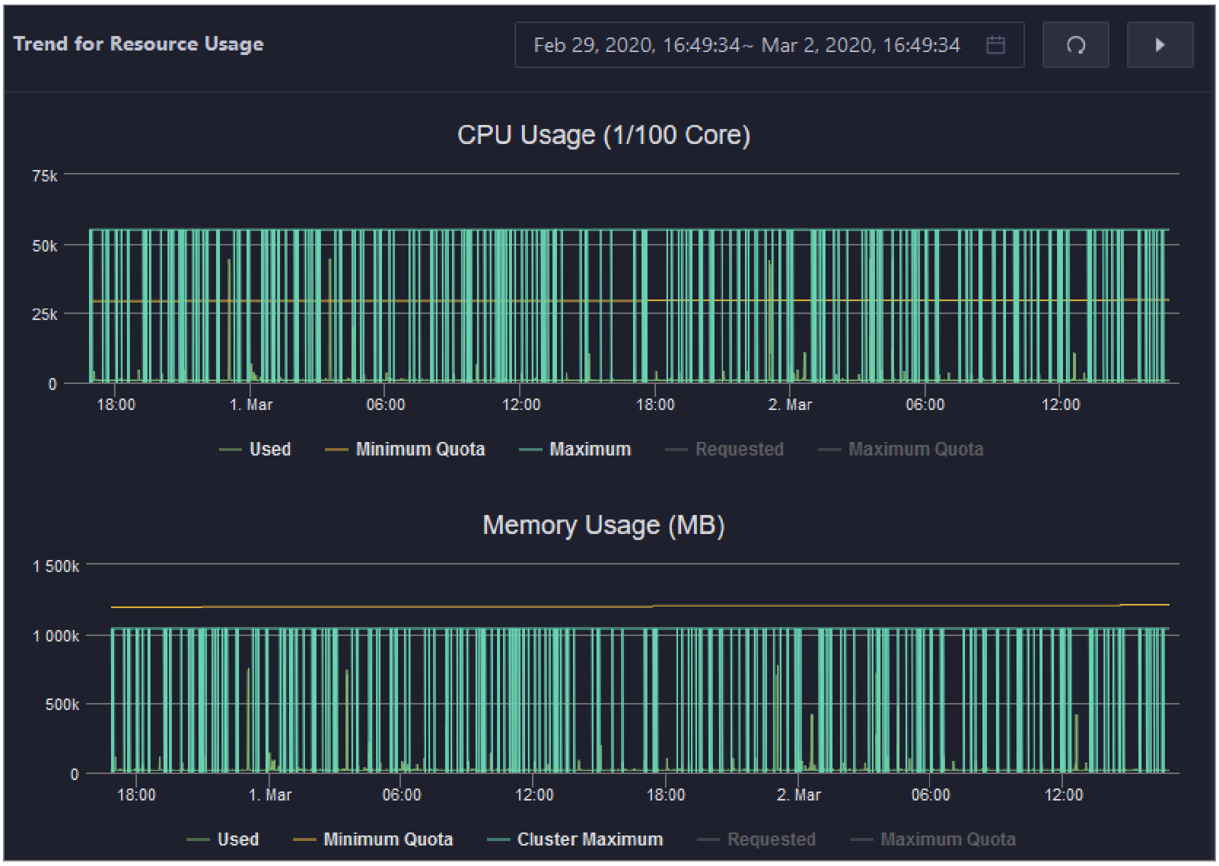
Roles

Role	Status	Expected	Ac
FuxiMonitor#	upgrading	15	14
DeployAgent#	upgrading	13	12
Tubo#	upgrading	13	12
TianjiMonData#	good	0	0
Package#	good	1	1
DefaultAppMasterPackage#	good	1	1
FuxiDecider#	good	2	2
FuxiApiServer#	good	2	2
PackageManager#	good	2	2
FuxiTools#	good	1	1

Click the name of a server role to go to the Apsara Infrastructure Management Framework console and view its details.

CPU Usage (1/100 Core) and Memory Usage (MB)

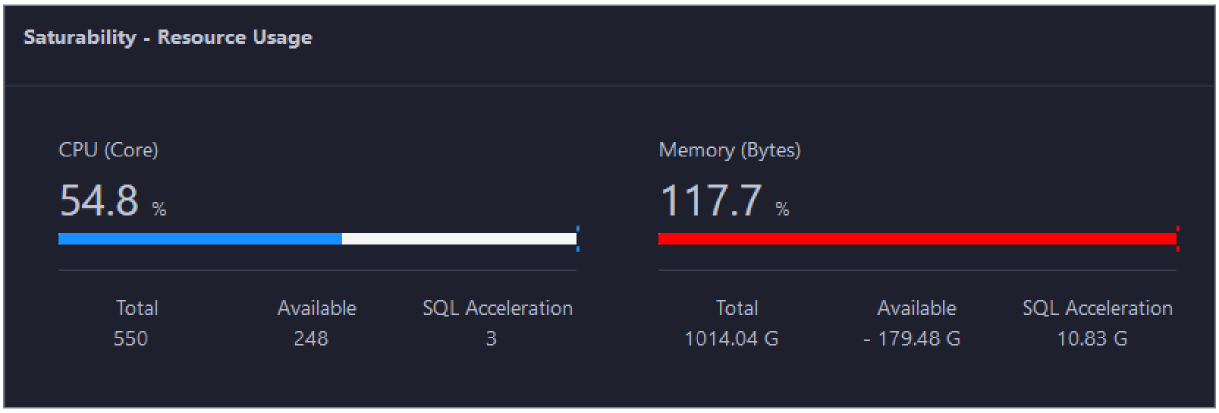
The Trend for Resource Usage section shows the trend charts of CPU utilization and memory usage for Job Scheduler. Each trend chart shows information about the used quota, minimum quota, maximum cluster quota, requested quota, and maximum quota in different colors. The trend charts are periodically refreshed. You can also manually refresh the trend charts. You can also view the trend charts of CPU utilization and memory usage for a specific period.



Saturability - Resource Usage

This section shows the allocation of CPU and memory resources.

- CPU (Core): shows the CPU utilization, the total number of CPU cores, the number of available CPU cores, and the CPU cores for SQL acceleration.
- Memory (Bytes): shows the memory usage, the total memory size, the available memory size, and the memory size for SQL acceleration.


Saturability - Resource Usage

CPU (Core)
54.8 %

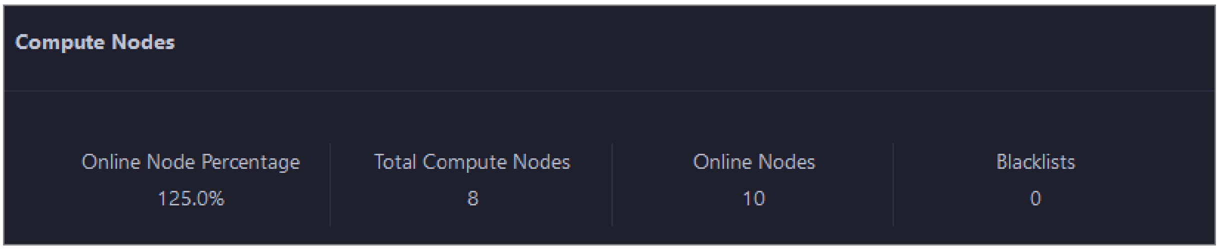
Total	Available	SQL Acceleration
550	248	3

Memory (Bytes)
117.7 %

Total	Available	SQL Acceleration
1014.04 G	- 179.48 G	10.83 G

Compute Nodes

This section shows the details of compute nodes in Job Scheduler. The details include the percentage of online compute nodes, the total number of compute nodes, the number of online compute nodes, and the number of compute nodes in a blacklist.



Compute Nodes

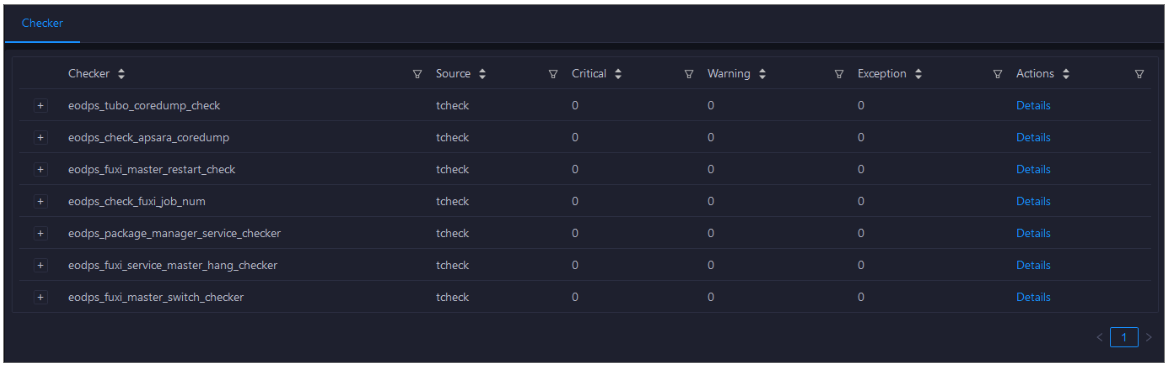
Online Node Percentage	Total Compute Nodes	Online Nodes	Blacklists
125.0%	8	10	0

11.2.5.3.2.3. Job Scheduler health

On the Health Status page for Job Scheduler, you can view all checkers of Job Scheduler, including the checker details, check results, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Entry

1. On the **Services** page, click **Fuxi** in the left-side navigation pane.
2. Select a cluster from the drop-down list, and then click the **Health Status** tab. The **Health Status** page for Job Scheduler appears.



	Checker	Source	Critical	Warning	Exception	Actions
+	eodps_tubo_coredump_check	tcheck	0	0	0	Details
+	eodps_check_apsara_coredump	tcheck	0	0	0	Details
+	eodps_fuxi_master_restart_check	tcheck	0	0	0	Details
+	eodps_check_fuxi_job_num	tcheck	0	0	0	Details
+	eodps_package_manager_service_checker	tcheck	0	0	0	Details
+	eodps_fuxi_service_master_hang_checker	tcheck	0	0	0	Details
+	eodps_fuxi_master_switch_checker	tcheck	0	0	0	Details

On the **Health Status** page, you can view all checkers of the Job Scheduler service and the check results for all hosts in the cluster. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

Supported operations

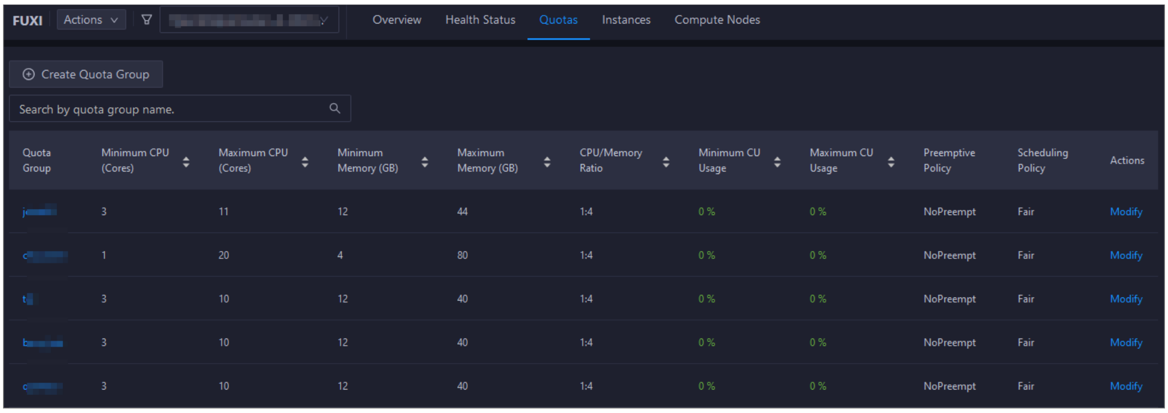
On the Health Status page, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host. For more information, see Cluster health.

11.2.5.3.2.4. Quotas

You can view, create, or modify quota groups in Job Scheduler on the Quotas tab. A quota group is used to allocate computing resources to MaxCompute projects, including CPU and memory resources.

Go to the Quotas tab

1. In the left-side navigation pane of the **Services** tab, click **Fuxi**.
2. Select a cluster and click the **Quotas** tab. The **Quotas** tab for the selected cluster appears.



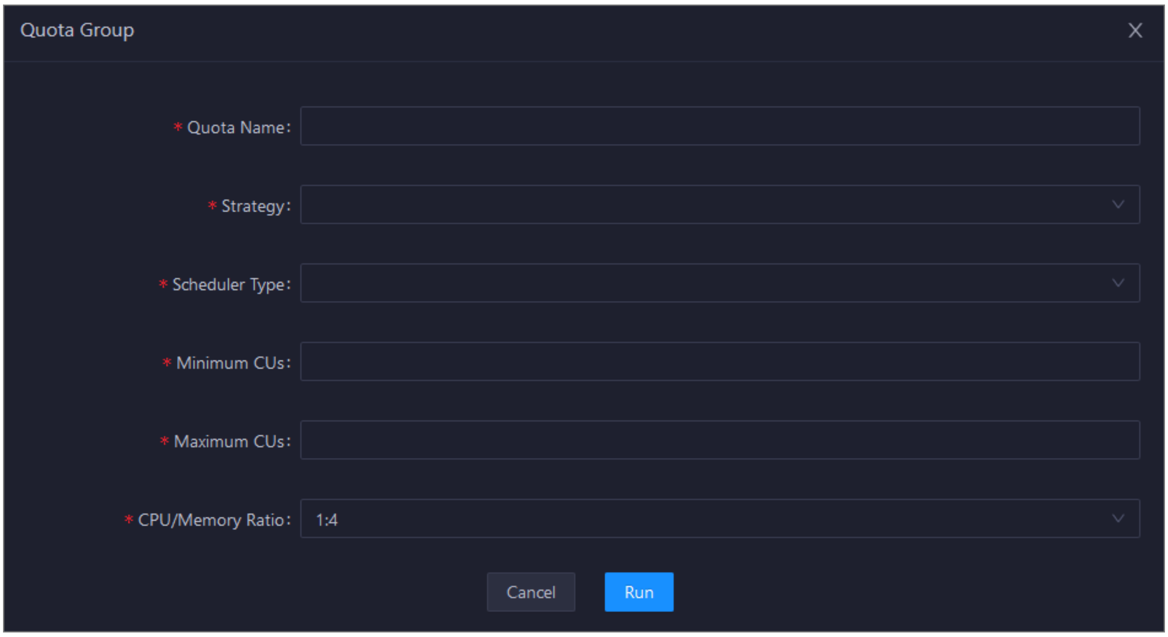
[redacted]

Quota Group	Minimum CPU (Cores)	Maximum CPU (Cores)	Minimum Memory (GB)	Maximum Memory (GB)	CPU/Memory Ratio	Minimum CU Usage	Maximum CU Usage	Preemptive Policy	Scheduling Policy	Actions
[redacted]	3	11	12	44	1:4	0 %	0 %	NoPreempt	Fair	Modify
[redacted]	1	20	4	80	1:4	0 %	0 %	NoPreempt	Fair	Modify
[redacted]	3	10	12	40	1:4	0 %	0 %	NoPreempt	Fair	Modify
[redacted]	3	10	12	40	1:4	0 %	0 %	NoPreempt	Fair	Modify
[redacted]	3	10	12	40	1:4	0 %	0 %	NoPreempt	Fair	Modify

The **Quotas** tab lists existing quota groups in Job Scheduler.

Create a quota group

1. In the upper-left corner of the **Quotas** tab, click **Create Quota Group**.
2. In the **Quota Group** pane, specify the required parameters.



* Quota Name:

* Strategy:

* Scheduler Type:

* Minimum CUs:

* Maximum CUs:

* CPU/Memory Ratio: 1:4

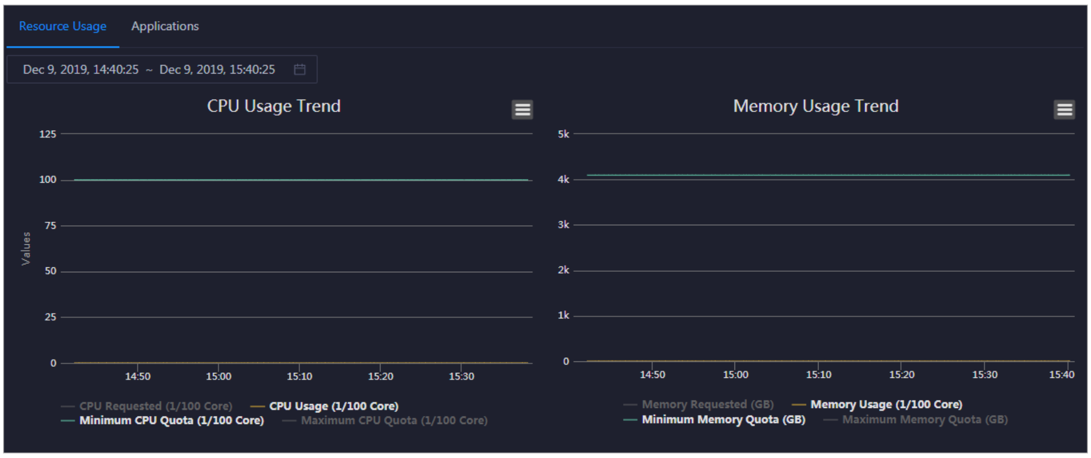
3. Click **Run**.

   The newly created quota group appears in the quota group list.

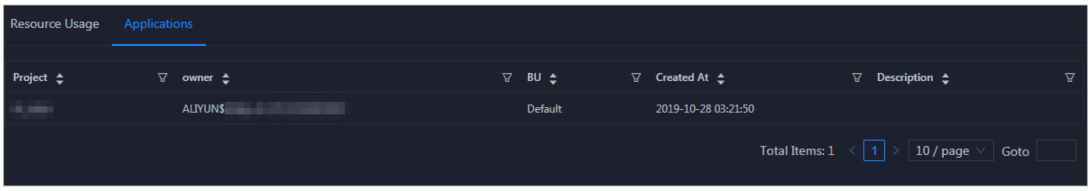
View quota group details

Click the name of a quota group to view its details. The **Resource Usage** tab shows the trend charts of CPU utilization and memory usage. The **Applications** tab shows the projects that use the quota group resources.

Resource usage


Resource Usage
Applications
Dec 9, 2019, 14:40:25 ~ Dec 9, 2019, 15:40:25
CPU Usage Trend
Values
125
100
75
50
25
0
14:50
15:00
15:10
15:20
15:30
CPU Requested (1/100 Core)
CPU Usage (1/100 Core)
Minimum CPU Quota (1/100 Core)
Maximum CPU Quota (1/100 Core)
Memory Usage Trend
5k
4k
3k
2k
1k
0
14:50
15:00
15:10
15:20
15:30
15:40
Memory Requested (GB)
Memory Usage (1/100 Core)
Minimum Memory Quota (GB)
Maximum Memory Quota (GB)

Applications



Project	owner	BU	Created At	Description
[redacted]	ALIYUN$[redacted]	Default	2019-10-28 03:21:50	

Modify a quota group

1. On the **Quotas** tab, find the quota group that you want to modify and click **Modify** in the Actions column. In the pane that appears, modify parameters as instructed.
2. Click **Run**.

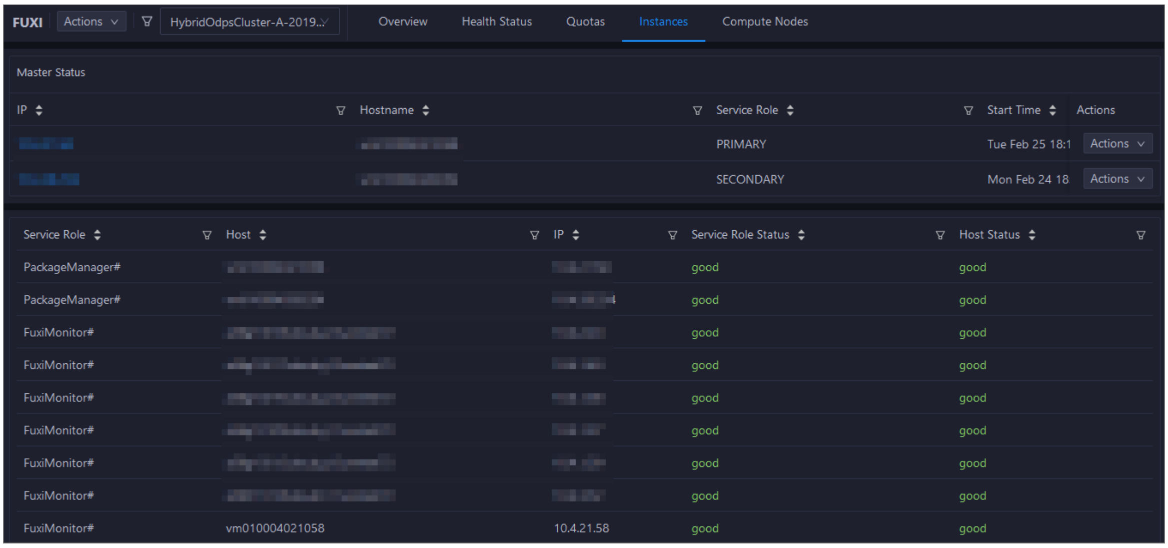
   After the configuration is complete, you can check whether the quota group is modified in the quota group list.

11.2.5.3.2.5. Instances

This topic describes how to view information about the master nodes and server roles of Job Scheduler and how to restart the master nodes.

Go to the Instances tab

1. In the left-side navigation pane of the **Services** tab, click **Fuxi**.
2. Select a cluster and click the **Instances** tab. The **Instances** tab for the selected cluster appears.



Master Status

IP	Hostname	Service Role	Start Time	Actions
[redacted]	[redacted]	PRIMARY	Tue Feb 25 18:1	Actions
[redacted]	[redacted]	SECONDARY	Mon Feb 24 18	Actions

Service Role	Host	IP	Service Role Status	Host Status
PackageManager#	[redacted]	[redacted]	good	good
PackageManager#	[redacted]	[redacted]	good	good
FuxiMonitor#	[redacted]	[redacted]	good	good
FuxiMonitor#	[redacted]	[redacted]	good	good
FuxiMonitor#	[redacted]	[redacted]	good	good
FuxiMonitor#	[redacted]	[redacted]	good	good
FuxiMonitor#	[redacted]	[redacted]	good	good
FuxiMonitor#	[redacted]	[redacted]	good	good
FuxiMonitor#	vm010004021058	10.4.21.58	good	good

The **Instances** tab shows information about the master nodes and server roles of Job Scheduler. The information about the master nodes includes the IP address, hostname, server role, and start time. The information about a server role includes the role name, hostname, role status, and host status.

Supported operations

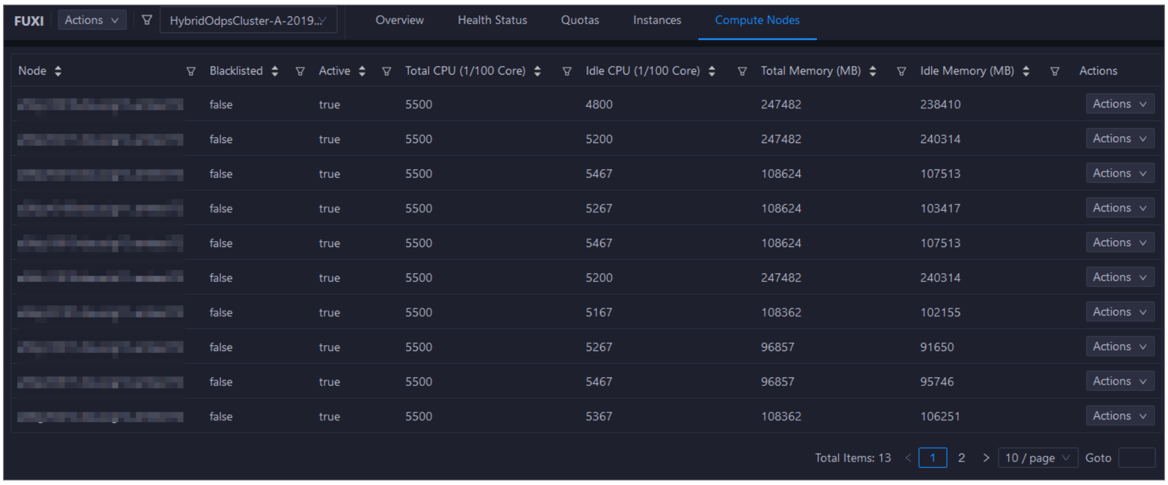
You can restart the master nodes of Job Scheduler. For more information, see Restart the primary master node of Job Scheduler.

11.2.5.3.2.6. Job Scheduler compute nodes

You can view the details of compute nodes on the Compute Nodes page for Job Scheduler, including the total CPU, idle CPU, total memory, and idle memory of each compute node. You can also check whether a node is added to the blacklist and whether it is active. In addition, you can add compute nodes to or remove compute nodes from the blacklist or read-only list on the Compute Nodes page.

Entry

1. On the **Services** page, click **Fuxi** in the left-side navigation pane.
2. Select a cluster from the drop-down list, and then click the **Compute Nodes** tab. The **Compute Nodes** page for Job Scheduler appears.



Node	Blacklisted	Active	Total CPU (1/100 Core)	Idle CPU (1/100 Core)	Total Memory (MB)	Idle Memory (MB)	Actions
[redacted]	false	true	5500	4800	247482	238410	Actions
[redacted]	false	true	5500	5200	247482	240314	Actions
[redacted]	false	true	5500	5467	108624	107513	Actions
[redacted]	false	true	5500	5267	108624	103417	Actions
[redacted]	false	true	5500	5467	108624	107513	Actions
[redacted]	false	true	5500	5200	247482	240314	Actions
[redacted]	false	true	5500	5167	108362	102155	Actions
[redacted]	false	true	5500	5267	96857	91650	Actions
[redacted]	false	true	5500	5467	96857	95746	Actions
[redacted]	false	true	5500	5367	108362	106251	Actions

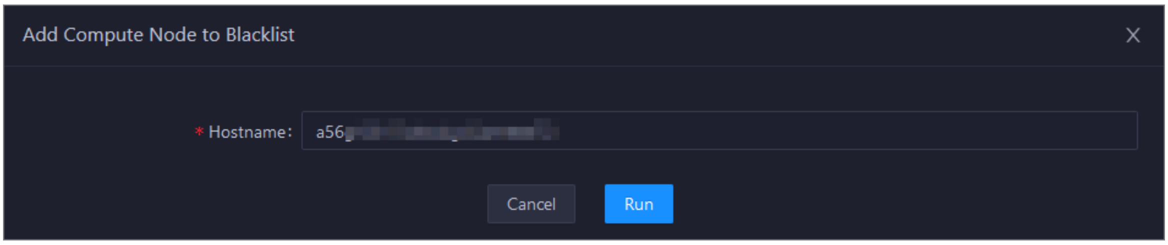
Total Items: 13 < 1 2 > 10 / page Goto

You can view the details of compute nodes on the Compute Nodes page for Job Scheduler, including the total CPU, idle CPU, total memory, and idle memory of each compute node. You can also check whether a node is added to the blacklist and whether it is active.

Blacklist and read-only setting

You can add compute nodes to or remove compute nodes from the blacklist or read-only list. To add compute nodes to the blacklist, follow these steps:

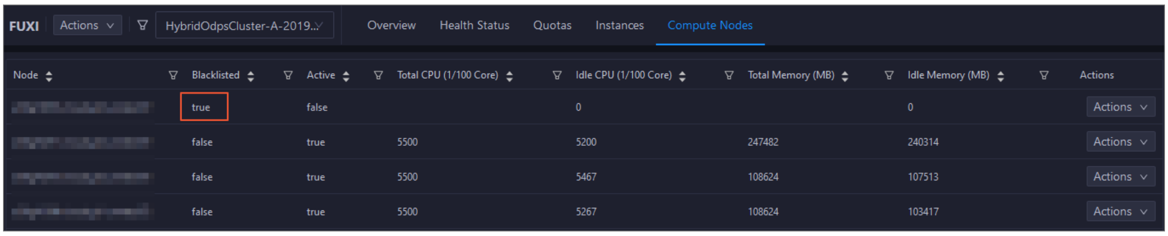
1. On the **Compute Nodes** page, click **Actions** for the target compute node and then select **Add to Blacklist**.
2. In the dialog box that appears, click **Run**. A message appears, indicating that the action has been submitted.



* Hostname: a56[redacted]

The value of the **Hostname** parameter is automatically filled. You do not need to specify a value for this parameter.

You can check whether a compute node is added to the blacklist in the compute node list after the configuration is completed.



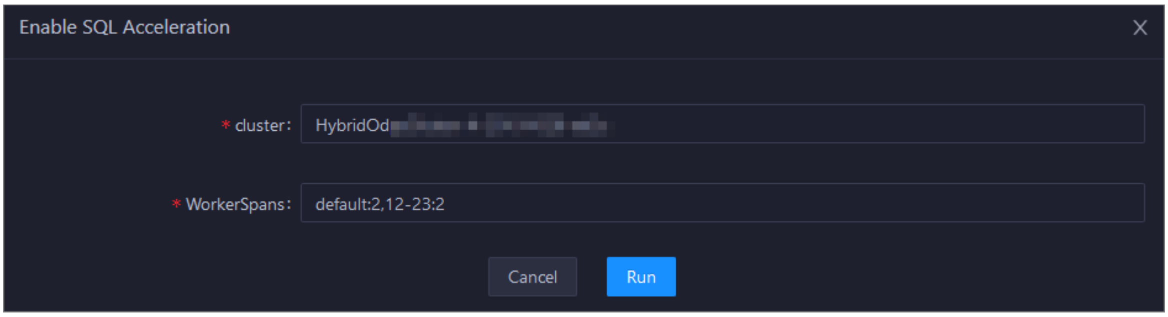
Node	Blacklisted	Active	Total CPU (1/100 Core)	Idle CPU (1/100 Core)	Total Memory (MB)	Idle Memory (MB)	Actions
[redacted]	true	false		0		0	Actions
[redacted]	false	true	5500	5200	247482	240314	Actions
[redacted]	false	true	5500	5467	108624	107513	Actions
[redacted]	false	true	5500	5267	108624	103417	Actions

11.2.5.3.2.7. Enable and disable SQL acceleration

You can enable or disable SQL acceleration for Job Scheduler in the Apsara Big Data Manager (ABM) console. The execution speed of SQL statements in Job Scheduler is greatly increased with SQL acceleration enabled, but more computing resources are consumed.

Enable SQL acceleration

1. In the left-side navigation pane of the **Services** tab, click **Fuxi**. Then, select a cluster.
2. In the upper-right corner of the tab that appears, choose **Actions** > **Enable SQL Acceleration**.
3. In the Enable SQL Acceleration panel, set the **WorkerSpans** parameter.



Enable SQL Acceleration

* cluster: HybridOd[redacted]

* WorkerSpans: default:2,12-23:2

WorkerSpans: the default resource quota of the cluster and the resource quota for a specific period. Default value: **default:2,12-23:2**.

> **Note** The default value indicates that the default resource quota is 2 and the resource quota for the period from 12:00 to 23:00 is also 2. You can set the resource quota as needed. For example, you can set this parameter to default:2,12-23:4 to increase the resource quota in peak hours.

4. Click **Run**.

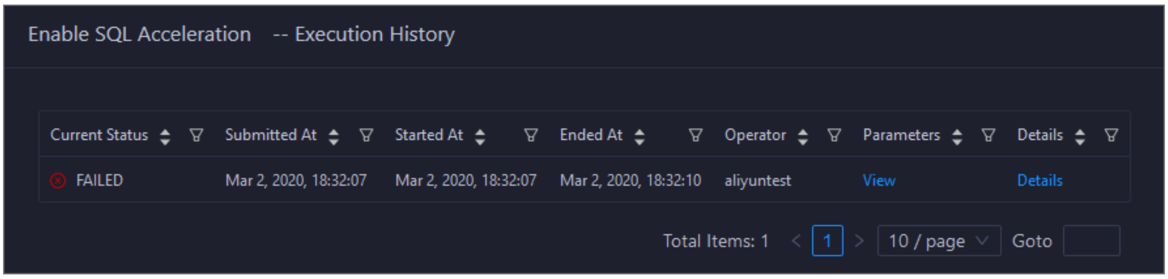
Disable SQL acceleration

1. In the left-side navigation pane of the **Services** tab, click **Fuxi**. Then, select a cluster.
2. In the upper-right corner of the tab that appears, choose **Actions** > **Disable SQL Acceleration**.
3. In the Disable SQL Acceleration panel, click **Run**.

View the execution history of enabling or disabling SQL acceleration

After you submit the action of enabling or disabling SQL acceleration, you can view the execution history to check whether the action is complete. The system executes the action as a job. It provides execution records and logs for each execution so that you can identify faults encountered during its execution. This section describes how to view the execution history of enabling SQL acceleration.

1. In the left-side navigation pane of the **Services** tab, click **Fuxi**. Then, select a cluster.
2. In the upper-right corner of the tab that appears, click **Actions** and select **Execution History** next to **Enable SQL Acceleration**.
3. In the Execution History panel, view the execution history of enabling SQL acceleration.



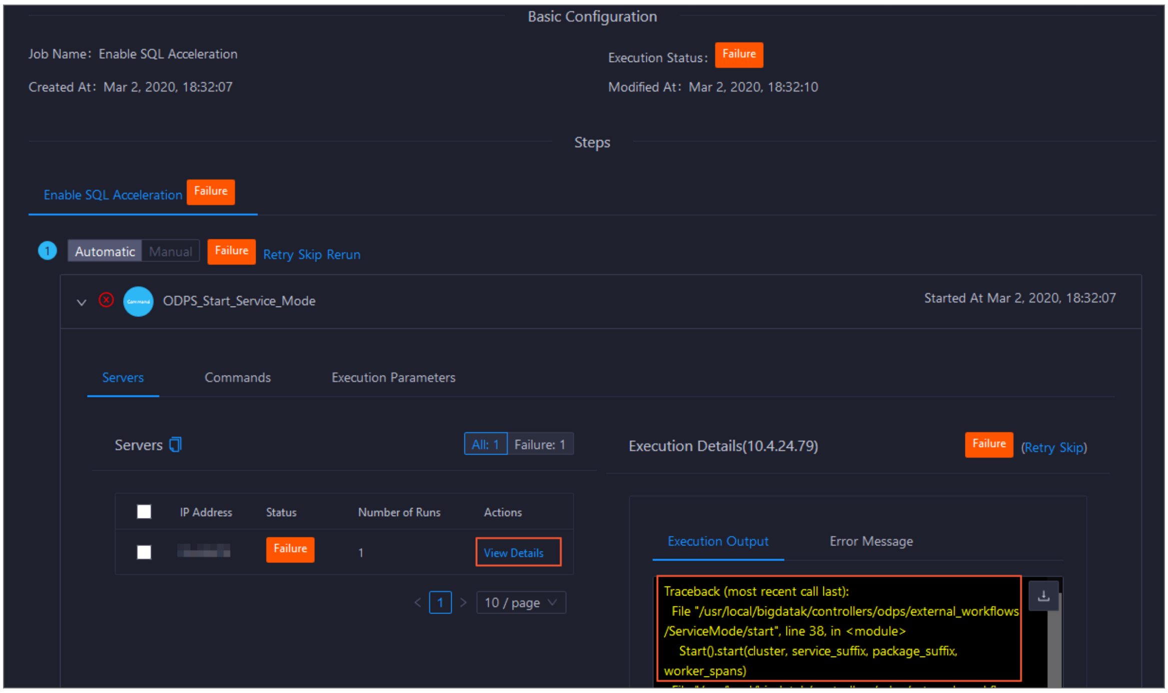
Enable SQL Acceleration -- Execution History

Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
⊗ FAILED	Mar 2, 2020, 18:32:07	Mar 2, 2020, 18:32:07	Mar 2, 2020, 18:32:10	aliyuntest	View	Details

Total Items: 1 < 1 > 10 / page Goto

The execution history shows the current status, submission time, start time, end time, and operator of each execution.

4. If the execution fails, click **Details** in the Details column to identify the cause of the failure.



Basic Configuration

Job Name: Enable SQL Acceleration

Execution Status: Failure

Created At: Mar 2, 2020, 18:32:07

Modified At: Mar 2, 2020, 18:32:10

Steps

Started At Mar 2, 2020, 18:32:07

Execution Details(10.4.24.79)

□	IP Address	Status	Number of Runs	Actions
□	[redacted]	Failure	1	View Details

```
Traceback (most recent call last):
  File "/usr/local/bigdatak/controllers/odps/external_workflows
/ServiceMode/start", line 38, in <module>
    Start().start(cluster, service_suffix, package_suffix,
worker_spans)
```

11.2.5.3.2.8. Restart a master node of Job Scheduler

Job Scheduler is the resource management and task scheduling system of the Apsara distributed operating system. Apsara Big Data Manager (ABM) allows you to quickly restart the primary and secondary master nodes of Job Scheduler. Cluster services are not affected during the restart process.

Prerequisites

Your ABM account is granted the required permissions to perform O&M operations on MaxCompute.

Step 1: Restart a master node of Job Scheduler

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Fuxi**. Then, click the **Instances** tab.
5. On the **Instances** tab, choose **Actions** > **Restart Fuxi Master Node** in the Actions column of a primary or secondary master node.
6. In the **Restart Fuxi Master Node** panel, click **Run**. The **Restart Fuxi Master Node** panel appears.

Step 2: View the execution status or progress

1. In the **Restart Fuxi Master Node** panel, check the execution history of restarting master nodes.

   The **Restart Fuxi Master Node** panel displays the restart history. **RUNNING** indicates that the execution is in progress. **SUCCESS** indicates that the execution succeeds. **FAILED** indicates that the execution fails.
2. If the status is **RUNNING**, click **Details** in the Details column to view the execution progress.

Step 3: (Optional) Identify the cause of a failure

If the status is **FAILED**, you can view the execution logs to identify the cause of the failure.

1. In the **Restart Fuxi Master Node** panel, check the execution history of restarting master nodes.
2. Click **Details** in the Details column of the task to view the details.
3. On the **Servers** tab of the failed step, click **View Details** in the Actions column of a failed server. The **Execution Output** tab appears in the Execution Details section. You can view the output to identify the cause of the failure.

11.2.5.3.3. Apsara Distribute File System O&M

11.2.5.3.3.1. O&M features and entry

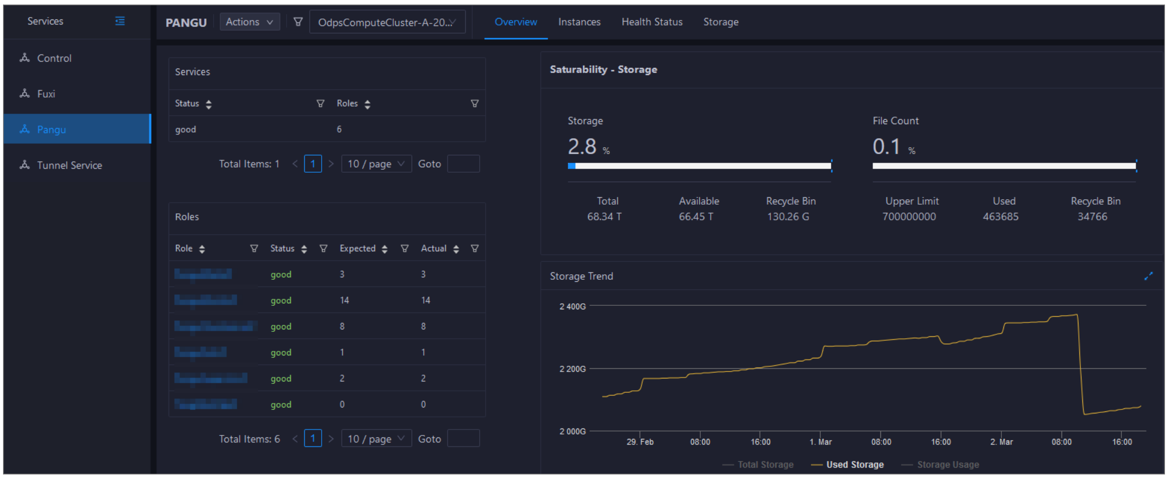
This topic describes the O&M features of Apsara Distributed File System. It also provides more information about how to go to the Apsara Distributed File System O&M page.

Apsara Distributed File System O&M features

- Overview: shows the key operating information of Apsara Distributed File System. The information includes the service overview, service status, storage usage, storage node overview, and the trend charts of storage usage and file count.
- Health Status: shows all checkers for Apsara Distributed File System. You can query checker details, check results for hosts in a cluster, and schemes to clear alerts (if any exists). You can also log on to a host and perform manual checks on the host.
- Instances: shows information about the master nodes and server roles of Apsara Distributed File System. You can change the primary master node or run a checkpoint on a master node of Apsara Distributed File System.
- Storage Nodes: shows information about the storage nodes of Apsara Distributed File System. You can set the status of a storage node to Disabled or Normal. You can also set the status of a disk on a storage node to Normal or Error.
- Change Primary Master Node: allows you to change the primary master node of Apsara Distributed File System in a cluster.
- Run Checkpoint on Master Node: allows you to run checkpoints on master nodes of Apsara Distributed File System to write memory data to disks.
- Empty Recycle Bin: allows you to clear the recycle bin of Apsara Distributed File System.
- Enable Data Rebalancing or Disable Data Rebalancing: allows you to enable or disable the data rebalancing feature of Apsara Distributed File System.

Go to the Pangu page

1. Log on to the Apsara Big Data Manager (ABM) console.
2. In the upper-left corner, click the ▦ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Pangu**. Then, select a cluster. The **Overview** tab for the selected cluster appears.



Services

Status	Roles
good	6

Total Items: 1 < 1 > 10 / page Goto

Roles

Role	Status	Expected	Actual
[redacted]	good	3	3
[redacted]	good	14	14
[redacted]	good	8	8
[redacted]	good	1	1
[redacted]	good	2	2
[redacted]	good	0	0

Total Items: 6 < 1 > 10 / page Goto

Saturability - Storage

Storage 2.8 %

Total	Available	Recycle Bin
68.34 T	66.45 T	130.26 G

File Count 0.1 %

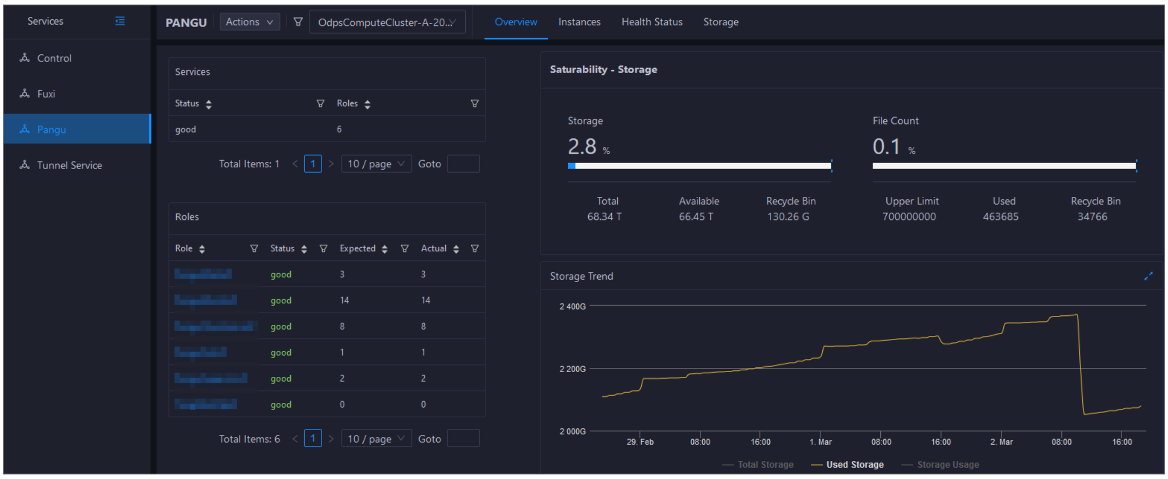
Upper Limit	Used	Recycle Bin
700000000	463685	34766

11.2.5.3.3.2. Overview

The Overview tab shows the key operating information about Apsara Distributed File System. The information includes the service overview, service status, storage usage, storage node overview, and the trend charts of storage usage and file count.

Go to the Overview tab

1. In the left-side navigation pane of the **Services** tab, click **Pangu**.
2. Select a cluster and click the **Overview** tab. The **Overview** tab for the selected cluster appears.



Services

Status	Roles
good	6

Total Items: 1 < 1 > 10 / page Goto

Roles

Role	Status	Expected	Actual
[redacted]	good	3	3
[redacted]	good	14	14
[redacted]	good	8	8
[redacted]	good	1	1
[redacted]	good	2	2
[redacted]	good	0	0

Total Items: 6 < 1 > 10 / page Goto

Saturability - Storage

Storage 2.8 %

Total	Available	Recycle Bin
68.34 T	66.45 T	130.26 G

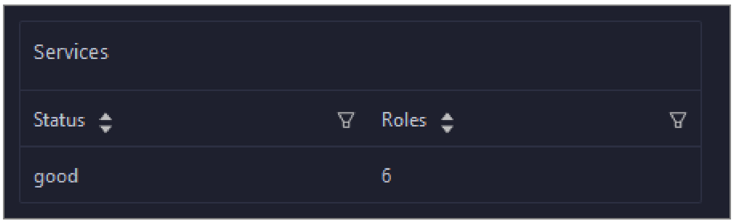
File Count 0.1 %

Upper Limit	Used	Recycle Bin
700000000	463685	34766

The **Overview** tab shows the key operating information about Apsara Distributed File System. The information includes the service overview, service status, health check result, health check history, storage usage, storage node overview, and the trend charts of storage usage and file count.

Services

This section shows the status of Apsara Distributed File System and the number of server roles.

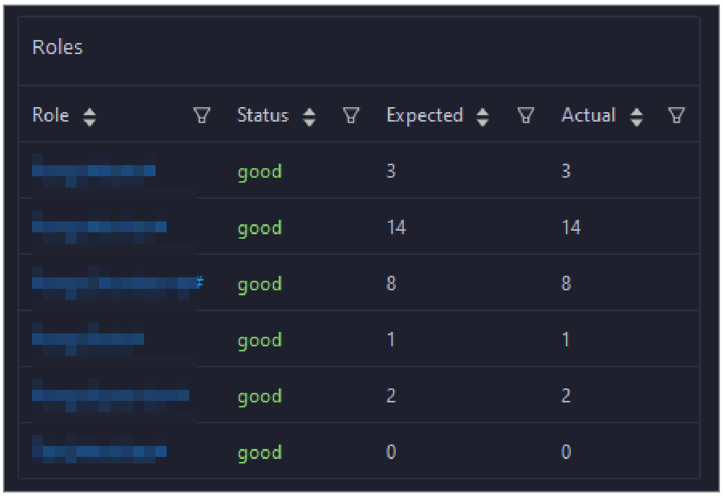


Services

Status	Roles
good	6

Roles

This section shows all server roles of Apsara Distributed File System and their states. You can also view the expected and actual numbers of hosts for each server role.



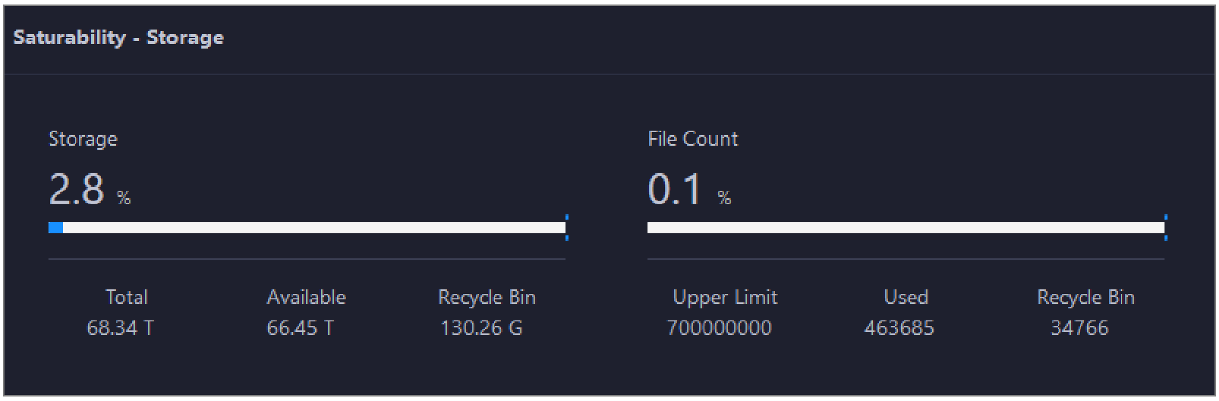
Roles

Role	Status	Expected	Actual
[redacted]	good	3	3
[redacted]	good	14	14
[redacted]	good	8	8
[redacted]	good	1	1
[redacted]	good	2	2
[redacted]	good	0	0

Saturability - Storage

This section shows the storage usage and file count.

- Storage: shows the storage usage, total storage space, available storage space, and recycle bin size.
- File Count: shows the file count usage, maximum number of files, number of existing files, and number of files in the recycle bin.



Saturability - Storage

Storage
2.8 %

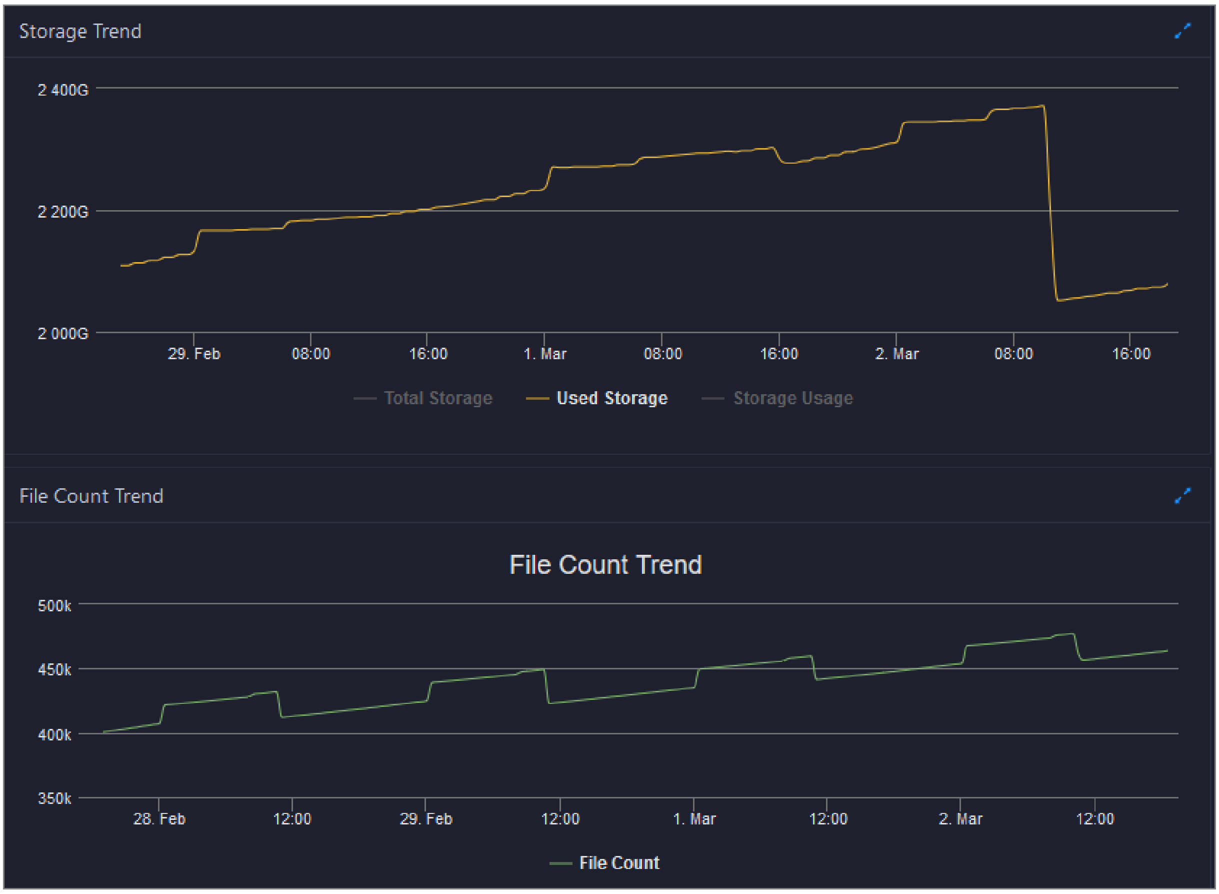
Total	Available	Recycle Bin
68.34 T	66.45 T	130.26 G

File Count
0.1 %

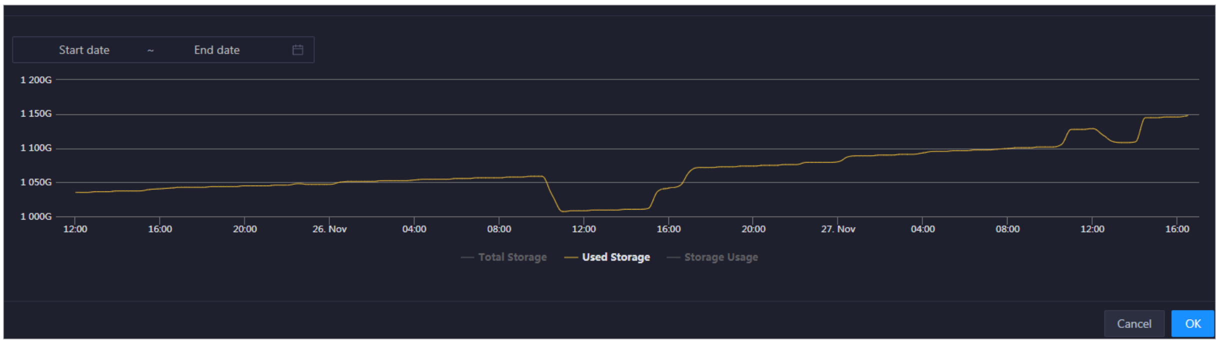
Upper Limit	Used	Recycle Bin
700000000	463685	34766

Storage Trend and File Count Trend

This section shows the trend charts of the storage usage and file count. The storage usage chart shows the trend lines of the total storage space, used storage space, and storage usage in different colors. The file count chart shows the trend line of the file count.



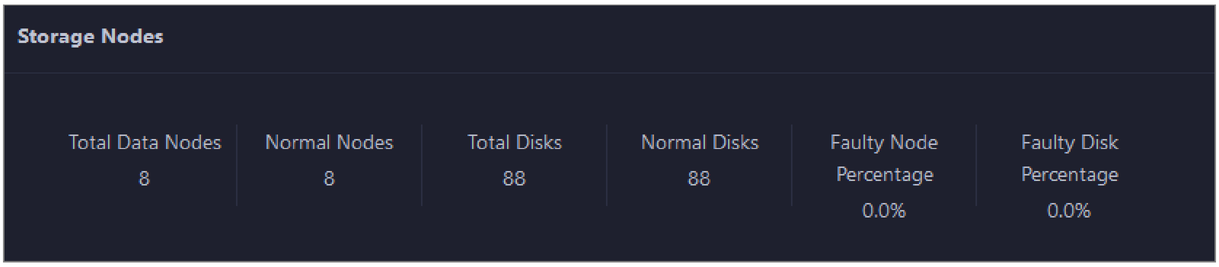
In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart. The following figure shows an enlarged chart of storage usage.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

Storage Nodes

This section shows information about the storage nodes of Apsara Distributed File System. The information includes the numbers of data nodes, normal nodes, disks, and normal disks. You can also view the faulty node percentage and faulty disk percentage.



Storage Nodes

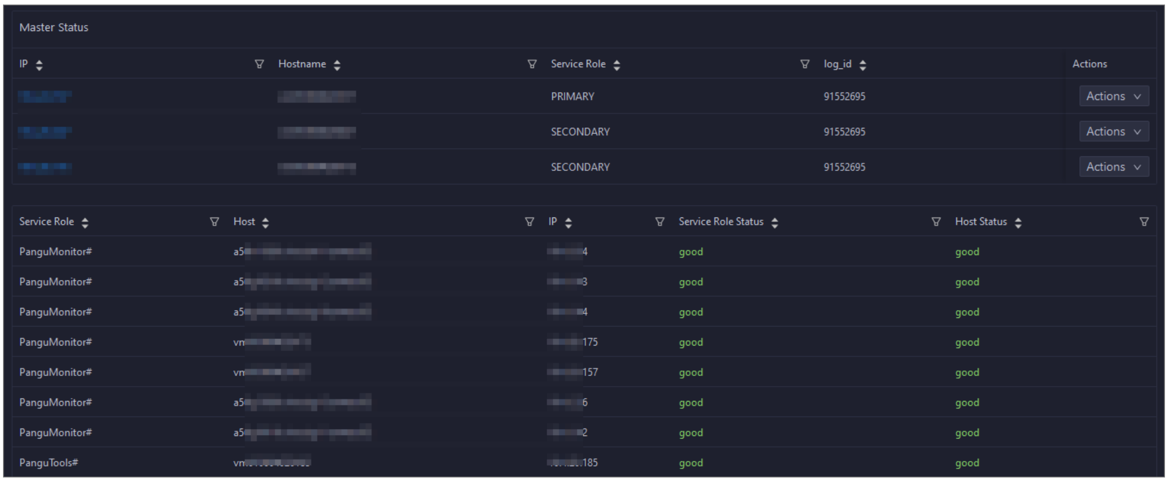
Total Data Nodes	Normal Nodes	Total Disks	Normal Disks	Faulty Node Percentage	Faulty Disk Percentage
8	8	88	88	0.0%	0.0%

11.2.5.3.3.3. Instances

This topic describes how to view information about the master nodes and server roles of Apsara Distributed File System. It also describes how to change the primary master node or run a checkpoint on a master node of Apsara Distributed File System.

Go to the Instances tab

1. In the left-side navigation pane of the **Services** tab, click **Pangu**.
2. Select a cluster and click the **Instances** tab. The **Instances** tab for the selected cluster appears.



Master Status

IP	Hostname	Service Role	log_id	Actions
[redacted]	[redacted]	PRIMARY	91552695	Actions
[redacted]	[redacted]	SECONDARY	91552695	Actions
[redacted]	[redacted]	SECONDARY	91552695	Actions

Service Role	Host	IP	Service Role Status	Host Status
PanguMonitor#	a5[redacted]	[redacted]4	good	good
PanguMonitor#	a5[redacted]	[redacted]3	good	good
PanguMonitor#	a5[redacted]	[redacted]4	good	good
PanguMonitor#	vn[redacted]	[redacted]175	good	good
PanguMonitor#	vn[redacted]	[redacted]157	good	good
PanguMonitor#	a5[redacted]	[redacted]6	good	good
PanguMonitor#	a5[redacted]	[redacted]2	good	good
PanguTools#	vn[redacted]	[redacted]185	good	good

The **Instances** tab shows information about the master nodes and server roles of Apsara Distributed File System. The information about a master node includes the IP address, hostname, server role, and log ID. The information about a server role includes the role name, hostname, role status, and host status.

Supported operations

You can change the primary master node or run a checkpoint on a master node of Apsara Distributed File System. For more information, see Change the primary master node for Apsara Distributed File System and Run a checkpoint on the master nodes of Apsara Distributed File System.

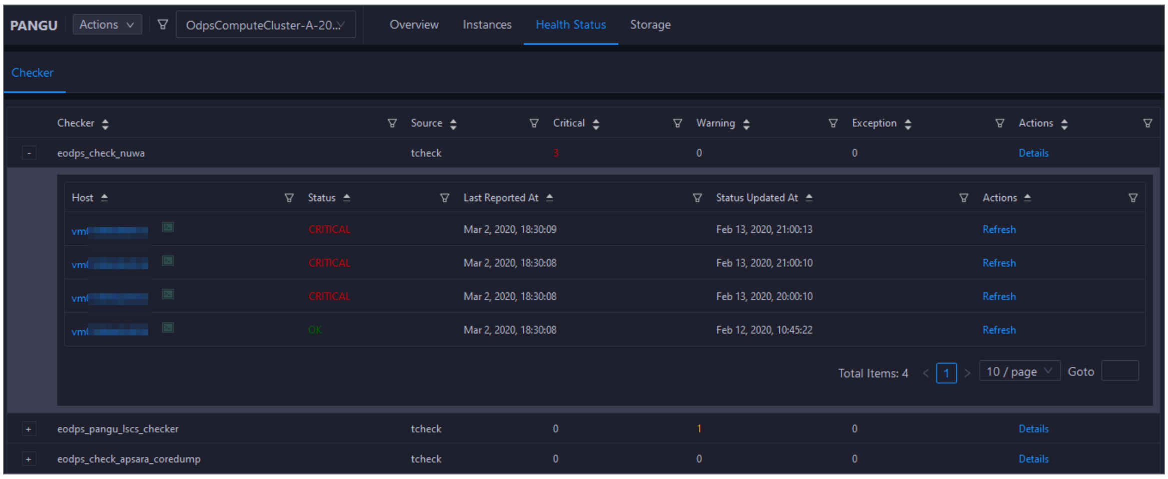
11.2.5.3.3.4. Apsara Distributed File System health

On the Health Status page for Apsara Distributed File System, you can view all checkers of Apsara Distributed File System, including the checker details, check results, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Entry

1. On the **Services** page, click **Pangu** in the left-side navigation pane.

2. Select a cluster from the drop-down list, and then click the **Health Status** tab. The **Health Status** page for Apsara Distributed File System appears.



	Checker	Source	Critical	Warning	Exception	Actions
-	eodps_check_nuwa	tcheck	3	0	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
vm[redacted]	CRITICAL	Mar 2, 2020, 18:30:09	Feb 13, 2020, 21:00:13	Refresh
vm[redacted]	CRITICAL	Mar 2, 2020, 18:30:08	Feb 13, 2020, 21:00:10	Refresh
vm[redacted]	CRITICAL	Mar 2, 2020, 18:30:08	Feb 13, 2020, 20:00:10	Refresh
vm[redacted]	OK	Mar 2, 2020, 18:30:08	Feb 12, 2020, 10:45:22	Refresh

Total Items: 4 < 1 > 10 / page Goto

	Checker	Source	Critical	Warning	Exception	Actions
+	eodps_pangu_lscs_checker	tcheck	0	1	0	Details
+	eodps_check_apsara_coredump	tcheck	0	0	0	Details

On the **Health Status** page, you can view all checkers of Apsara Distributed File System and the check results for all hosts in the cluster. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

Supported operations

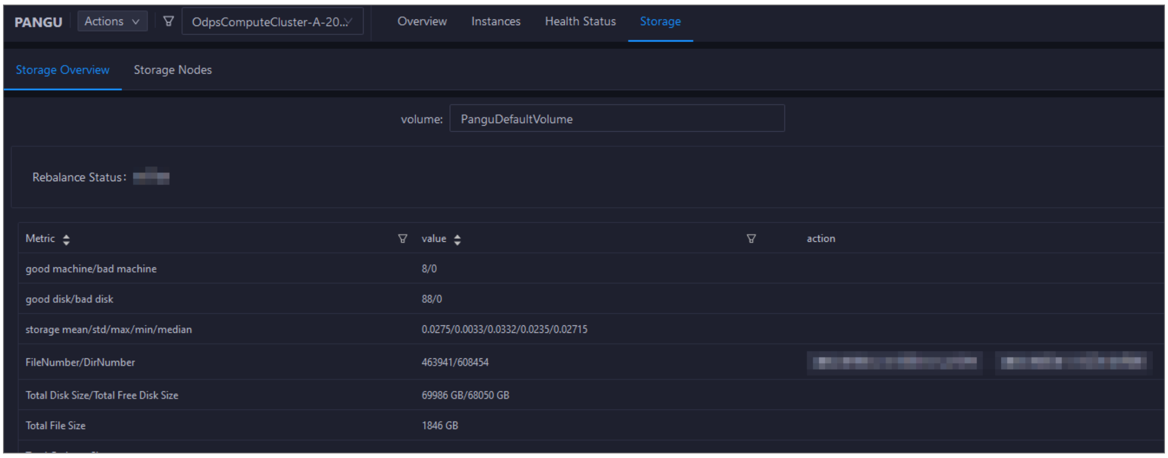
On the Health Status page, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host. For more information, see Cluster health.

11.2.5.3.3.5. Apsara Distributed File System storage

This topic describes how to view the storage overview and storage node information of Apsara Distributed File System, and how to set the status of storage nodes and data disks.

Entry to the Storage Overview page

1. On the **Services** page, click **Pangu** in the left-side navigation pane.
2. Select a cluster from the drop-down list, and then click the **Storage** tab. The **Storage Overview** page for Apsara Distributed File System appears.



volume: PanguDefaultVolume

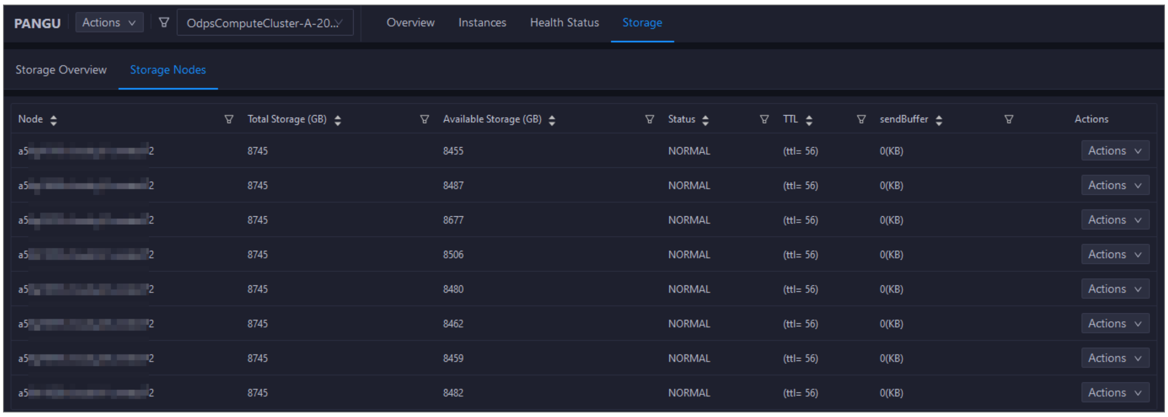
Rebalance Status: [redacted]

Metric	value	action
good machine/bad machine	8/0	
good disk/bad disk	88/0	
storage mean/std/max/min/median	0.0275/0.0033/0.0332/0.0235/0.02715	
FileNumber/DirNumber	463941/608454	[redacted] [redacted]
Total Disk Size/Total Free Disk Size	69986 GB/68050 GB	
Total File Size	1846 GB	

The **Storage Overview** page displays whether data rebalancing is enabled, key metrics and their values, suggestions to handle exceptions, and rack specifications of Apsara Distributed File System. The **Storage Nodes** page displays the information about all storage nodes of Apsara Distributed File System, including the total storage size, available storage size, status, time to live (TTL), and send buffer size. You can also set the status of storage nodes and data disks on this page.

Entry to the Storage Nodes page

1. On the **Services** page, click **Pangu** in the left-side navigation pane.
2. Select a cluster from the drop-down list, and then click the **Storage** tab. The **Storage Overview** page for Apsara Distributed File System appears.
3. Click the **Storage Nodes** tab. The **Storage Nodes** page appears.



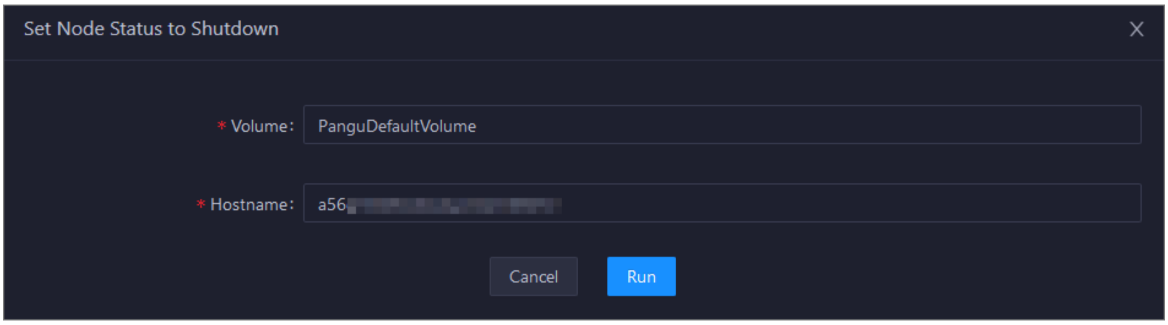
Node	Total Storage (GB)	Available Storage (GB)	Status	TTL	sendBuffer	Actions
a5[redacted]2	8745	8455	NORMAL	(ttl= 56)	0(KB)	Actions
a5[redacted]2	8745	8487	NORMAL	(ttl= 56)	0(KB)	Actions
a5[redacted]2	8745	8677	NORMAL	(ttl= 56)	0(KB)	Actions
a5[redacted]2	8745	8506	NORMAL	(ttl= 56)	0(KB)	Actions
a5[redacted]2	8745	8480	NORMAL	(ttl= 56)	0(KB)	Actions
a5[redacted]2	8745	8462	NORMAL	(ttl= 56)	0(KB)	Actions
a5[redacted]2	8745	8459	NORMAL	(ttl= 56)	0(KB)	Actions
a5[redacted]2	8745	8482	NORMAL	(ttl= 56)	0(KB)	Actions

The **Storage Nodes** page displays the information about all storage nodes of Apsara Distributed File System, including the total storage size, available storage size, status, TTL, and send buffer size.

Set the storage node status

You can set the storage node status to Disabled or Normal. This section describes how to set the status of a storage node to Disabled.

1. On the **Storage Nodes** page, find the target storage node and choose **Actions** > **Set Node Status to Disabled** in the Actions column.
2. In the dialog box that appears, click **Run**. A message appears, indicating that the action has been submitted.



* Volume: PanguDefaultVolume

* Hostname: a56[redacted]

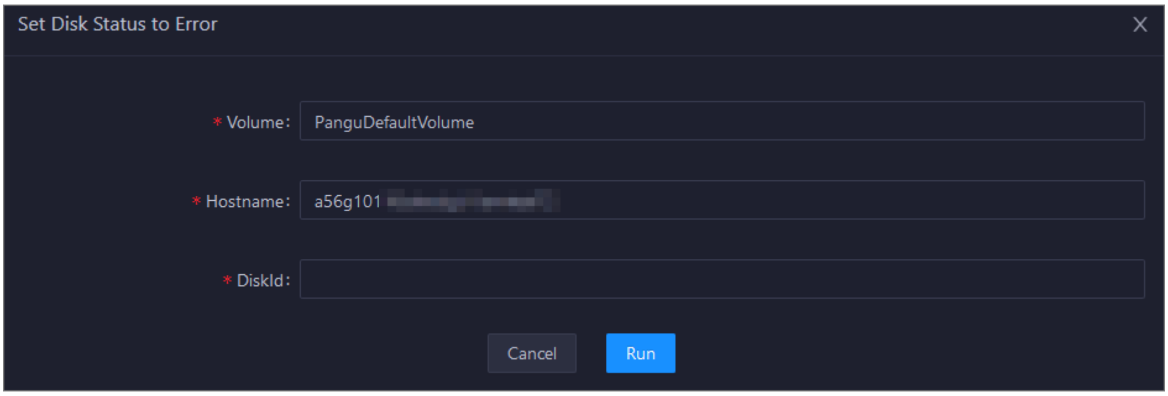
The values of the **Volume** and **Hostname** parameters are automatically filled based on the selected storage node. You do not need to specify values for the parameters.

You can check whether the status of storage node is changed in the storage node list.

Set the data disk status

You can set the data disk status to Error or Normal. This section describes how to set the status of a data disk to Error.

1. On the **Storage Nodes** page, find the target storage node and choose **Actions** > **Set Disk Status to Error** in the Actions column.
2. In the dialog box that appears, set the **Diskid** parameter.

   Set Disk Status to Error

   * Volume: PanguDefaultVolume

   * Hostname: a56g101 [redacted]

   * DiskId:

   The values of the **Volume** and **Hostname** parameters are automatically filled based on the selected storage node. You do not need to specify values for the parameters.
3. Click **Run**. A message appears, indicating that the action has been submitted.

11.2.5.3.3.6. Change the primary master node of Apsara Distributed File System

Apsara Big Data Manager (ABM) allows you to perform a primary/secondary switchover on the master nodes of Apsara Distributed File System. After the primary/secondary switchover is complete, an original secondary master node becomes the primary master node, and the original primary master node becomes a secondary master node.

Prerequisites

Your ABM account is granted the required permissions to perform O&M operations on MaxCompute.

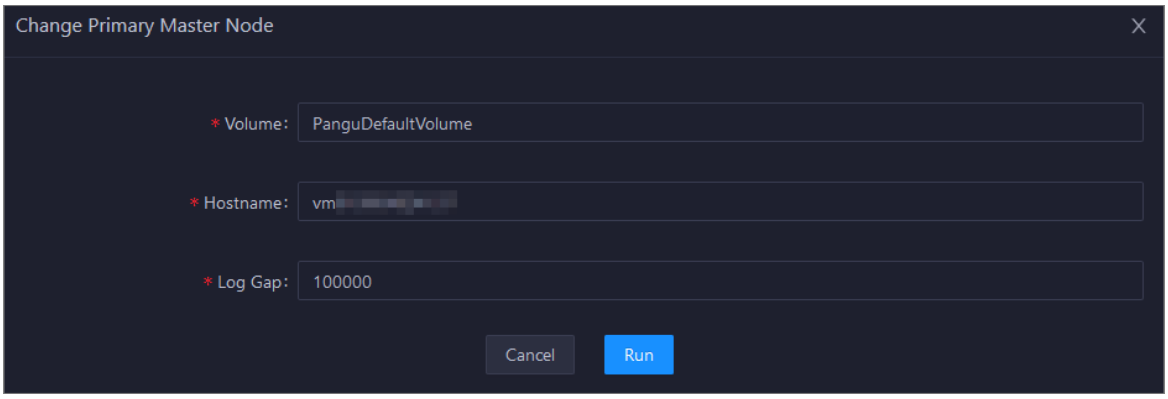
Background information

A volume in Apsara Distributed File System is similar to a namespace. The default volume is PanguDefaultVolume. If a cluster contains a large number of nodes, multiple volumes may exist. A volume has three master nodes. One of the nodes serves as the primary master node, and the other two nodes serve as secondary master nodes.

Procedure

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Pangu**. Then, select a cluster and click the **Instances** tab.

5. In the **Master Status** section of the **Instances** tab, find the required master node and choose **Actions** > **Change Primary Master Node** in the Actions column. In the Change Primary Master Node panel, specify the required parameters.



Change Primary Master Node

* Volume: PanguDefaultVolume

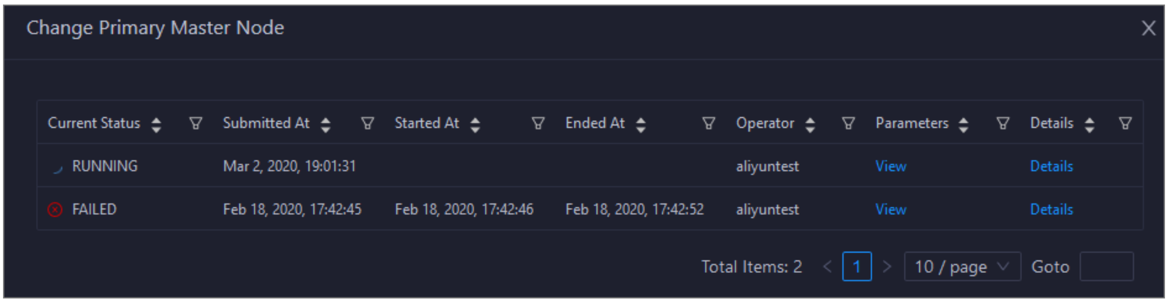
* Hostname: vm[redacted]

* Log Gap: 100000

Parameter description:

- **Volume**: the volume whose primary master node needs to be changed. Default value: **PanguDefaultVolume**. If a cluster contains multiple volumes, set this parameter to the name of the actual volume whose primary master node needs to be changed.
- **Hostname**: the hostname of the secondary master node that is to be the new primary master node.
- **Log Gap**: the maximum log number gap between the original primary and secondary master nodes you want to switch. During the switchover, the system checks the log number gap. If the gap is less than the specified value, the switchover is allowed. Otherwise, you cannot change the primary master node. Default value: **100000**.

6. Click **Run**. The **Change Primary Master Node** panel appears.

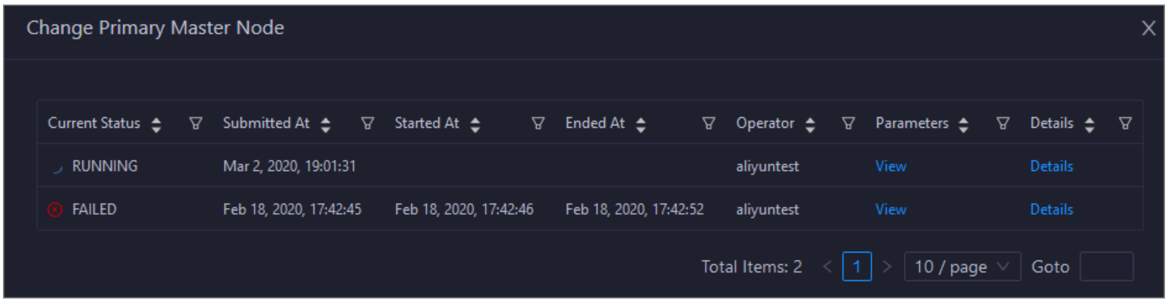


Change Primary Master Node

Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
RUNNING	Mar 2, 2020, 19:01:31			aliyuntest	View	Details
FAILED	Feb 18, 2020, 17:42:45	Feb 18, 2020, 17:42:46	Feb 18, 2020, 17:42:52	aliyuntest	View	Details

The **Change Primary Master Node** panel shows the switchover history. **RUNNING** indicates that the execution is in progress. **SUCCESS** indicates that the execution succeeds. **FAILED** indicates that the execution fails.

7. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure.



Change Primary Master Node

Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
RUNNING	Mar 2, 2020, 19:01:31			aliyuntest	View	Details
FAILED	Feb 18, 2020, 17:42:45	Feb 18, 2020, 17:42:46	Feb 18, 2020, 17:42:52	aliyuntest	View	Details

You can view information about parameter settings, host details, script, and runtime parameters to identify the cause of the failure.

11.2.5.3.3.7. Clear the recycle bin of Apsara Distributed File System

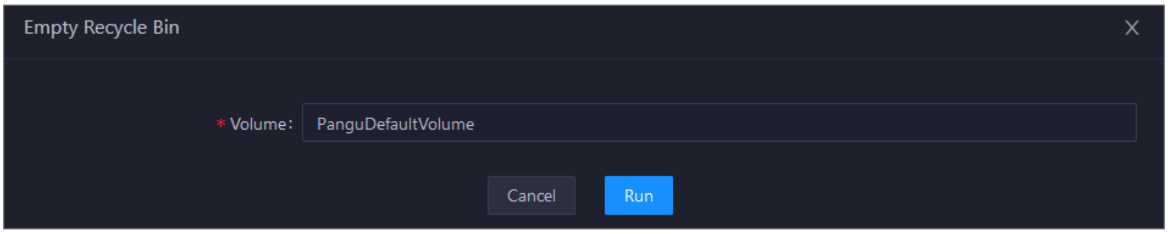
Apsara Big Data Manager (ABM) allows you to clear the recycle bin of Apsara Distributed File System to release storage space.

Prerequisites

Your ABM account is granted the required permissions to perform O&M operations on MaxCompute.

Procedure

1. In the left-side navigation pane of the **Services** tab, click **Pangu**. Then, select a cluster. The **Overview** tab for the selected cluster appears.
2. In the upper-right corner, choose **Actions** > **Empty Recycle Bin**.
3. In the Empty Recycle Bin panel, set the **Volume** parameter. The default value is **PanguDefaultVolume**.

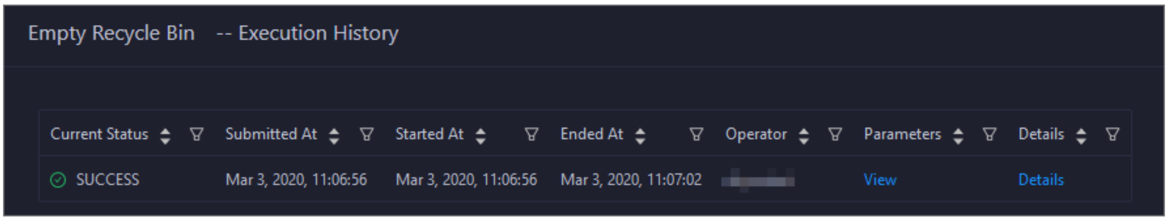


Empty Recycle Bin

* Volume: PanguDefaultVolume

4. Click **Run**.
5. View the execution status.

   In the upper-right corner, click **Actions** and select **Execution History** next to **Empty Recycle Bin** to view the execution history.

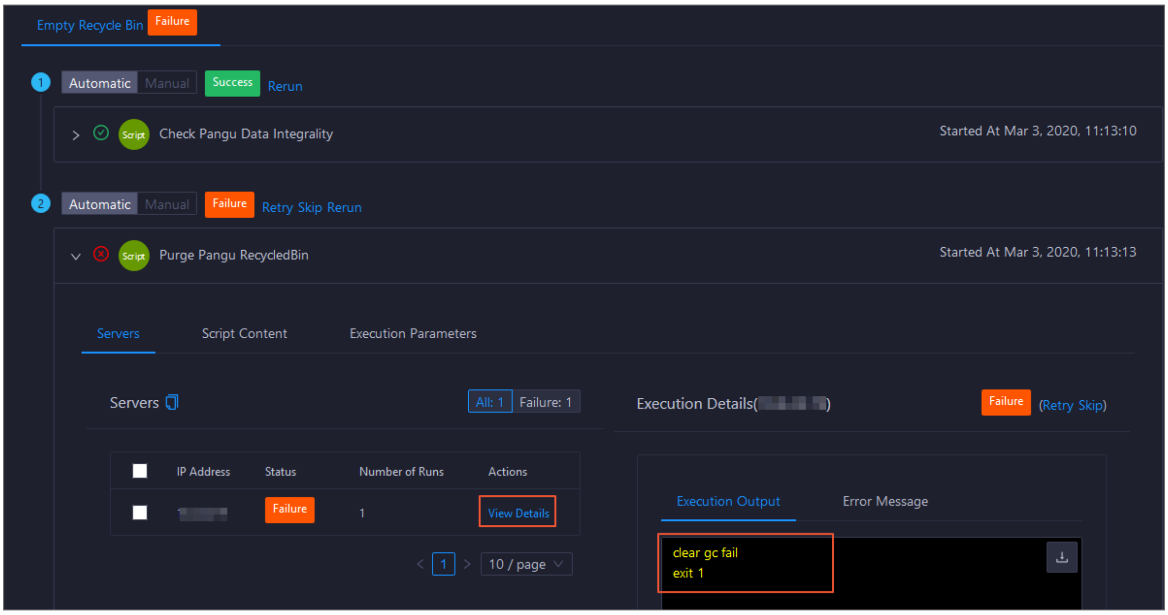


Empty Recycle Bin -- Execution History

Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
SUCCESS	Mar 3, 2020, 11:06:56	Mar 3, 2020, 11:06:56	Mar 3, 2020, 11:07:02	[redacted]	View	Details

   RUNNING indicates that the execution is in progress. **SUCCESS** indicates that the execution succeeds. **FAILED** indicates that the execution fails.

6. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure.


Empty Recycle Bin Failure
1 Automatic Manual Success Rerun
Check Pangu Data Integrality
Started At Mar 3, 2020, 11:13:10
2 Automatic Manual Failure Retry Skip Rerun
Purge Pangu RecycledBin
Started At Mar 3, 2020, 11:13:13
Servers Script Content Execution Parameters
Servers All: 1 Failure: 1
Execution Details([redacted]) Failure (Retry Skip)
IP Address Status Number of Runs Actions
Execution Output Error Message
1 10 / page

□	IP Address	Status	Number of Runs	Actions
□	[redacted]	Failure	1	View Details

```
clear gc fail
exit 1
```

You can view information about parameter settings, host details, script, and runtime parameters to identify the cause of the failure.

11.2.5.3.3.8. Enable or disable data rebalancing for Apsara Distributed File System

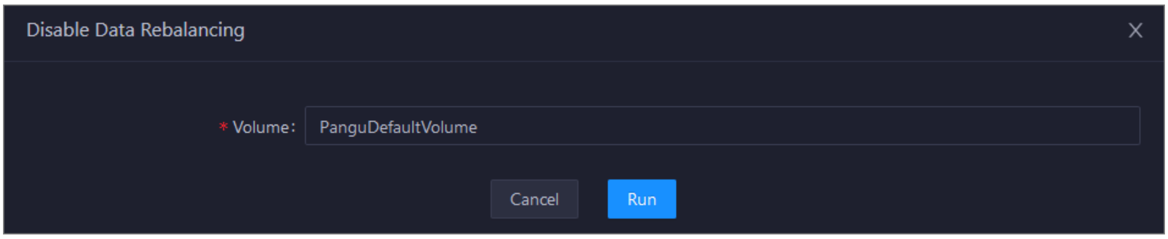
Apsara Big Data Manager (ABM) allows you to enable or disable data rebalancing for Apsara Distributed File System.

Prerequisites

Your ABM account is granted the required permissions to perform O&M operations on MaxCompute.

Disable data rebalancing

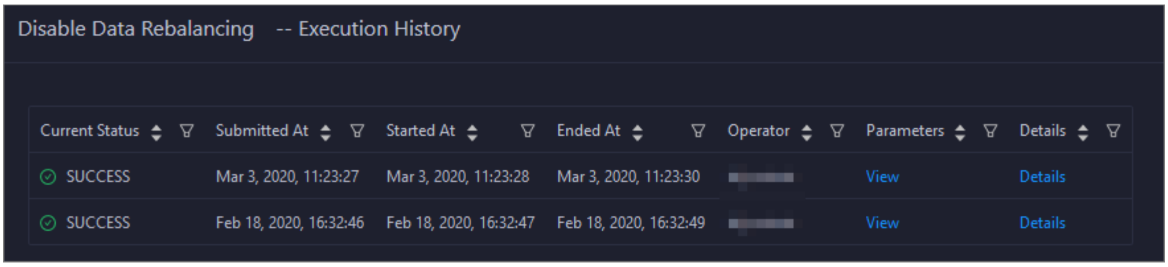
1. In the left-side navigation pane of the **Services** tab, click **Pangu**. Then, select a cluster. The Overview tab for the selected cluster appears.
2. In the upper-right corner of the tab that appears, choose **Actions** > **Disable Data Rebalancing**.
3. In the Disable Data Rebalancing panel, set the **Volume** parameter. The default value is **PanguDefaultVolume**.



* Volume: PanguDefaultVolume

4. Click **Run**.
5. View the execution status.

   Click **Actions** and select **Execution History** next to **Disable Data Rebalancing** to view the execution history.



Disable Data Rebalancing -- Execution History

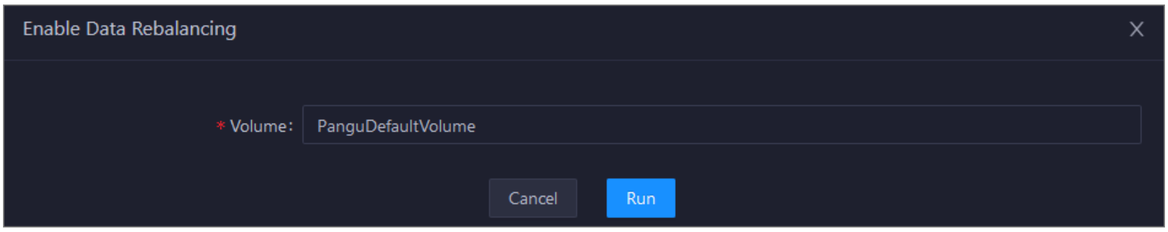
Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
SUCCESS	Mar 3, 2020, 11:23:27	Mar 3, 2020, 11:23:28	Mar 3, 2020, 11:23:30	[redacted]	View	Details
SUCCESS	Feb 18, 2020, 16:32:46	Feb 18, 2020, 16:32:47	Feb 18, 2020, 16:32:49	[redacted]	View	Details

RUNNING indicates that the execution is in progress. **SUCCESS** indicates that the execution succeeds. **FAILED** indicates that the execution fails.

6. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure. For more information, see Identify the cause of a failure.

Enable data rebalancing

1. In the left-side navigation pane of the **Services** tab, click **Pangu**. Then, select a cluster. The Overview tab for the selected cluster appears.
2. In the upper-right corner of the tab that appears, choose **Actions** > **Enable Data Rebalancing**.
3. In the Enable Data Rebalancing panel, set the **Volume** parameter. The default value is **PanguDefaultVolume**.

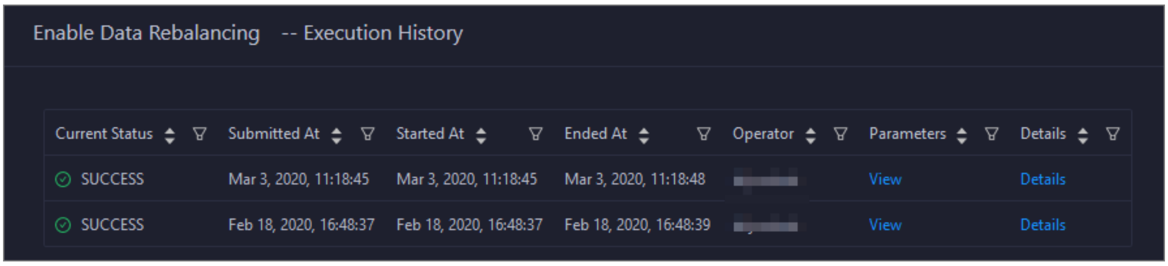


Enable Data Rebalancing

* Volume: PanguDefaultVolume

4. Click **Run**.
5. View the execution status.

   Click **Actions** and select **Execution History** next to **Enable Data Rebalancing** to view the execution history.



Enable Data Rebalancing -- Execution History

Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
SUCCESS	Mar 3, 2020, 11:18:45	Mar 3, 2020, 11:18:45	Mar 3, 2020, 11:18:48	[redacted]	View	Details
SUCCESS	Feb 18, 2020, 16:48:37	Feb 18, 2020, 16:48:37	Feb 18, 2020, 16:48:39	[redacted]	View	Details

RUNNING indicates that the execution is in progress. **SUCCESS** indicates that the execution succeeds. **FAILED** indicates that the execution fails.

6. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure. For more information, see Identify the cause of a failure.

Identify the cause of a failure

This section uses the procedure of identifying the cause of the failure to enable data rebalancing as an example.

1. In the Execution History panel, click **Details** in the Details column for a failed execution.

2. In the Enable Data Rebalancing panel, click **View Details** for a failed step to identify the cause of the failure.

   You can view information about parameter settings, host details, script, and runtime parameters to identify the cause of the failure.

11.2.5.3.3.9. Run a checkpoint on a master node of Apsara Distributed File System

Apsara Big Data Manager (ABM) allows you to run checkpoints on master nodes of Apsara Distributed File System. This operation writes memory data to disks. If Apsara Distributed File System is faulty, you can use checkpoints to restore data to the status before the failure. This ensures data consistency.

Prerequisites

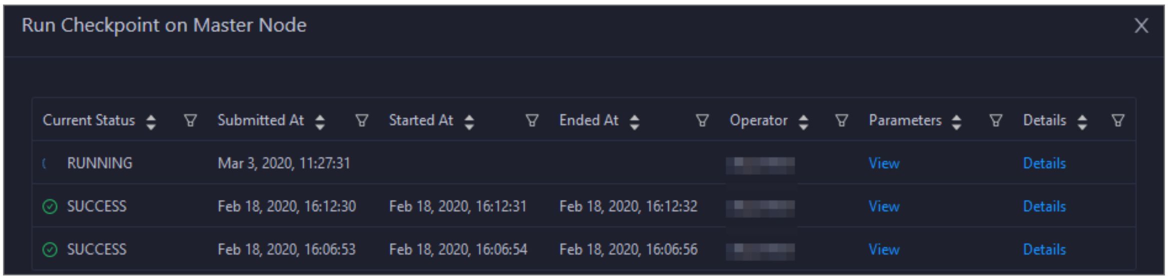
Your ABM account is granted the required permissions to perform O&M operations on MaxCompute.

Procedure

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Pangu**. Then, select a cluster and click the **Instances** tab.
5. In the **Master Status** section of the **Instances** tab, find the required master node and choose **Actions** > **Run Checkpoint on Master Node** in the Actions column. In the Run Checkpoint on Master Node panel, set the **Volume** parameter.

   > Note The default value of **Volume** is **PanguDefaultVolume**.

6. Click **Run**. The **Run Checkpoint on Master Node** panel appears.

   Run Checkpoint on Master Node

Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
RUNNING	Mar 3, 2020, 11:27:31			[redacted]	View	Details
✓ SUCCESS	Feb 18, 2020, 16:12:30	Feb 18, 2020, 16:12:31	Feb 18, 2020, 16:12:32	[redacted]	View	Details
✓ SUCCESS	Feb 18, 2020, 16:06:53	Feb 18, 2020, 16:06:54	Feb 18, 2020, 16:06:56	[redacted]	View	Details

   The **Run Checkpoint on Master Node** panel shows the execution history of the checkpoint on the master node. **RUNNING** indicates that the execution is in progress. **SUCCESS** indicates that the execution succeeds. **FAILED** indicates that the execution fails.

7. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure.

   You can also view information about parameter settings, host details, script, and execution parameters to identify the cause of the failure.

11.2.5.3.4. Tunnel service

11.2.5.3.4.1. O&M features and entry

This topic describes the definition and O&M features of the Tunnel service. It also provides more information about how to go to the O&M page of the Tunnel service.

Definition of the Tunnel service

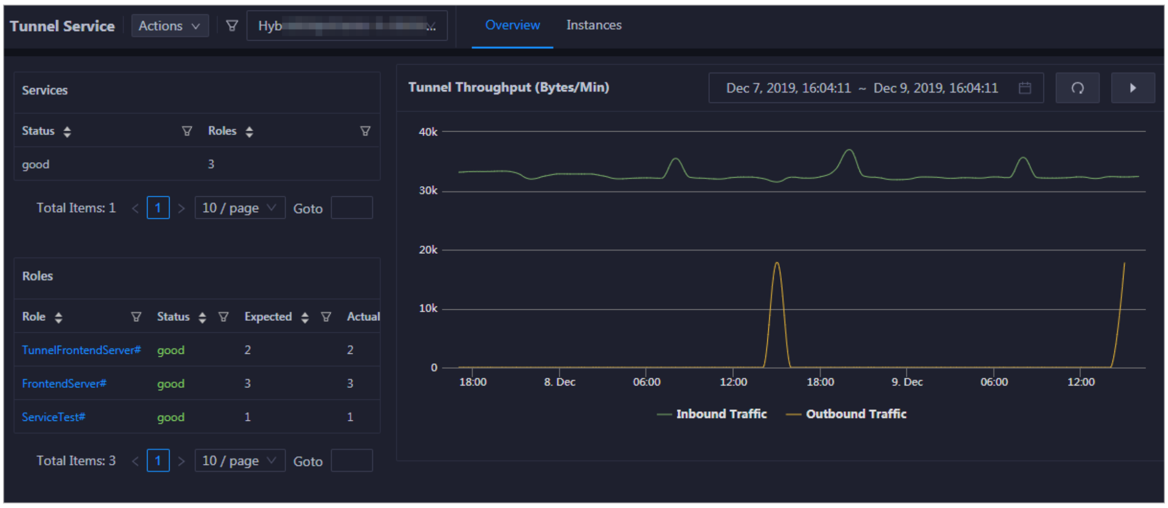
The Tunnel service serves as a data tunnel of MaxCompute. You can use this service to upload data to or download data from MaxCompute.

O&M features of the Tunnel service

- Overview: shows information about the Tunnel service. The information includes the service overview, service status, and throughput trend chart.
- Instances: shows information about the server roles of the Tunnel service.
- Traffic Analysis: shows the traffic curves of specific projects in a specific period. The curves show traffic types and the peak throughout in the specified period, which helps you make informed decisions.
- Restart Tunnel Server: allows you to restart one or more Tunnel servers.

Go to the Tunnel Service page

1. Log on to the Apsara Big Data Manager (ABM) console.
2. In the upper-right corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Tunnel Service**. The **Overview** tab for the Tunnel service appears.



Services

Status	Roles
good	3

Total Items: 1 < 1 > 10 / page Goto

Roles

Role	Status	Expected	Actual
TunnelFrontendServer#	good	2	2
FrontendServer#	good	3	3
ServiceTest#	good	1	1

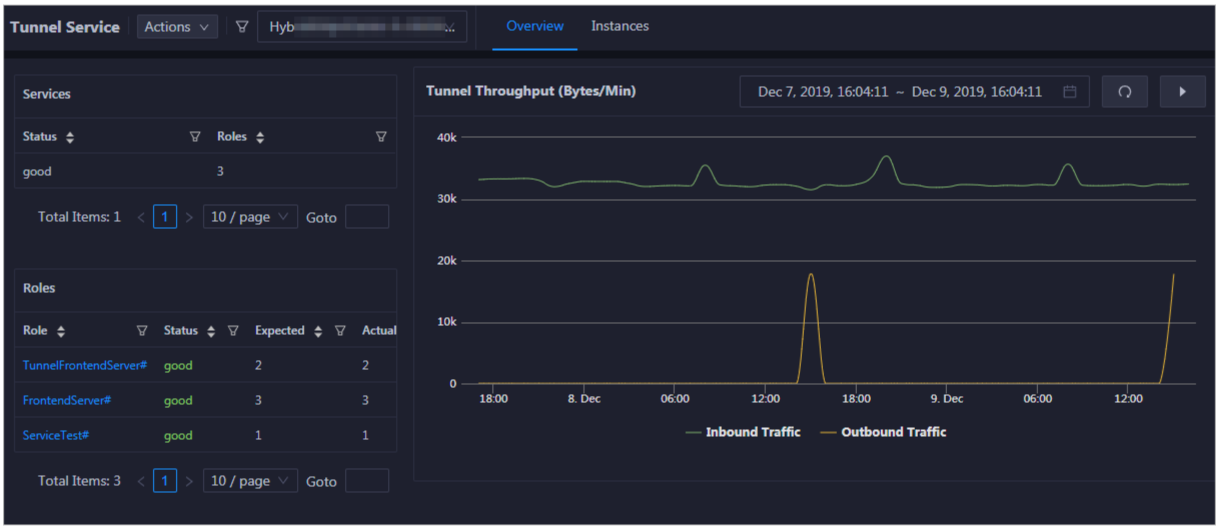
Total Items: 3 < 1 > 10 / page Goto

11.2.5.3.4.2. Overview

The Overview tab for the Tunnel service shows key operating information. The information includes the service overview, service status, and throughput.

Go to the Overview tab

In the left-side navigation pane of the **Services** tab, click **Tunnel Service**. The **Overview** tab for the Tunnel service appears.



Services

Status	Roles
good	3

Total Items: 1 &lt; 1 &gt; 10 / page Goto

Roles

Role	Status	Expected	Actual
TunnelFrontendServer#	good	2	2
FrontendServer#	good	3	3
ServiceTest#	good	1	1

Total Items: 3 &lt; 1 &gt; 10 / page Goto

The **Overview** tab shows key operating information about the Tunnel service. The information includes the service overview, service status, and throughput trend chart.

Services

The Services section shows the numbers of available services, unavailable services, and services that are being updated.

Roles

The Roles section shows all Tunnel server roles and their status. You can also view the expected and actual numbers of hosts for each server role.

Tunnel throughput

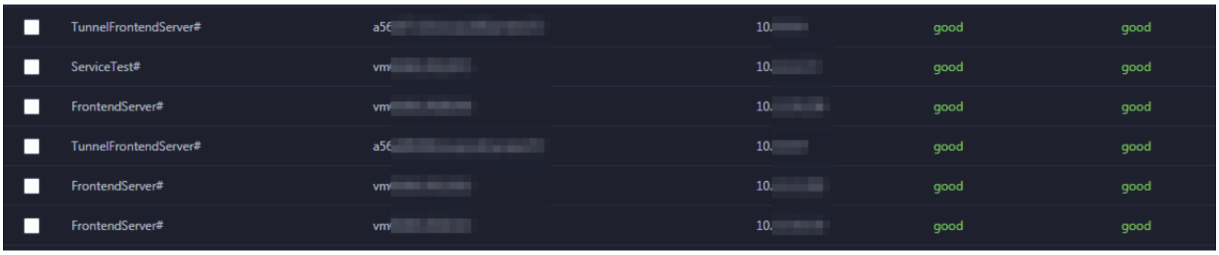
The Tunnel Throughput (Bytes/Min) chart shows the trend lines of the inbound and outbound traffic in different colors. This trend chart can be automatically or manually refreshed. You can view the trend chart of Tunnel throughput in a specific period.

11.2.5.3.4.3. Instances

The Instances tab shows information about the Tunnel server roles. The information includes the role name, hostname, IP address, role status, and host status.

Go to the Instances tab

In the left-side navigation pane of the **Services** tab, click **Tunnel Service**. Then, click the **Instances** tab. The **Instances** tab for the Tunnel service appears.



□	TunnelFrontendServer#	a5[redacted]	10.[redacted]	good	good
□	ServiceTest#	vm[redacted]	10.[redacted]	good	good
□	FrontendServer#	vm[redacted]	10.[redacted]	good	good
□	TunnelFrontendServer#	a5[redacted]	10.[redacted]	good	good
□	FrontendServer#	vm[redacted]	10.[redacted]	good	good
□	FrontendServer#	vm[redacted]	10.[redacted]	good	good

The **Instances** tab shows information about all Tunnel server roles. The information includes the role name, hostname, IP address, role status, and host status. The status can be good, error, or upgrading.

11.2.5.3.4.4. Traffic analysis

The Traffic Analysis tab displays the traffic curves of specific projects in a specific period. The curves show traffic types and the peak throughout in the specified period, which helps you make informed decisions.

Go to the Traffic Analysis tab

In the left-side navigation pane of the **Services** tab, click **Tunnel Service**. Then, click the **Traffic Analysis** tab. The **Traffic Analysis** tab for the Tunnel service appears.

After you specify a period and the project for traffic analysis, click the 🔍 icon. Then, you can view the upstream and downstream throughput curves of Tunnel traffic for traffic analysis.

> ⓘ Note
>
> - The traffic data comes from Monitoring System. Make sure that this system is normal.
> - By default, the top five projects that have the most traffic are selected. You can also filter projects based on your business requirements.
> - By default, the beginning of the period is two days before the current time, and the end of the period is one day before the current time. You can also specify the period based on your business requirements.

11.2.5.3.4.5. Restart Tunnel servers

Apsara Big Data Manager (ABM) allows you to restart Tunnel servers for the corresponding server roles.

Prerequisites

Your ABM account is granted the required permissions to perform O&M operations on MaxCompute.

Context

You can restart one or more Tunnel servers at a time on the **Instances** tab.

Step 1: Restart Tunnel servers

1. Log on to the ABM console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Services** tab.
4. In the left-side navigation pane of the **Services** tab, click **Tunnel Service**. Then, click the **Instances** tab.
5. On the Instances tab, select one or more server roles for which you want to restart the Tunnel service. In the upper-right corner, choose **Actions > Restart Tunnel Server**.
6. In the **Restart Tunnel Server** panel, configure the required parameters.

   The following table describes the required parameters.

Parameter	Description
Force Restart	Specifies whether to forcibly restart the Tunnel server for the selected server role. Valid values: ○ **no_force**: Do not forcibly restart the Tunnel server. If a server role is in the running state, the corresponding Tunnel server is not restarted. ○ **force**: Forcibly restart the Tunnel server. The Tunnel server is restarted regardless of the server role state.
Hostname	The hostname of the selected server role. The value is automatically provided. You do not need to specify a value for this parameter.

7. Click **Run**.

Step 2: View the execution status or progress

1. On the **Overview** or **Instances** tab of the **Tunnel Service** page, click **Actions** in the upper-right corner. Then, select **Execution History** next to **Restart Tunnel Server** to view the execution history.

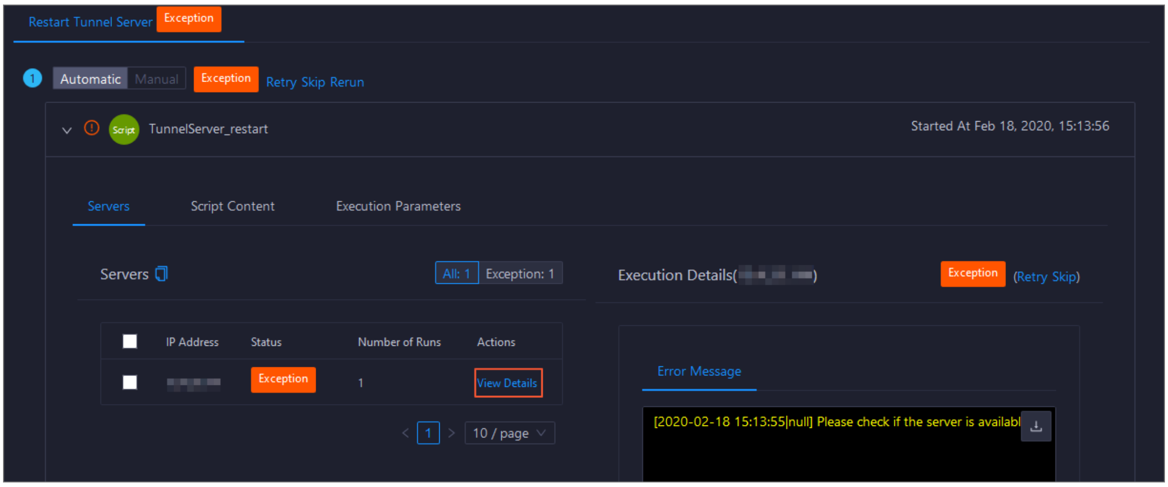
   RUNNING indicates that the execution is in progress. **SUCCESS** indicates that the execution succeeds. **FAILED** indicates that the execution fails.

2. If the status is **RUNNING**, click **Details** in the Details column to view the execution progress.

Step 3: (Optional) Identify the cause of a failure

If the status is **FAILED**, you can view the execution logs to identify the cause of the failure.

1. On the **Overview** or **Instances** tab of the **Tunnel Service** page, click **Actions** in the upper-right corner. Then, select **Execution History** next to **Restart Tunnel Server** to view the execution history.
2. In the Execution History panel, click **Details** in the Details column of the task to view the details.
3. On the **Servers** tab of the failed step, click **View Details** in the Actions column of a failed server. The **Execution Output** tab appears in the Execution Details section. You can view the output to identify the cause of the failure.



TunnelServer_restart

Started At Feb 18, 2020, 15:13:56

Execution Details([redacted])

□	IP Address	Status	Number of Runs	Actions
□	[redacted]	Exception	1	View Details

```
[2020-02-18 15:13:55|null] Please check if the server is availabl
```

11.2.5.4. Cluster O&M

11.2.5.4.1. O&M features and entry

This topic describes the O&M features of MaxCompute clusters. It also provides more information about how to go to the MaxCompute cluster O&M page.

Cluster O&M features

O&M features of MaxCompute clusters:

- Overview: shows the overall running information about a cluster. You can view the host status, service status, health check result, and health check history. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, and packet transmission for the cluster. In the Log on section, you can click the name of the host whose role is pangu master, fuxi master, or odps ag to log on to the host.
- Health Status: shows all checkers for a cluster. You can query checker details, check results for hosts in the cluster, and schemes to clear alerts (if any exists). You can also log on to a host and perform manual checks on the host.
- Servers: shows information about hosts in a cluster. The information includes the hostname, IP address, role, type, CPU utilization, memory usage, root disk usage, packet loss rate, and packet error rate.
- Scale out Cluster or Scale in Cluster: allows you to add or remove physical hosts to scale out or scale in a MaxCompute cluster.
- Enable Auto Repair: allows you to enable auto repair for MaxCompute clusters.
- Restore Environment Settings: allows you to restore environment settings for multiple hosts in a MaxCompute cluster at a time.

Go to the Clusters tab

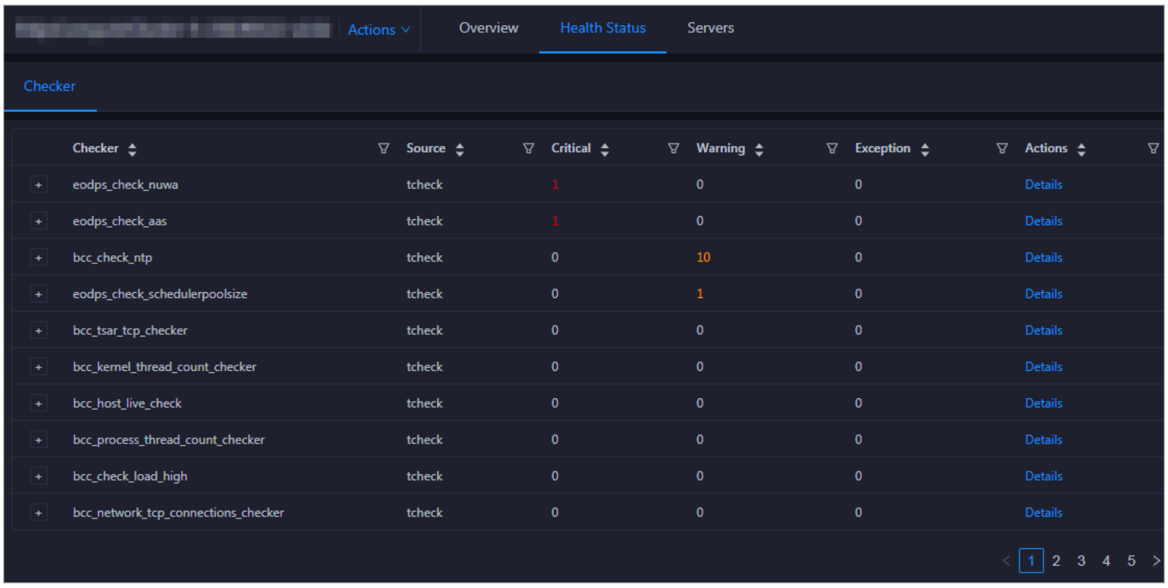
1. Log on to the Apsara Big Data Manager (ABM) console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Clusters** tab.
4. In the left-side navigation pane of the **Clusters** tab, click a cluster. The **Overview** tab for the selected cluster appears.

11.2.5.4.2. Cluster health

The Health Status tab shows all checkers for a cluster. You can query checker details, check results for hosts in the cluster, and schemes to clear alerts (if any exists). You can also log on to a host and perform manual checks on the host.

Go to the Health Status tab

1. Log on to the Apsara Big Data Manager (ABM) console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Clusters** tab.
4. In the left-side navigation pane of the **Clusters** tab, select a cluster. Then, click the **Health Status** tab. The **Health Status** tab for the selected cluster appears.

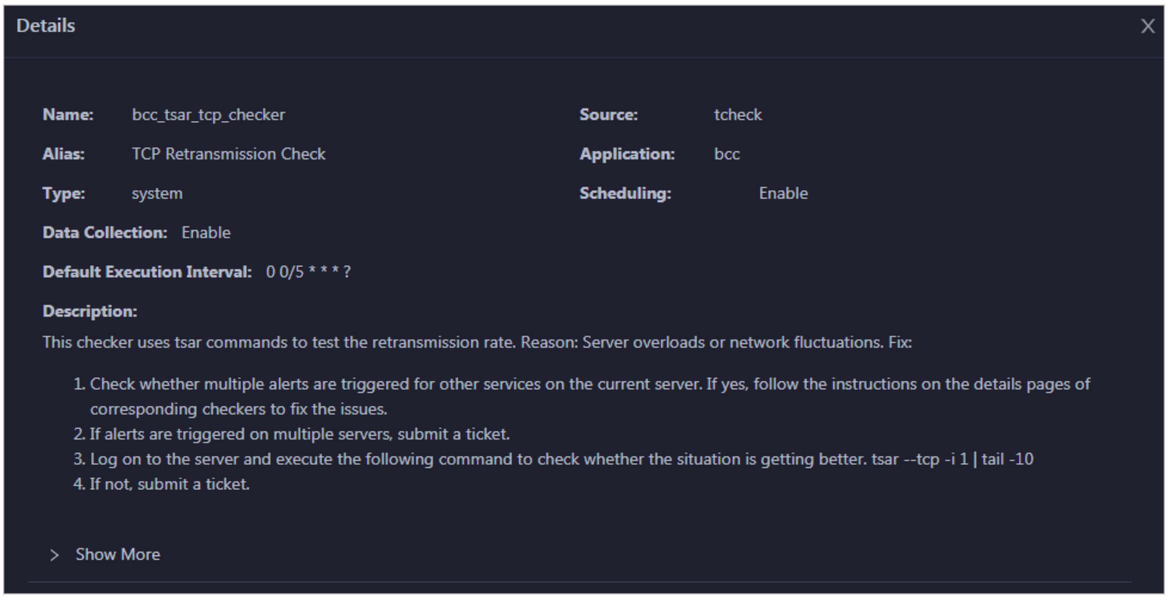


	Checker	Source	Critical	Warning	Exception	Actions
+	eodps_check_nuwa	tcheck	1	0	0	Details
+	eodps_check_aas	tcheck	1	0	0	Details
+	bcc_check_ntp	tcheck	0	10	0	Details
+	eodps_check_schedulerpoolsize	tcheck	0	1	0	Details
+	bcc_tsar_tcp_checker	tcheck	0	0	0	Details
+	bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
+	bcc_host_live_check	tcheck	0	0	0	Details
+	bcc_process_thread_count_checker	tcheck	0	0	0	Details
+	bcc_check_load_high	tcheck	0	0	0	Details
+	bcc_network_tcp_connections_checker	tcheck	0	0	0	Details

On the **Health Status** tab, you can view all checkers for the cluster and the check results for the hosts in the cluster. The following alerts may be reported on a host: **CRITICAL**, **WARNING**, and **EXCEPTION**. The alerts are represented in different colors. You must handle the alerts in a timely manner, especially the **CRITICAL** and **WARNING** alerts.

View checker details

1. On the Health Status tab, click **Details** in the Actions column of a checker. On the Details page, view checker details.

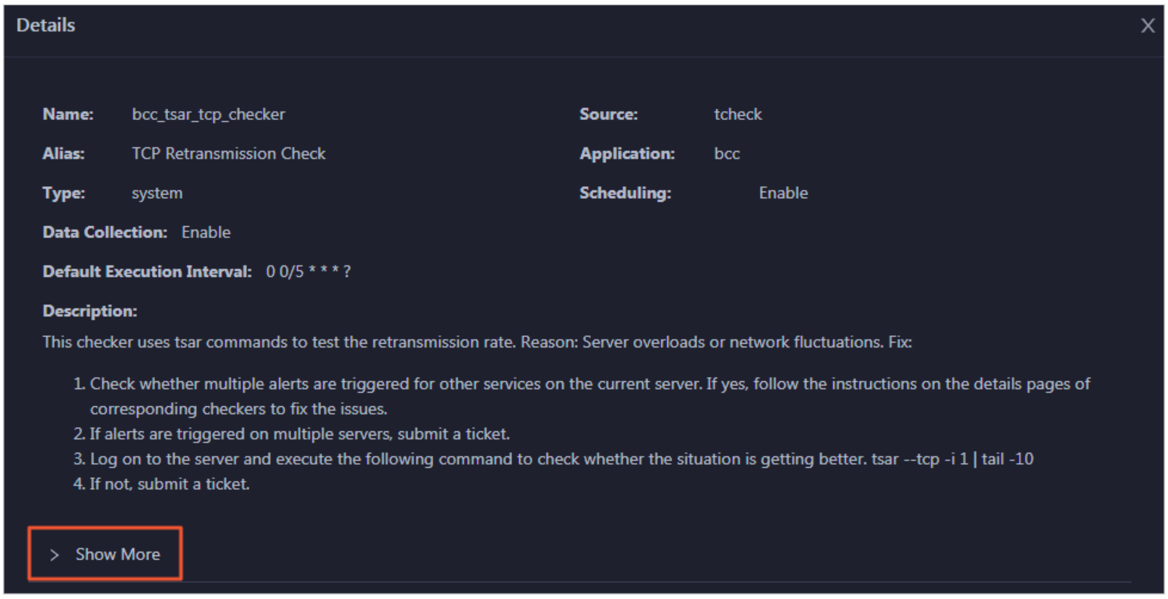


Name: bcc_tsar_tcp_checker
Source: tcheck
Alias: TCP Retransmission Check
Application: bcc
Type: system
Scheduling: Enable
Data Collection: Enable
Default Execution Interval: 0 0/5 * * * ?
Description:
This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include **Name**, **Source**, **Alias**, **Application**, **Type**, **Scheduling**, **Data Collection**, **Default Execution Interval**, and **Description**. The schemes to clear alerts are provided in the description.

2. Click **Show More** to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Alias: TCP Retransmission Check

Type: system

Source: tcheck

Application: bcc

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

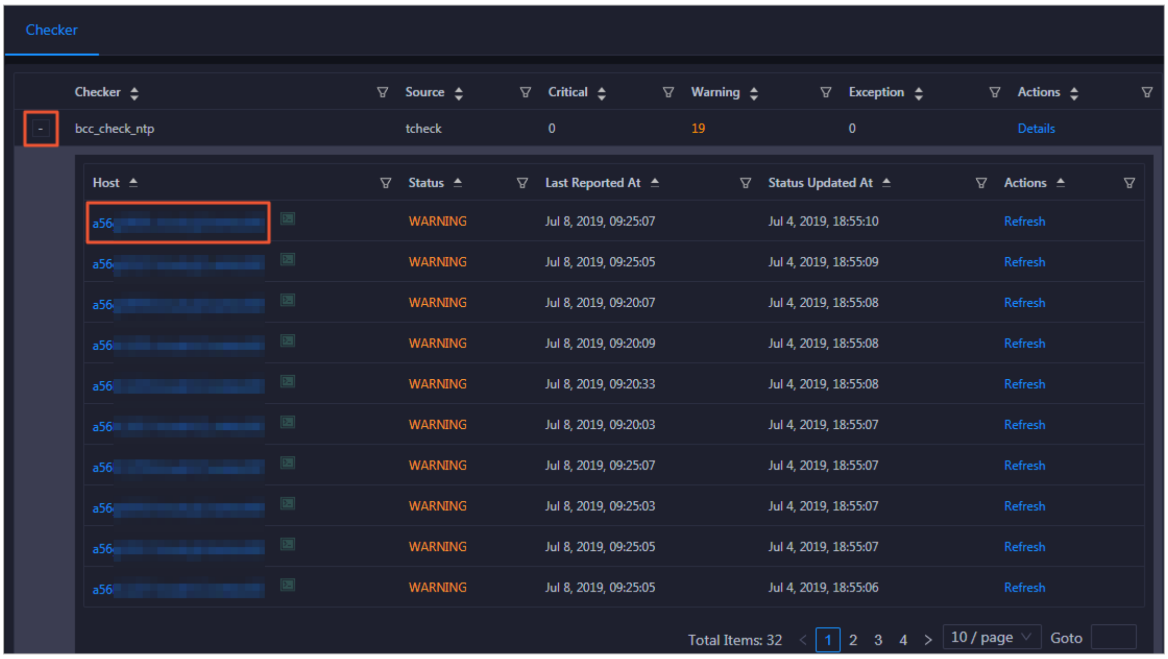
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about **Script**, **Target (TianJi)**, **Default Threshold**, and **Mount Point**.

View the hosts for which alerts are reported and causes for the alerts

You can view the check history and check results of a checker on a host.

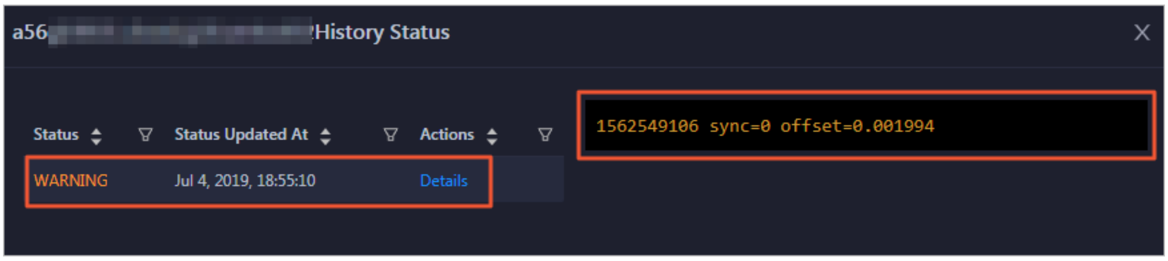
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported. You can view all hosts where the checker is run.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:06	Refresh

2. Click a hostname. In the panel that appears, click **Details** in the Actions column of a check result to view the cause of the alert.



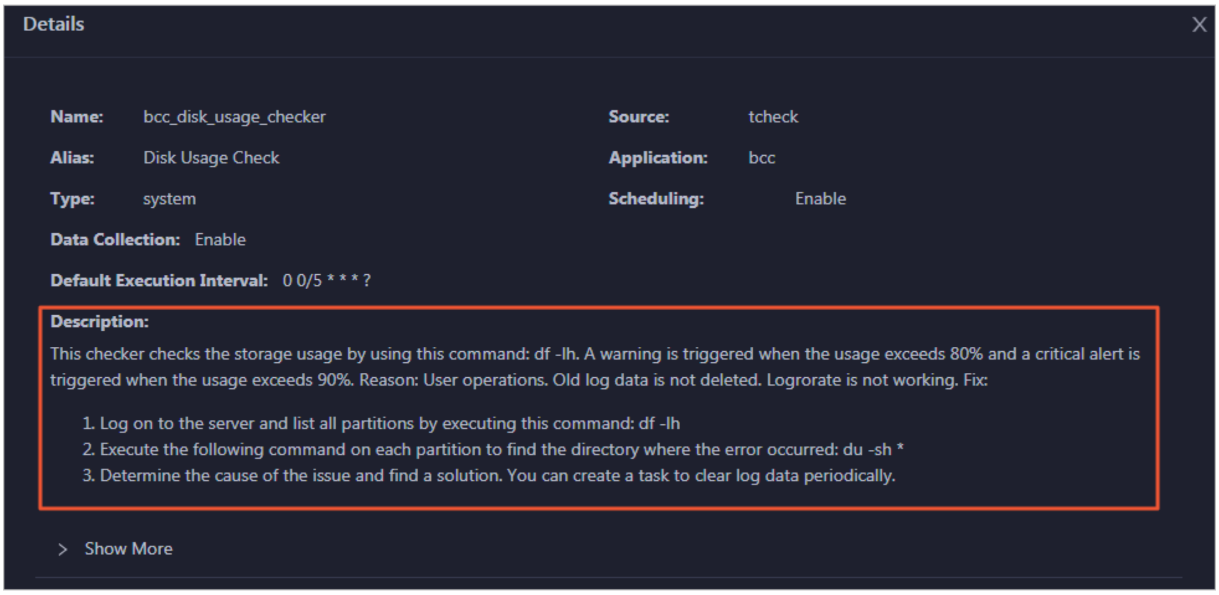
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status tab, click **Details** in the Actions column of a checker for which alerts are reported. On the Details page, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker

Alias: Disk Usage Check

Type: system

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Source: tcheck

Application: bcc

Scheduling: Enable

Description:

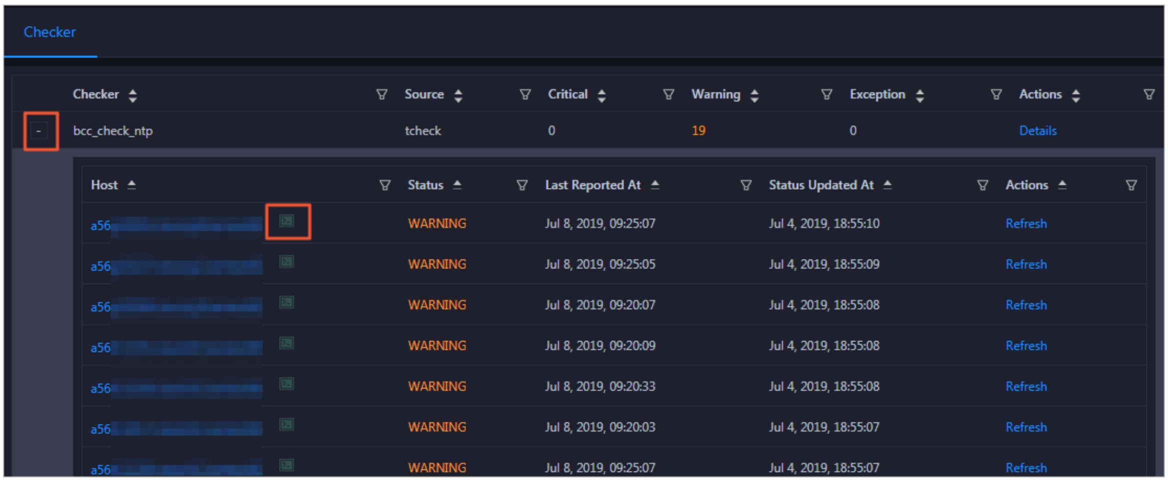
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

You may need to log on to a host to handle alerts or other issues that occurred on the host.

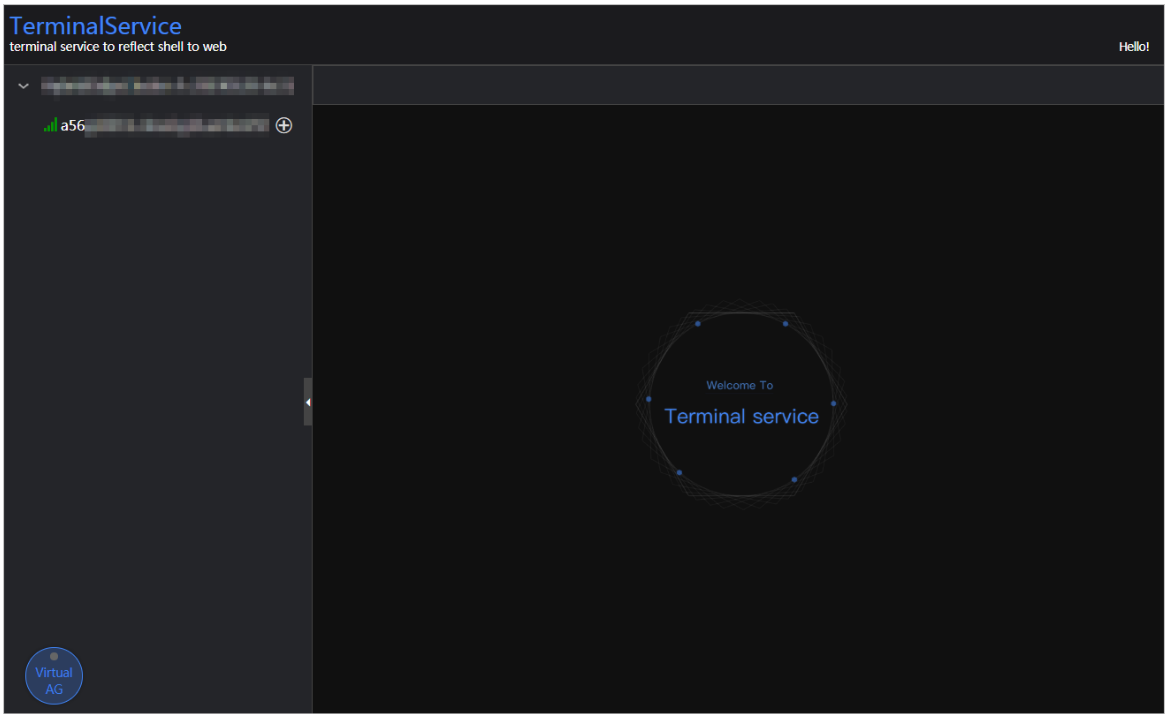
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported.



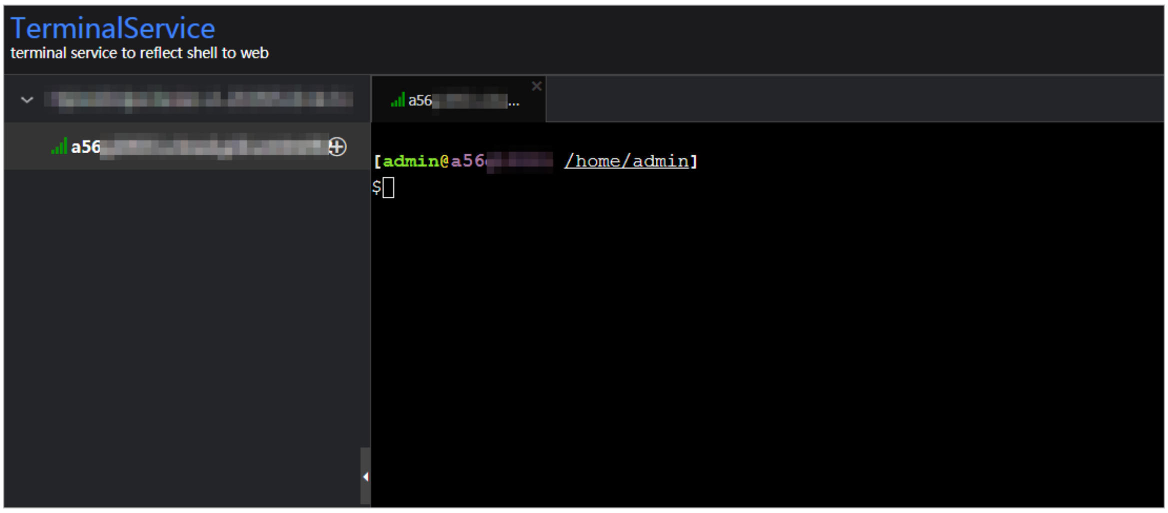
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

2. Click the **Login in** icon of a host. The **TerminalService** page appears.



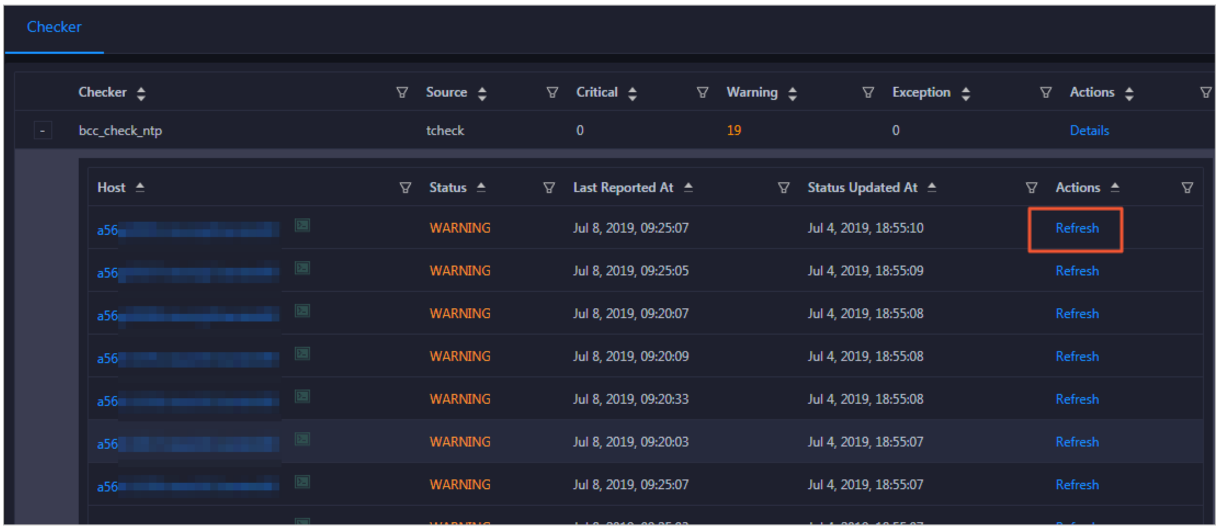
3. On the **TerminalService** page, click the hostname in the left-side navigation pane to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. This way, you can check whether the alert is cleared.



Checker

Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

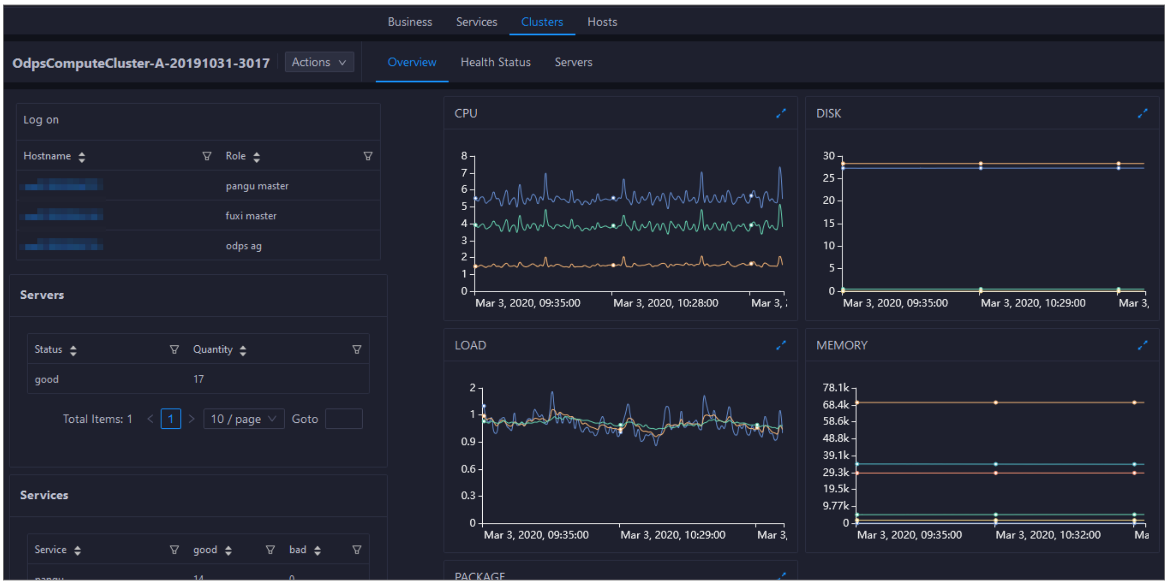
Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

11.2.5.4.3. Overview

This topic describes how to go to the Overview tab of a MaxCompute cluster. It also shows the cluster overview and describes the operations that you can perform on this tab.

Go to the Overview tab

1. Log on to the Apsara Big Data Manager (ABM) console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Clusters** tab.
4. In the left-side navigation pane of the **Clusters** tab, select a cluster. The **Overview** tab for the selected cluster appears.



Hostname	Role
[redacted]	pangu master
[redacted]	fuxi master
[redacted]	odps ag

Status	Quantity
good	17

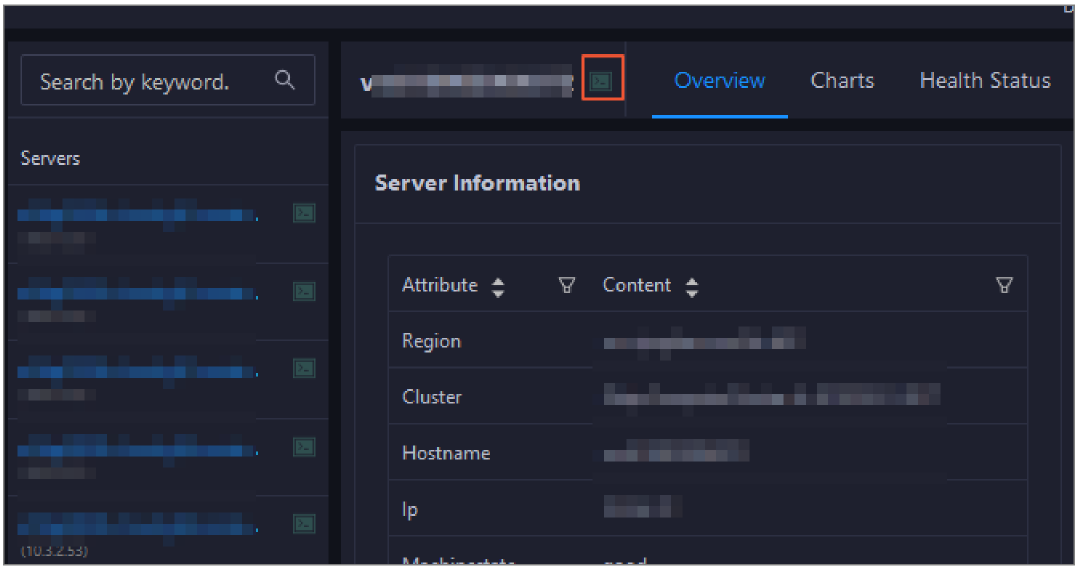
Service	good	bad

On the **Overview** tab, you can quickly log on to a host that is commonly used in MaxCompute cluster O&M. You can view the host status, service status, health check result, and health check history. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, and packet transmission for the cluster.

Log on

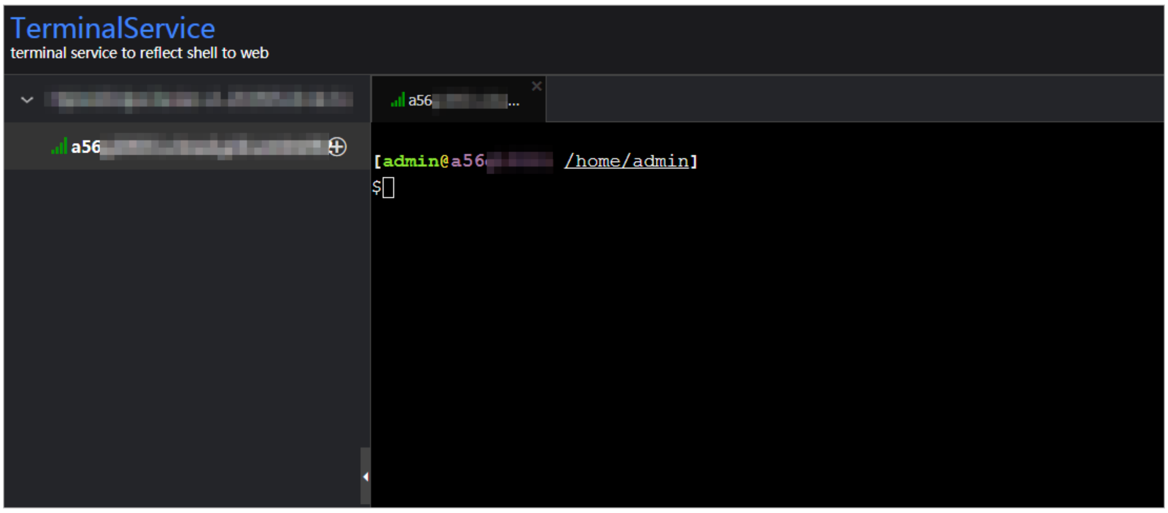
In this section, you can log on to a host that is commonly used in MaxCompute cluster O&M and whose role is pangu master, fuxi master, or odps ag.

1. In the **Log on** section, click the hostname in the **Hostname** column. The **Hosts** tab for the host appears.
2. In the upper-left corner, click the **Login in** icon of the host. The **TerminalService** page appears.



Attribute	Content
Region	[redacted]
Cluster	[redacted]
Hostname	[redacted]
Ip	[redacted]
Machinestate	good

3. In the left-side navigation pane, click the hostname to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Servers

This section shows all host status and the number of hosts in each state. A host can be in the **good** or **error** state.

Services

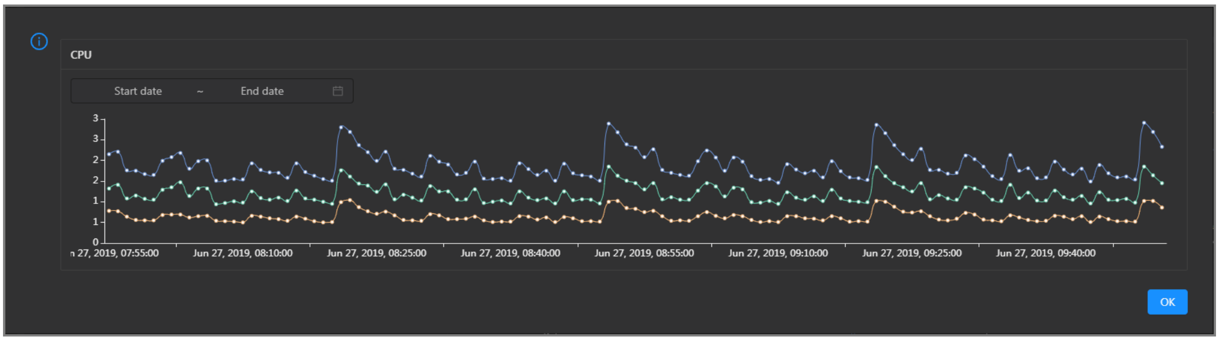
This section displays all services deployed in the cluster and the respective number of services in the **good** and **bad** states.

CPU

This chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

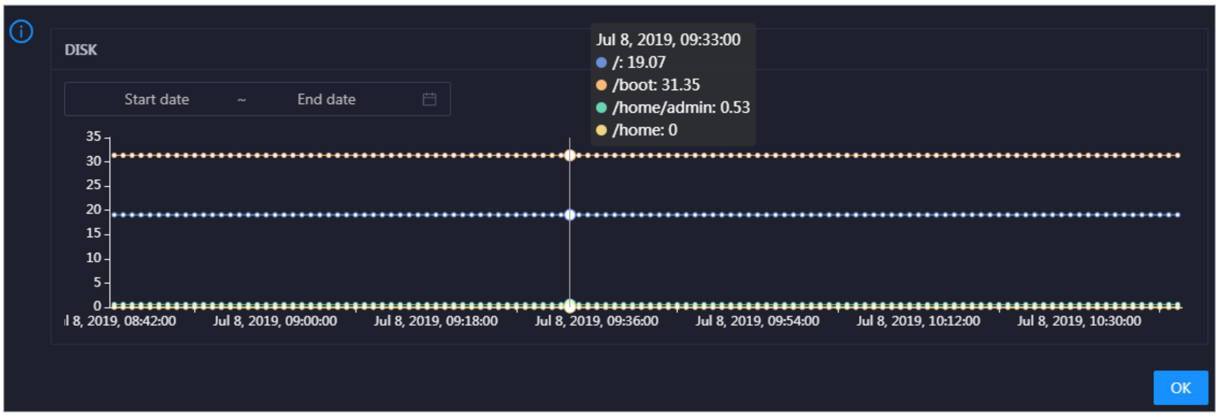
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the cluster in the specified period.



DISK

This chart shows the trend lines of the storage usage on the */*, */boot*, */home/admin*, and */home* directories for the cluster over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

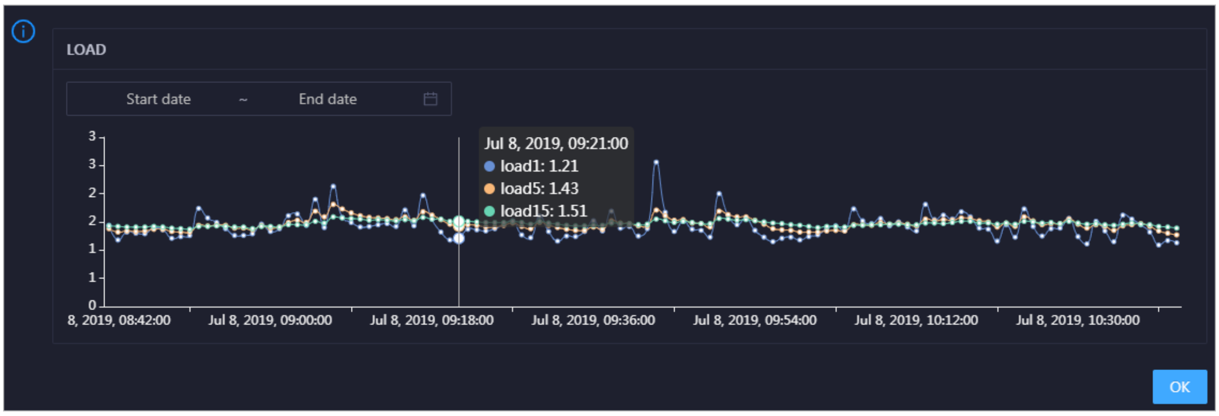


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

LOAD

This chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

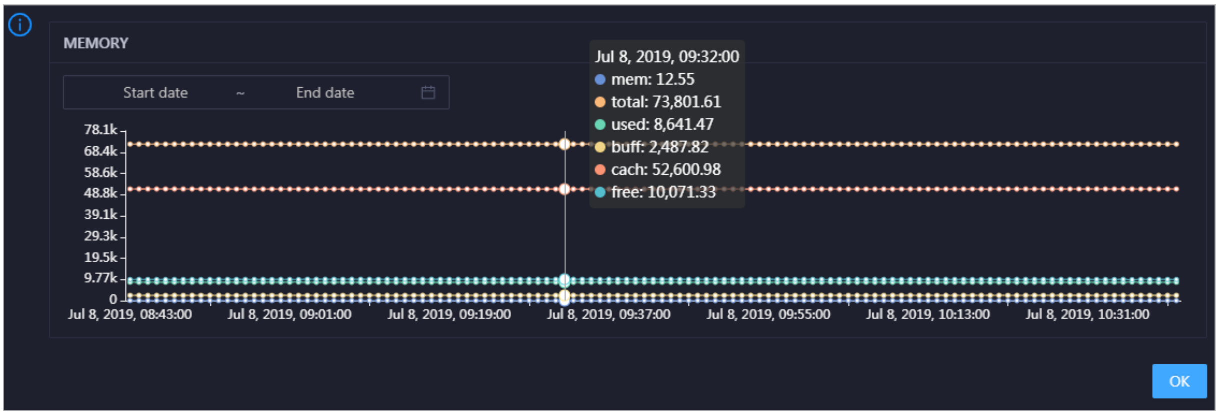


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the cluster in the specified period.

MEMORY

This chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

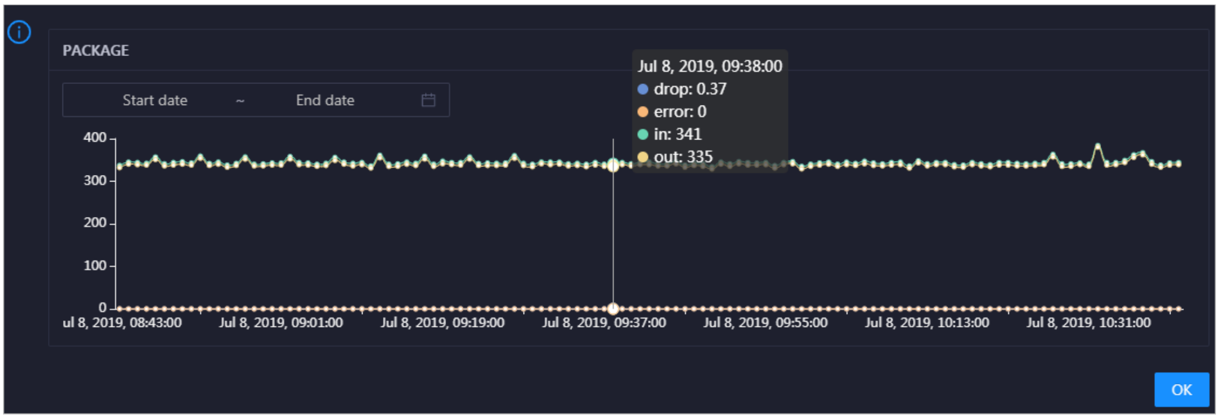


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the cluster in the specified period.

PACKAGE

This chart shows the trend lines of the numbers of dropped packets (drop), error packets (error), received packets (in), and sent packets (out) for the cluster in different colors. These trend lines reflect the data transmission status of the cluster.

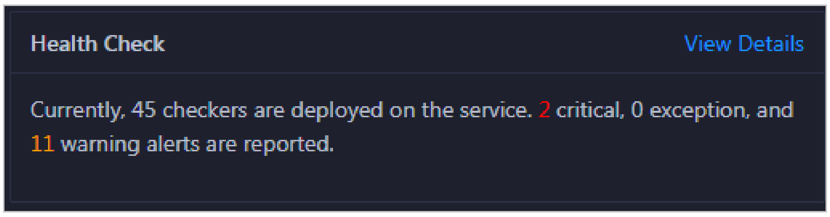
In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the cluster in the specified period.

Health Check

This section shows the number of checkers for the cluster and the numbers of CRITICAL, WARNING, and EXCEPTION alerts.



Health Check

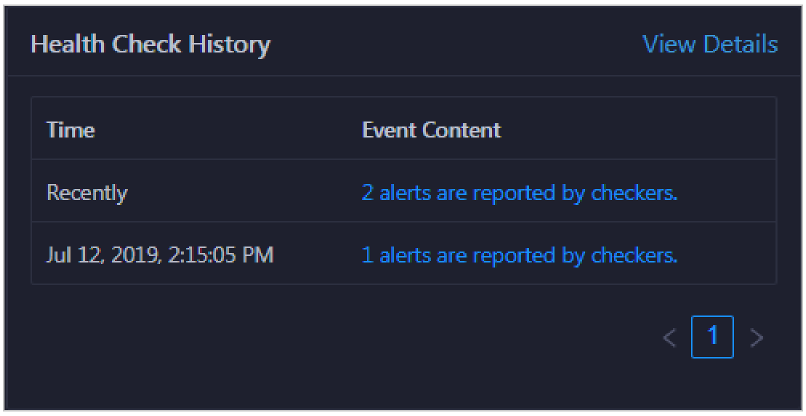
View Details

Currently, 45 checkers are deployed on the service. 2 critical, 0 exception, and 11 warning alerts are reported.

Click **View Details** to go to the Health Status tab. On this tab, you can view health check details. For more information, see Cluster health.

Health Check History

This section shows the records of the health checks performed on the cluster. You can view the numbers of CRITICAL, WARNING, and EXCEPTION alerts.



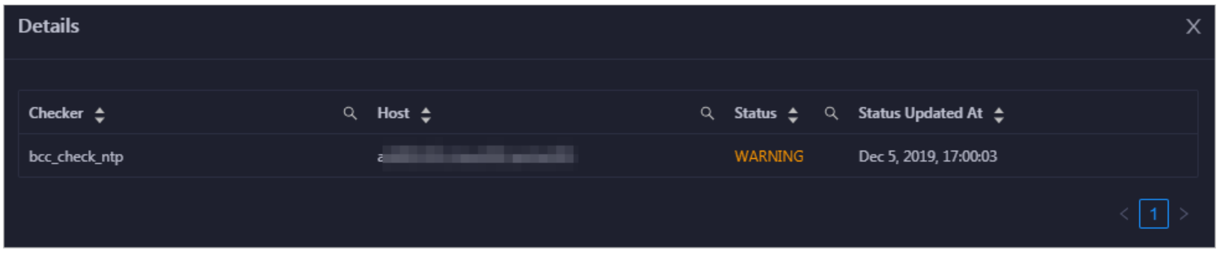
Health Check History

View Details

Time	Event Content
Recently	2 alerts are reported by checkers.
Jul 12, 2019, 2:15:05 PM	1 alerts are reported by checkers.

Click **View Details** to go to the Health Status tab. On this tab, you can view health check details. For more information, see Cluster health.

You can click the event content of a check to view the exception items.



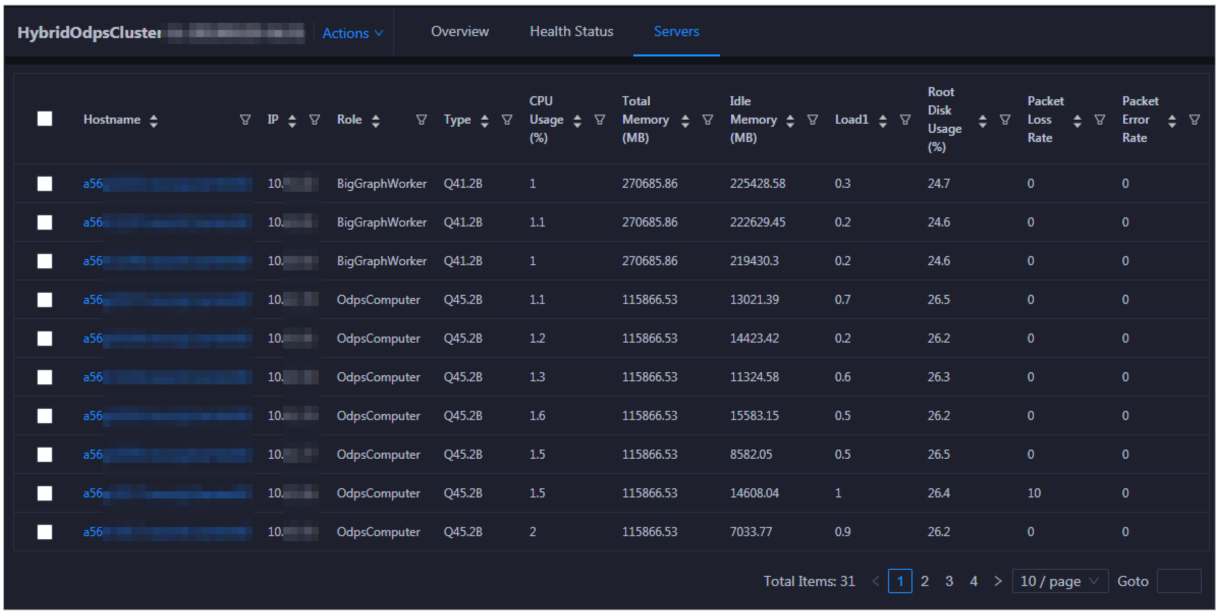
Details

Checker	Host	Status	Status Updated At
bcc_check_ntp	a[redacted]	WARNING	Dec 5, 2019, 17:00:03

11.2.5.4.4. Servers

The Servers tab shows information about hosts. The information includes the hostname, IP address, role, type, CPU utilization, total memory size, available memory size, load, root disk usage, packet loss rate, and packet error rate.

In the left-side navigation pane of the **Clusters** tab, click a cluster. Then, click the **Servers** tab. The **Servers** tab for the selected cluster appears.



□	Hostname	IP	Role	Type	CPU Usage (%)	Total Memory (MB)	Idle Memory (MB)	Load1	Root Disk Usage (%)	Packet Loss Rate	Packet Error Rate
□	a56[redacted]	10.[redacted]	BigGraphWorker	Q41.2B	1	270685.86	225428.58	0.3	24.7	0	0
□	a56[redacted]	10.[redacted]	BigGraphWorker	Q41.2B	1.1	270685.86	222629.45	0.2	24.6	0	0
□	a56[redacted]	10.[redacted]	BigGraphWorker	Q41.2B	1	270685.86	219430.3	0.2	24.6	0	0
□	a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.1	115866.53	13021.39	0.7	26.5	0	0
□	a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.2	115866.53	14423.42	0.2	26.2	0	0
□	a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.3	115866.53	11324.58	0.6	26.3	0	0
□	a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.6	115866.53	15583.15	0.5	26.2	0	0
□	a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.5	115866.53	8582.05	0.5	26.5	0	0
□	a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.5	115866.53	14608.04	1	26.4	10	0
□	a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	2	115866.53	7033.77	0.9	26.2	0	0

To view more information about a host, click the name of the host. The Hosts tab appears.

11.2.5.4.5. Scale in and scale out a MaxCompute cluster

Apsara Big Data Manager (ABM) supports MaxCompute cluster scaling. To scale out a MaxCompute cluster, add physical hosts in the default cluster of Apsara Infrastructure Management Framework to the MaxCompute cluster. To scale in a MaxCompute cluster, remove physical hosts from the MaxCompute cluster to the default cluster of Apsara Infrastructure Management Framework.

Description

In Apsara Stack, scaling out a cluster involves complex operations. You must configure a new physical host on Deployment Planner and Apsara Infrastructure Management Framework so that it can be added to the default cluster of Apsara Infrastructure Management Framework. The default cluster of Apsara Infrastructure Management Framework is an idle resource pool that provides resources to scale out clusters. If you want to scale out a cluster, add physical hosts in the default cluster of Apsara Infrastructure Management Framework to the cluster. If you want to scale in a cluster, remove physical hosts from the cluster to the default cluster of Apsara Infrastructure Management Framework.

You can use this method to scale out or in a MaxCompute cluster in the ABM console.

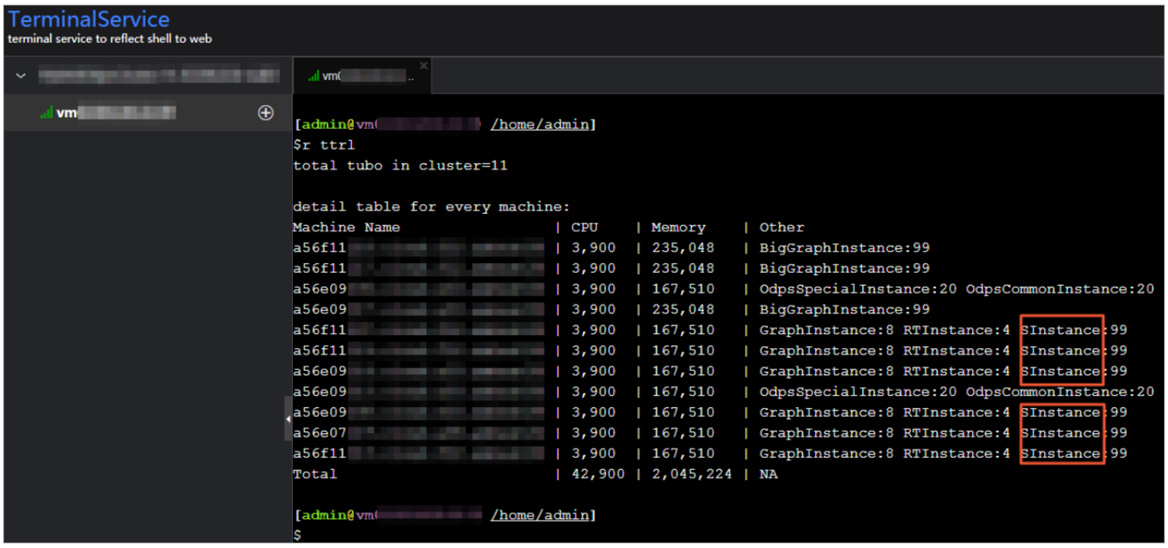
Prerequisites

- Scale-out: The physical host that you want to add is an SInstance host in the default cluster of Apsara Infrastructure Management Framework.
- Scale-out: The template host must be an SInstance host. You can log on to the admingateway host in a MaxCompute cluster to view SInstance hosts.
- Scale-in: The physical host that you want to remove is an SInstance host. You can log on to the admingateway host in a MaxCompute cluster to view SInstance hosts.

Scale out a MaxCompute cluster

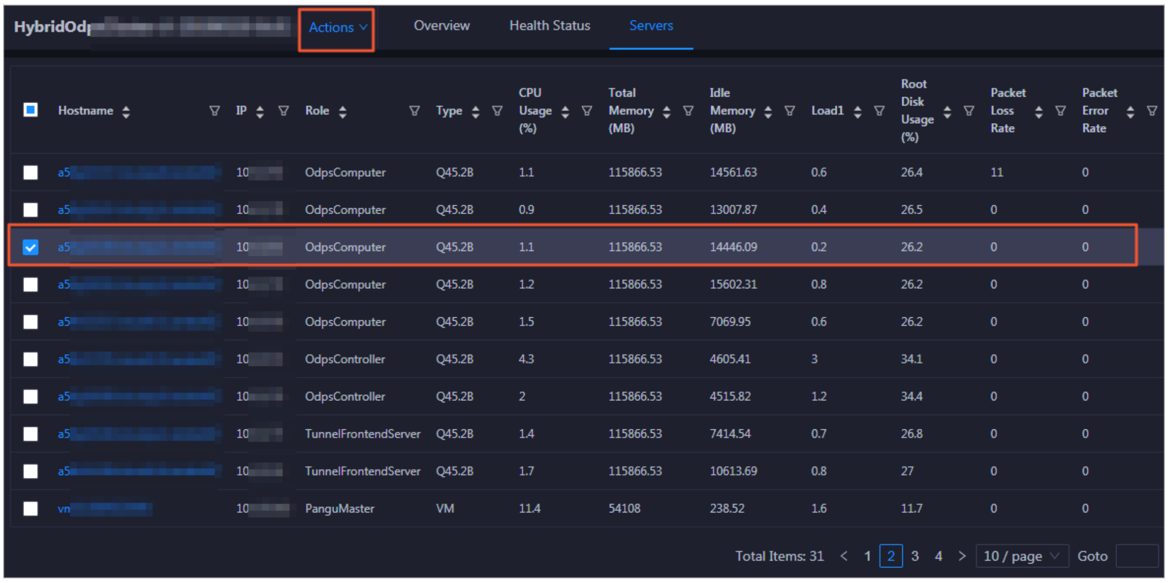
You can add multiple hosts to a MaxCompute cluster at a time to scale out the cluster. To add hosts to a MaxCompute cluster, you must specify an existing host as the template host. The hosts that you want to add copy configurations from the template host. This allows the hosts to be added to the cluster at a time.

1. Log on to the admingateway host in the MaxCompute cluster. Run the `r ttrl` command to query and record SInstance hosts. For more information about how to log on to a host, see Log on to a host.



```
[admin@vm[redacted] /home/admin]
$r ttrl
total tubo in cluster=11

detail table for every machine:
Machine Name                  | CPU    | Memory    | Other
a56f11[redacted]              | 3,900  | 235,048   | BigGraphInstance:99
a56f11[redacted]              | 3,900  | 235,048   | BigGraphInstance:99
a56e09[redacted]              | 3,900  | 167,510   | OdpsSpecialInstance:20 OdpsCommonInstance:20
a56e09[redacted]              | 3,900  | 235,048   | BigGraphInstance:99
a56f11[redacted]              | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56f11[redacted]              | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56e09[redacted]              | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56e09[redacted]              | 3,900  | 167,510   | OdpsSpecialInstance:20 OdpsCommonInstance:20
a56e09[redacted]              | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56e07[redacted]              | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56f11[redacted]              | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
Total                         | 42,900 | 2,045,224 | NA

[admin@vm[redacted] /home/admin]
$
```

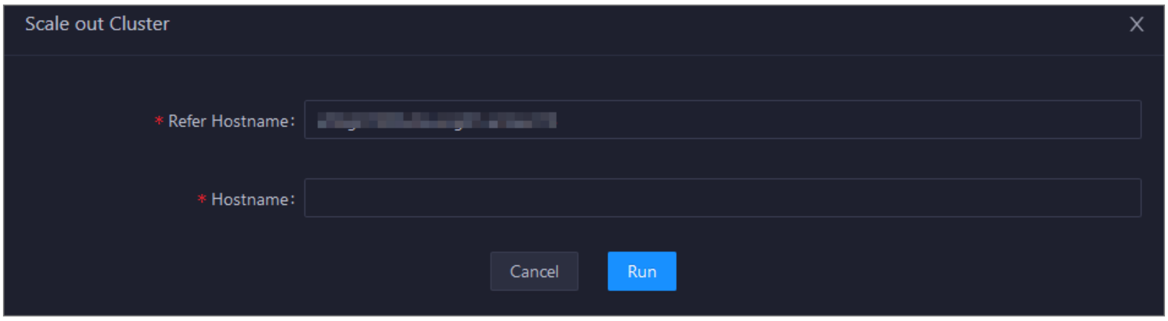
2. In the left-side navigation pane of the **Clusters** tab, click a cluster. Then, click the **Servers** tab. On the tab that appears, select an SInstance host and use it as the template host.



HybridOdp[redacted]

☐	Hostname	IP	Role	Type	CPU Usage (%)	Total Memory (MB)	Idle Memory (MB)	Load1	Root Disk Usage (%)	Packet Loss Rate	Packet Error Rate
☐	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	1.1	115866.53	14561.63	0.6	26.4	11	0
☐	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	0.9	115866.53	13007.87	0.4	26.5	0	0
☑	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	1.1	115866.53	14446.09	0.2	26.2	0	0
☐	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	1.2	115866.53	15602.31	0.8	26.2	0	0
☐	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	1.5	115866.53	7069.95	0.6	26.2	0	0
☐	a5[redacted]	10[redacted]	OdpsController	Q45.2B	4.3	115866.53	4605.41	3	34.1	0	0
☐	a5[redacted]	10[redacted]	OdpsController	Q45.2B	2	115866.53	4515.82	1.2	34.4	0	0
☐	a5[redacted]	10[redacted]	TunnelFrontendServer	Q45.2B	1.4	115866.53	7414.54	0.7	26.8	0	0
☐	a5[redacted]	10[redacted]	TunnelFrontendServer	Q45.2B	1.7	115866.53	10613.69	0.8	27	0	0
☐	vn[redacted]	10[redacted]	PanguMaster	VM	11.4	54108	238.52	1.6	11.7	0	0

3. In the upper-right corner, choose **Actions > Scale out Cluster**. In the **Scale out Cluster** panel, configure the parameters.



Scale out Cluster

* Refer Hostname: [redacted]

* Hostname:

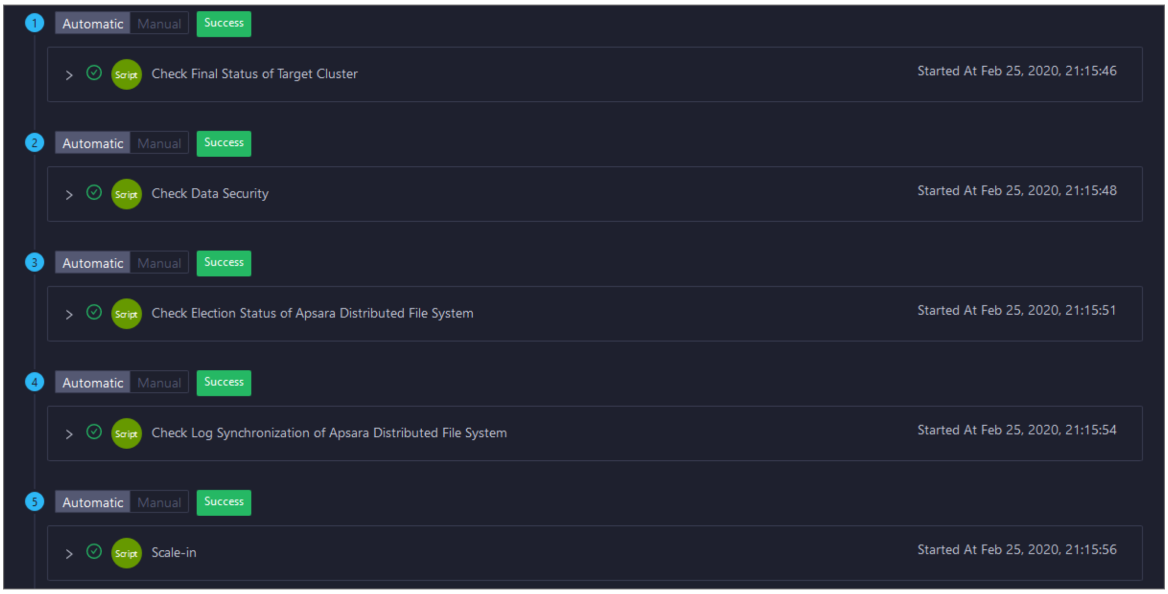
Parameters:

- Region: the region of the host that you want to add.
- Refer Hostname: the name of the template host. By default, the name of the selected host is used.
- Hostname: the name of the host that you want to add. The drop-down list displays all available hosts in the default cluster for scale-out operations. You can select one or more hosts from the drop-down list.

4. Click **Run**. A message appears, indicating that the request has been submitted.
5. View the scale-out status.

   In the upper-right corner, click **Actions** and select **Execution History** next to **Scale out Cluster** to view the scale-out history.

   It requires some time for the cluster to be scaled out. RUNNING indicates that the execution is in progress. SUCCESS indicates that the execution succeeds. FAILED indicates that the execution fails.
6. If the status is RUNNING, click **Details** in the Details column to view the steps and progress of the execution.



1 Automatic Manual Success

Check Final Status of Target Cluster — Started At Feb 25, 2020, 21:15:46

2 Automatic Manual Success

Check Data Security — Started At Feb 25, 2020, 21:15:48

3 Automatic Manual Success

Check Election Status of Apsara Distributed File System — Started At Feb 25, 2020, 21:15:51

4 Automatic Manual Success

Check Log Synchronization of Apsara Distributed File System — Started At Feb 25, 2020, 21:15:54

5 Automatic Manual Success

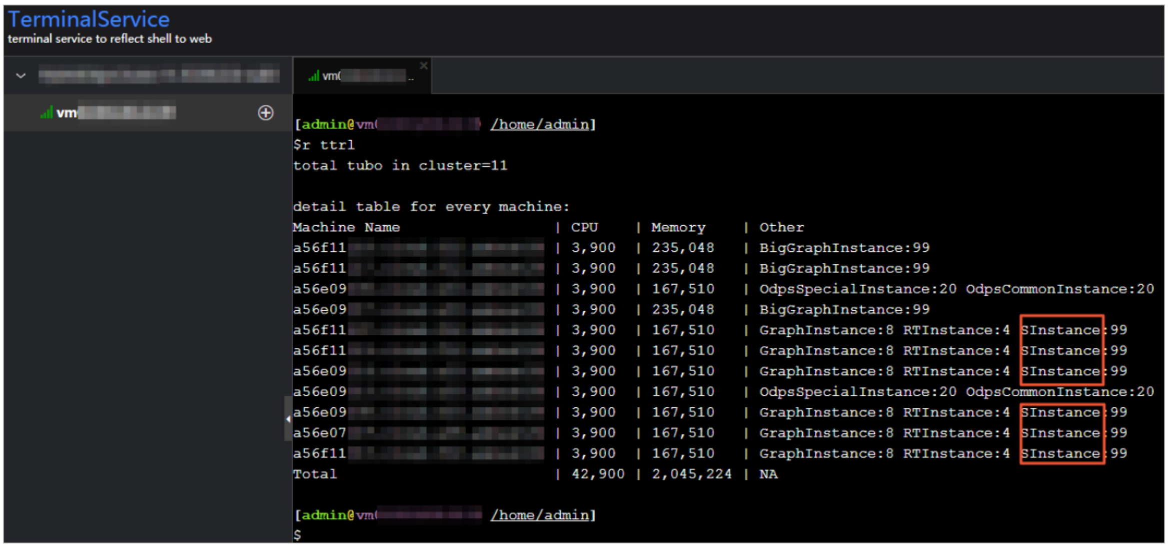
Scale-in — Started At Feb 25, 2020, 21:15:56

7. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure.

Scale in a MaxCompute cluster

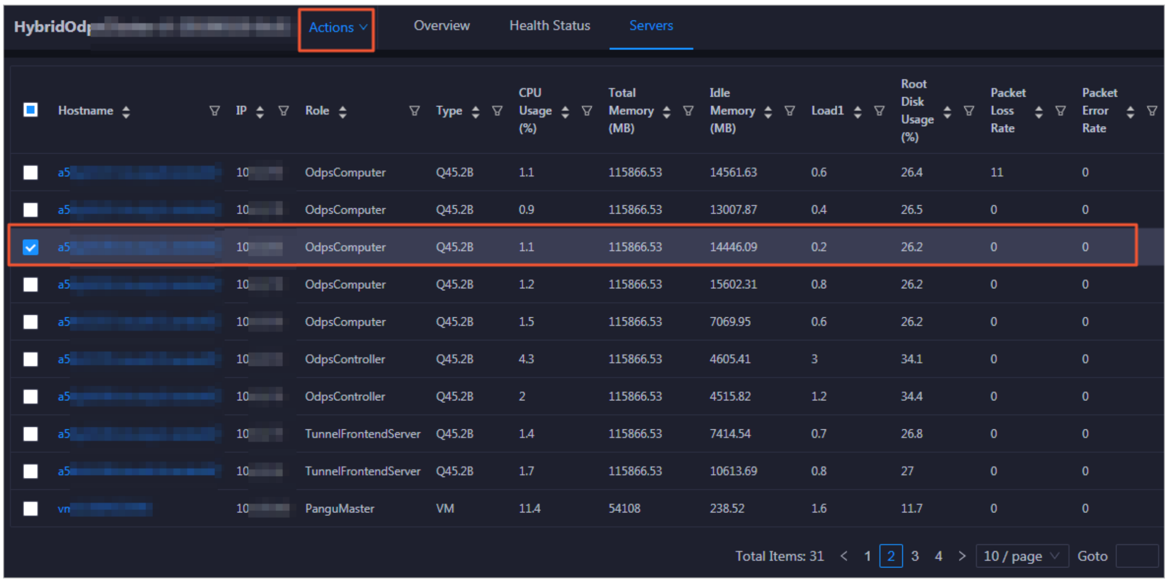
You can remove multiple hosts from a MaxCompute cluster at a time to scale in the cluster.

1. Log on to the admingateway host in the MaxCompute cluster. Run the `r ttrl` command to query and record SInstance hosts. For more information about how to log on to a host, see Log on to a host.



```
[admin@vm[redacted] /home/admin]
$r ttrl
total tubo in cluster=11

detail table for every machine:
Machine Name                      | CPU    | Memory    | Other
a56f11[redacted]                  | 3,900  | 235,048   | BigGraphInstance:99
a56f11[redacted]                  | 3,900  | 235,048   | BigGraphInstance:99
a56e09[redacted]                  | 3,900  | 167,510   | OdpsSpecialInstance:20 OdpsCommonInstance:20
a56e09[redacted]                  | 3,900  | 235,048   | BigGraphInstance:99
a56f11[redacted]                  | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56f11[redacted]                  | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56e09[redacted]                  | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56e09[redacted]                  | 3,900  | 167,510   | OdpsSpecialInstance:20 OdpsCommonInstance:20
a56e09[redacted]                  | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56e07[redacted]                  | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
a56f11[redacted]                  | 3,900  | 167,510   | GraphInstance:8 RTInstance:4 SInstance:99
Total                             | 42,900 | 2,045,224 | NA

[admin@vm[redacted] /home/admin]
$
```

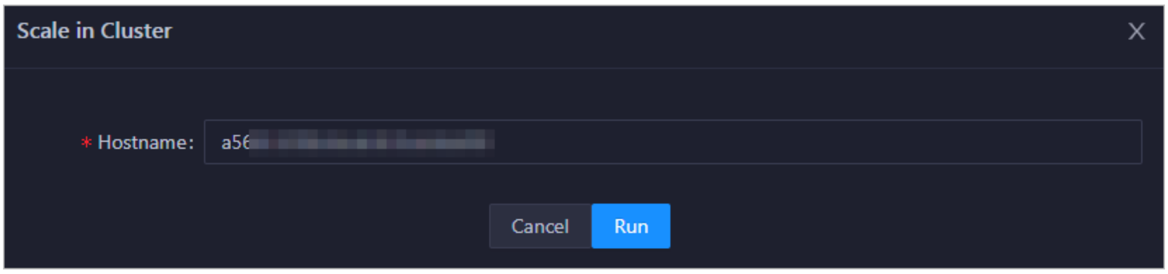
2. In the left-side navigation pane of the **Clusters** tab, click a cluster. Then, click the **Servers** tab. On the tab that appears, select one or more SInstance hosts that you want to remove.



■	Hostname	IP	Role	Type	CPU Usage (%)	Total Memory (MB)	Idle Memory (MB)	Load1	Root Disk Usage (%)	Packet Loss Rate	Packet Error Rate
□	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	1.1	115866.53	14561.63	0.6	26.4	11	0
□	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	0.9	115866.53	13007.87	0.4	26.5	0	0
☑	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	1.1	115866.53	14446.09	0.2	26.2	0	0
□	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	1.2	115866.53	15602.31	0.8	26.2	0	0
□	a5[redacted]	10[redacted]	OdpsComputer	Q45.2B	1.5	115866.53	7069.95	0.6	26.2	0	0
□	a5[redacted]	10[redacted]	OdpsController	Q45.2B	4.3	115866.53	4605.41	3	34.1	0	0
□	a5[redacted]	10[redacted]	OdpsController	Q45.2B	2	115866.53	4515.82	1.2	34.4	0	0
□	a5[redacted]	10[redacted]	TunnelFrontendServer	Q45.2B	1.4	115866.53	7414.54	0.7	26.8	0	0
□	a5[redacted]	10[redacted]	TunnelFrontendServer	Q45.2B	1.7	115866.53	10613.69	0.8	27	0	0
□	vn[redacted]	10[redacted]	PanguMaster	VM	11.4	54108	238.52	1.6	11.7	0	0

Total Items: 31 < 1 2 3 4 > 10 / page Goto

3. In the upper-right corner, choose **Actions > Scale in Cluster**. In the **Scale in Cluster** panel, configure the parameters.


Scale in Cluster

* Hostname: a56[redacted]

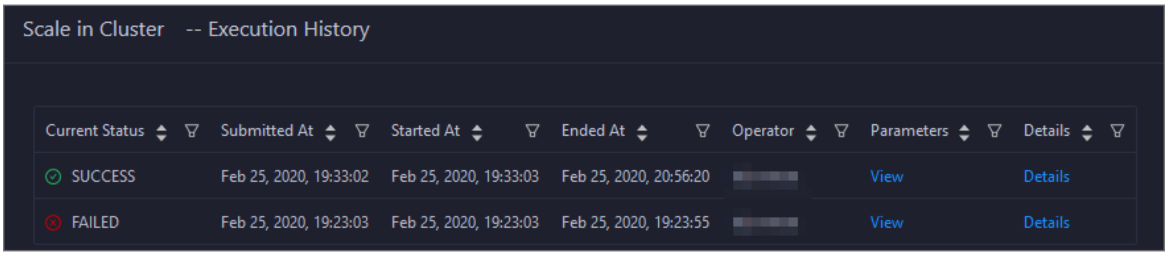
Parameters:

- Region: the region of the host that you want to remove.
- Hostname: the name of the host that you want to remove. By default, the name of the selected host is used.

4. Click **Run**. A message appears, indicating that the request has been submitted.
5. View the scale-in status.

   In the upper-right corner, click **Actions** and select **Execution History** next to **Scale in Cluster** to view the scale-in history.

   It requires some time for the cluster to be scaled in. RUNNING indicates that the execution is in progress. SUCCESS indicates that the execution succeeds. FAILED indicates that the execution fails.
6. If the status is RUNNING, click **Details** in the Details column to view the steps and progress of the execution.


Scale in Cluster -- Execution History

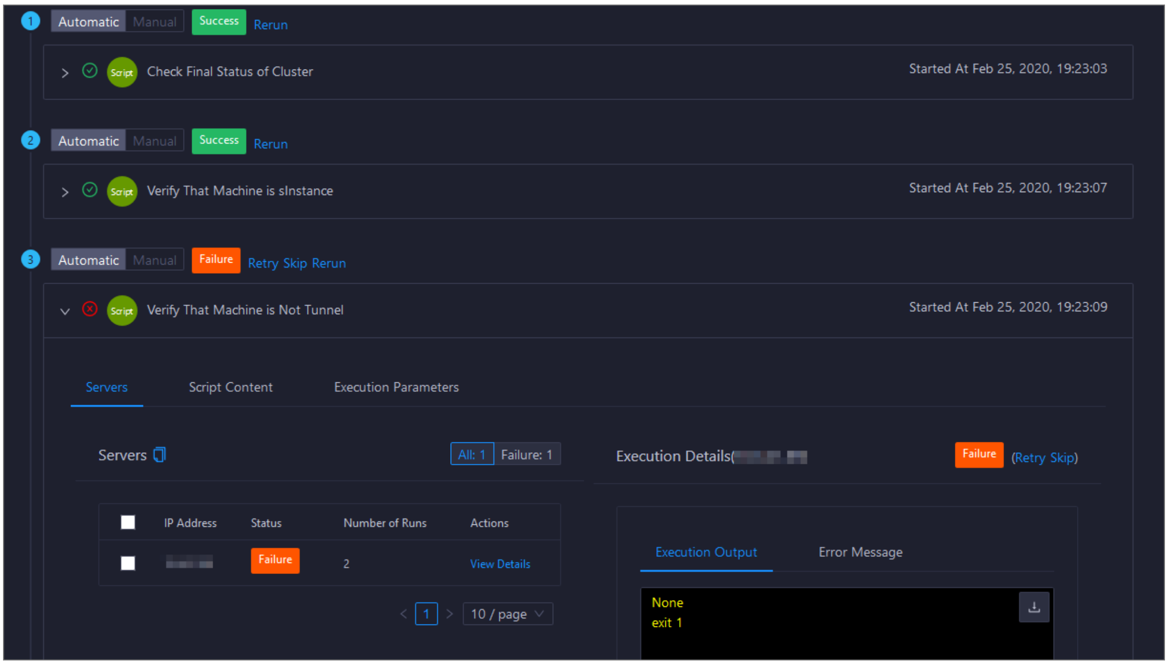
Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
✓ SUCCESS	Feb 25, 2020, 19:33:02	Feb 25, 2020, 19:33:03	Feb 25, 2020, 20:56:20	[redacted]	View	Details
☒ FAILED	Feb 25, 2020, 19:23:03	Feb 25, 2020, 19:23:03	Feb 25, 2020, 19:23:55	[redacted]	View	Details

7. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure.

Identify the cause of a scale-in or scale-out failure

This section uses cluster scale-in as an example to describe how to identify the cause of a failure.

1. In the upper-right corner of the **Clusters** tab, click **Actions** and select **Execution History** next to **Scale in Cluster** to view the scale-in history.
2. Click **Details** in the Details column of a failed operation to identify the cause of the failure.



```
None
exit 1
```

You can view information about parameter settings, host details, scripts, and runtime parameters to identify the cause of the failure.

11.2.5.4.6. Restore environment settings and enable auto repair

Apsara Big Data Manager (ABM) allows you to restore the environment settings for multiple hosts in a MaxCompute cluster at a time. It also allows you to enable the auto repair feature for a MaxCompute cluster.

Restore environment settings

ABM allows you to restore the environment settings for multiple hosts in a MaxCompute cluster at a time.

1. In the upper-right corner of the **Clusters** tab, choose **Actions > Restore Environment Settings**. In the **Restore Environment Settings** panel, set the Hosts parameter.

   > **Note** You can enter the names of multiple hosts and must separate the names with commas (,).

2. Click **Run**. A message appears, indicating that the request has been submitted.
3. View the restoration status.

Click **Actions** and select **Execution History** next to **Restore Environment Settings** to view the restoration history.

It requires some time for the restoration to complete. RUNNING indicates that the execution is in progress. SUCCESS indicates that the execution succeeds. FAILED indicates that the execution fails.

4. If the status is RUNNING, click **Details** in the Details column to view the steps and progress of the execution.
5. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure.

Enable auto repair

ABM allows you to enable the auto repair feature for a MaxCompute cluster. After this feature is enabled, repair tickets reported by Xunyangjian are automatically handled.

1. In the upper-right corner of the **Clusters** tab, choose **Actions > Enable Auto Repair**. In the **Enable Auto Repair** panel, set the Cluster parameter and select Enable for Auto Repair.

   Parameters:

   - Cluster: the name of the cluster for which you want to enable the auto repair feature.
   - Auto Repair: If you require the feature, select **Enable**. Otherwise, select **Disable**.
2. Click **Run**. A message appears, indicating that the request has been submitted.
3. View the status of the feature.

   Click **Actions** and select **Execution History** next to **Enable Auto Repair** to view the feature-related operation history.

   RUNNING indicates that the execution is in progress. SUCCESS indicates that the execution succeeds. FAILED indicates that the execution fails.
4. If the status is RUNNING, click **Details** in the Details column to view the steps and progress of the execution.
5. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure.

11.2.5.5. Host O&M

11.2.5.5.1. O&M features and entry

This topic describes MaxCompute host O&M features. It also provides more information about how to go to the host O&M page.

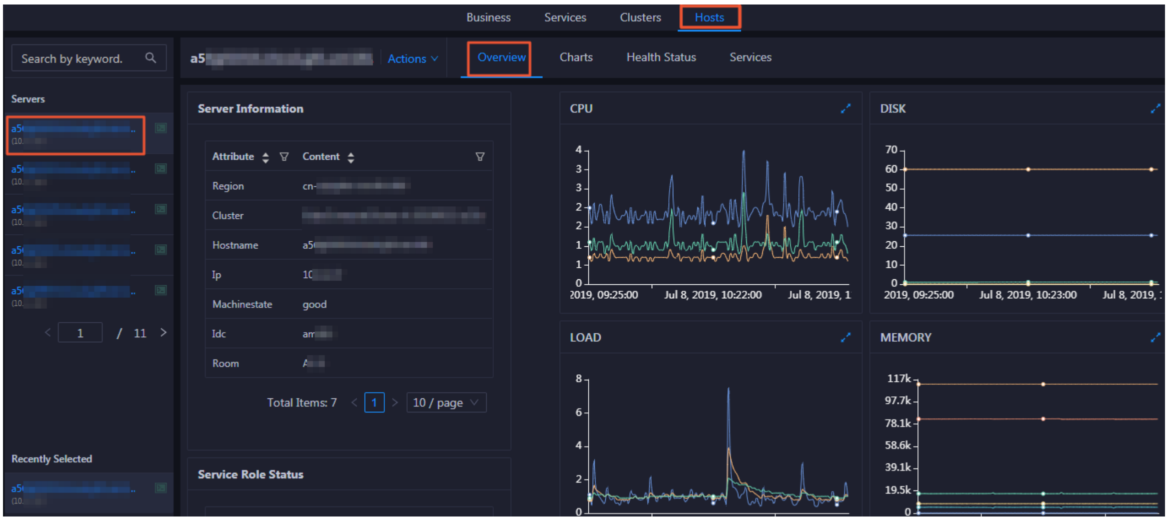
Host O&M features

- Overview: shows brief information about hosts in a MaxCompute cluster. The information includes the server information, server role status, health check result, and health check history. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, and packet transmission for the host.
- Charts: shows the enlarged trend charts of CPU utilization, memory usage, disk usage, load, and packet transmission.
- Health Status: shows all checkers for a host. You can query checker details, check results for hosts in a cluster, and schemes to clear alerts (if any exists). You can also log on to a host and perform manual checks on the host.

- Services: shows the cluster, service instances, and service instance roles of a host.

Go to the Hosts tab

1. Log on to the Apsara Big Data Manager (ABM) console.
2. In the upper-left corner, click the ⊞ icon and then **MaxCompute**.
3. On the MaxCompute page, click **O&M** in the top navigation bar. Then, click the **Hosts** tab.
4. In the left-side navigation pane of the **Hosts** tab, select a host. The **Overview** tab for the host appears.



Attribute	Content
Region	cn-[redacted]
Cluster	[redacted]
Hostname	a5[redacted]
Ip	10[redacted]
Machinestate	good
Idc	am[redacted]
Room	A[redacted]

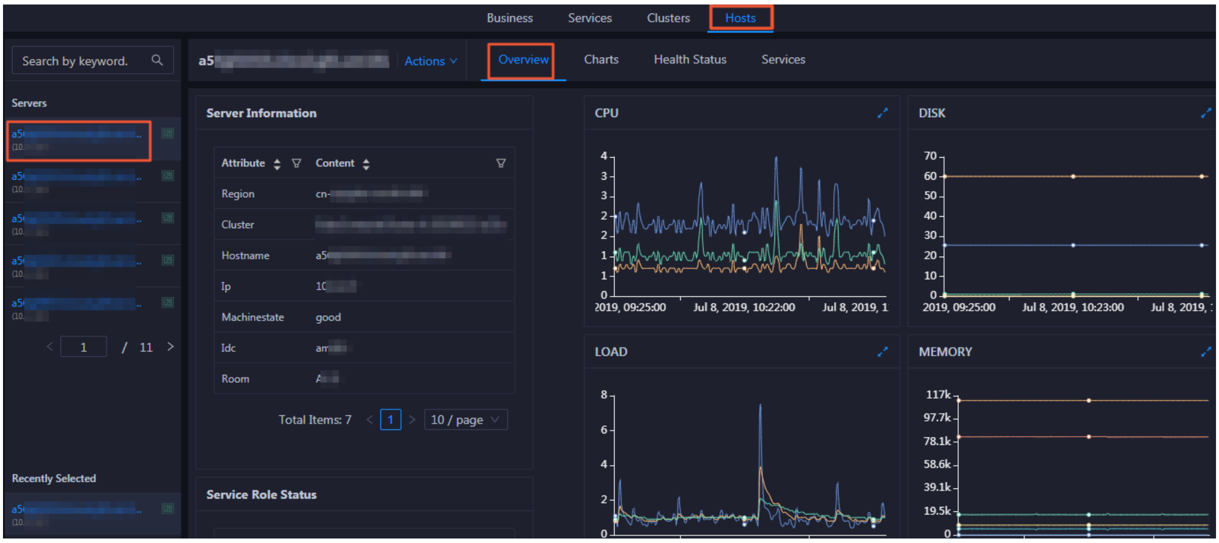
Total Items: 7 < 1 > 10 / page

11.2.5.5.2. Host overview

The Overview tab for a host shows brief information about the host in a MaxCompute cluster. On this tab, you can view server information, service role status, health check result, and health check history of the host. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, and packet transmission for the host.

Go to the Overview tab

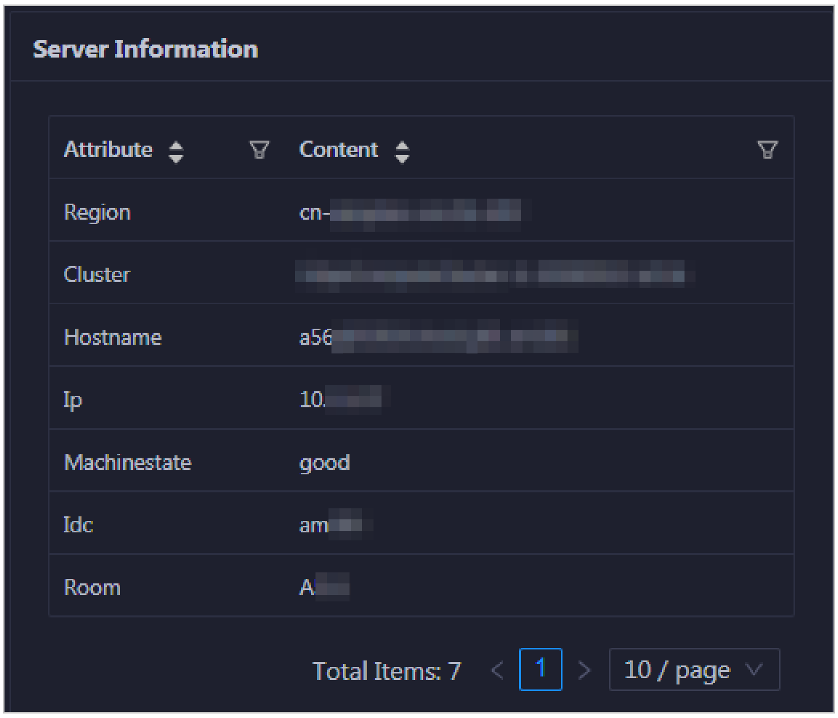
In the left-side navigation pane of the **Hosts** tab, click a host. Then, click the **Overview** tab. The **Overview** tab for the host appears.



On the **Overview** tab, you can view server information, service role status, health check result, and health check history of the host. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, and packet transmission for the host.

Server Information

The Server Information section shows information about the host. Server information includes the region, cluster, name, IP address, data center, and server room.



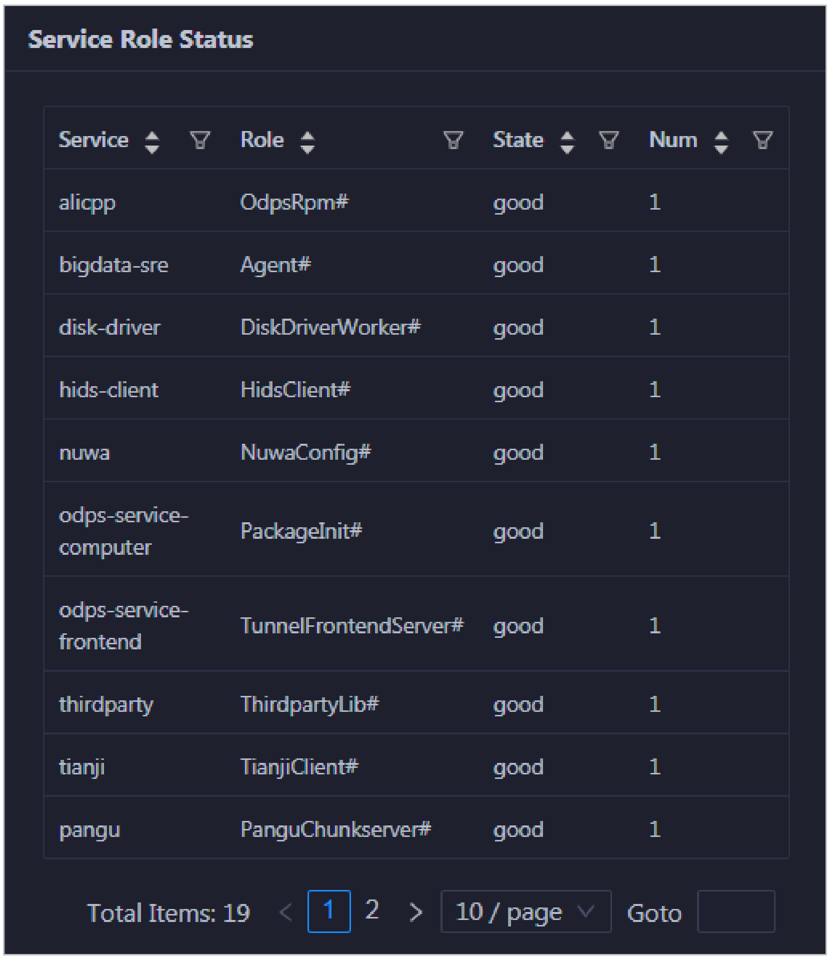
Server Information

Attribute	Content
Region	cn-[redacted]
Cluster	[redacted]
Hostname	a56[redacted]
Ip	10.[redacted]
Machinestate	good
Idc	am[redacted]
Room	A[redacted]

Total Items: 7 < 1 > 10 / page

Service Role Status

The Service Role Status section shows information about the services deployed on the host, including the roles, status, and number of services.



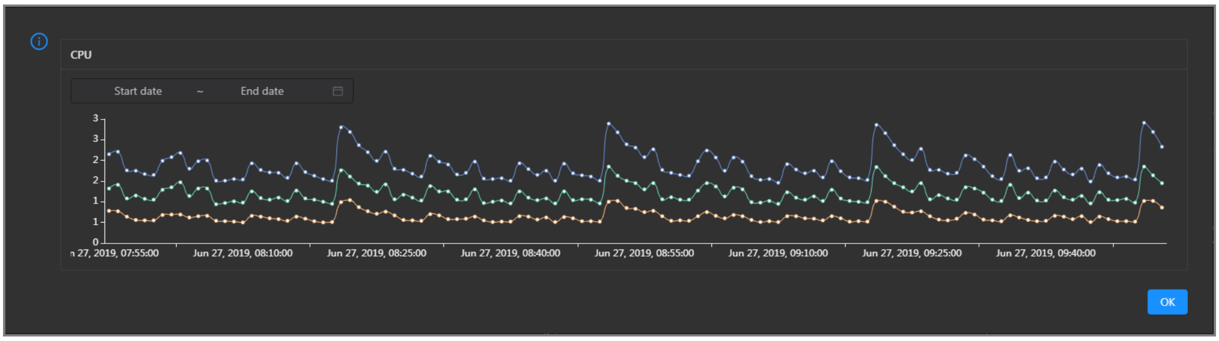
Service Role Status

Service	Role	State	Num
alicpp	OdpsRpm#	good	1
bigdata-sre	Agent#	good	1
disk-driver	DiskDriverWorker#	good	1
hids-client	HidsClient#	good	1
nuwa	NuwaConfig#	good	1
odps-service-computer	PackageInit#	good	1
odps-service-frontend	TunnelFrontendServer#	good	1
thirdparty	ThirdpartyLib#	good	1
tianji	TianjiClient#	good	1
pangu	PanguChunkserver#	good	1

CPU

The CPU chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) of the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

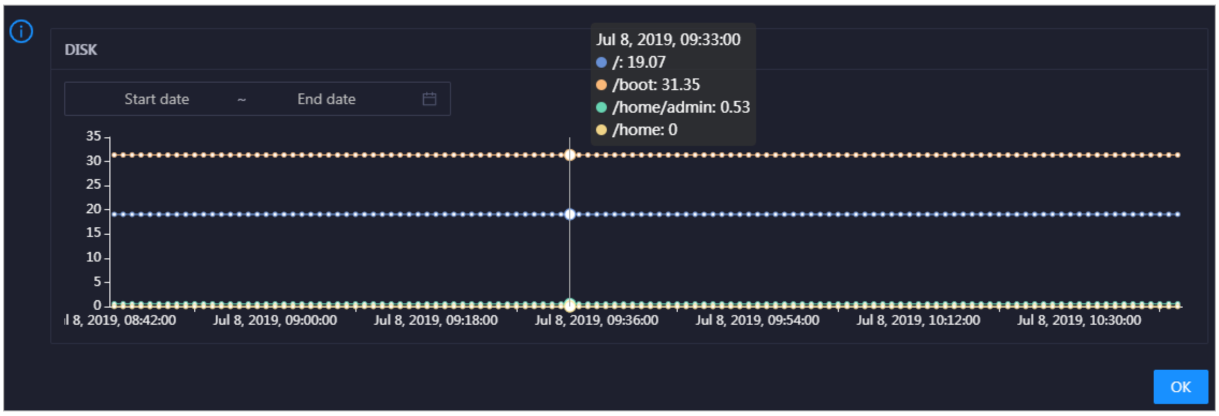


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the host in the specified period.

DISK

The DISK chart shows the trend lines of the storage usage in the */*, */boot*, */home/admin*, and */home* directories for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

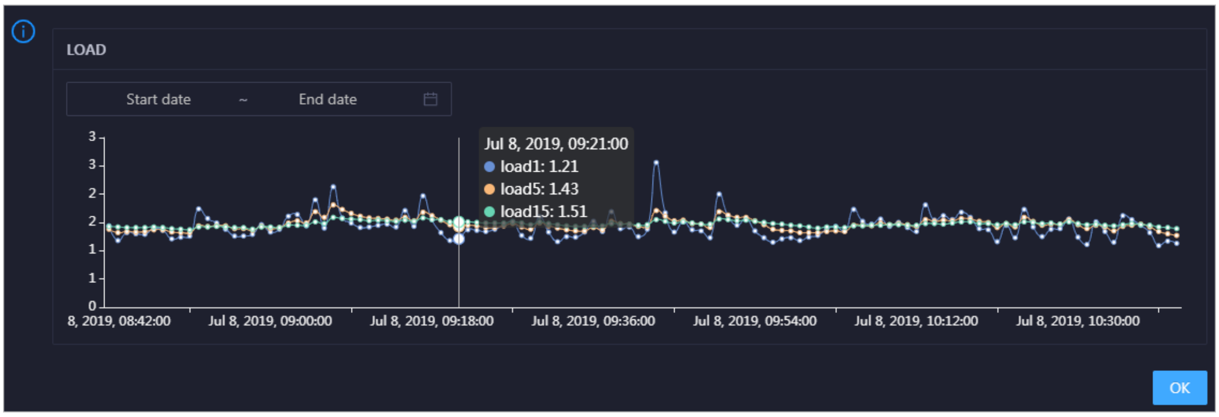


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the host in the specified period.

LOAD

The LOAD chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

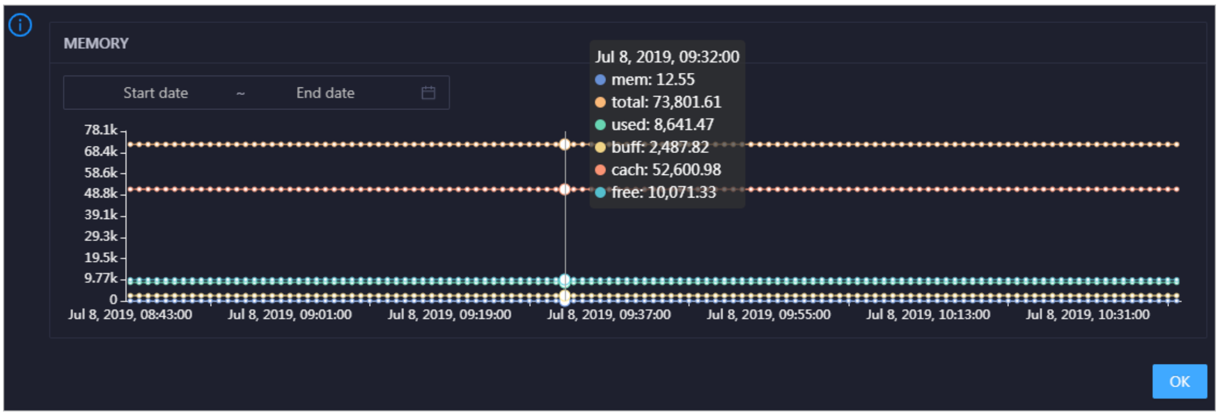


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the host in the specified period.

MEMORY

The MEMORY chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

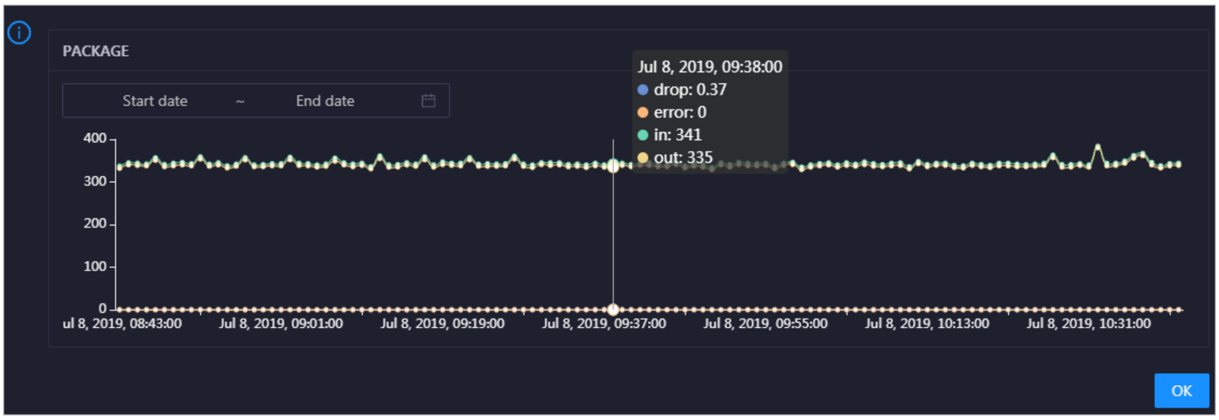


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the host in the specified period.

PACKAGE

The PACKAGE chart shows the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the host over time in different colors. These trend lines reflect the data transmission status of the host.

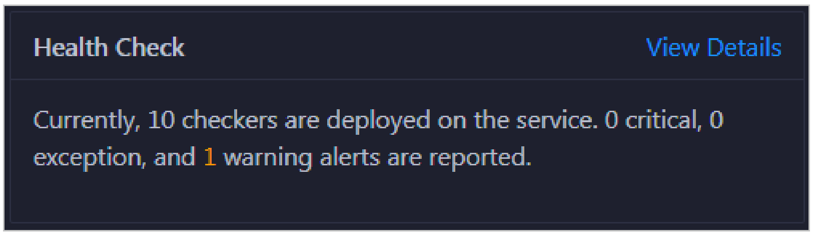
In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the host in the specified period.

Health Check

The Health Check section shows the number of checkers deployed for the host and the numbers of CRITICAL, WARNING, and EXCEPTION alerts.



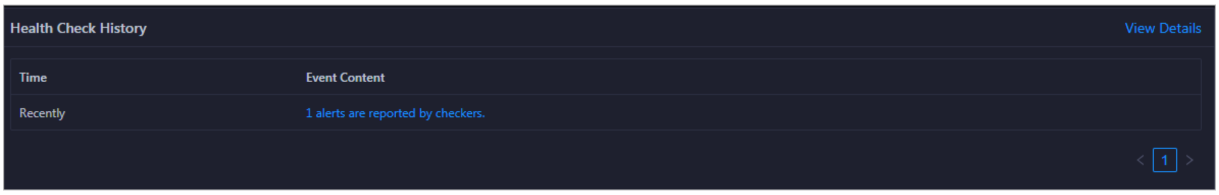
Health Check View Details

Currently, 10 checkers are deployed on the service. 0 critical, 0 exception, and 1 warning alerts are reported.

Click **View Details** to go to the Health Status tab. On this tab, you can view the health check details.

Health Check History

The Health Check History section shows the records of the health checks performed on the host.



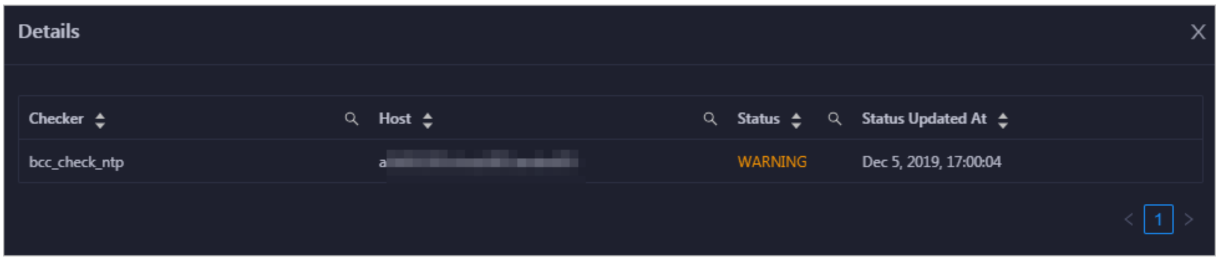
Health Check History

View Details

Time	Event Content
Recently	1 alerts are reported by checkers.

Click **View Details** to go to the Health Status tab. On this tab, you can view the health check details.

You can click the event content of a check to view the abnormal items.



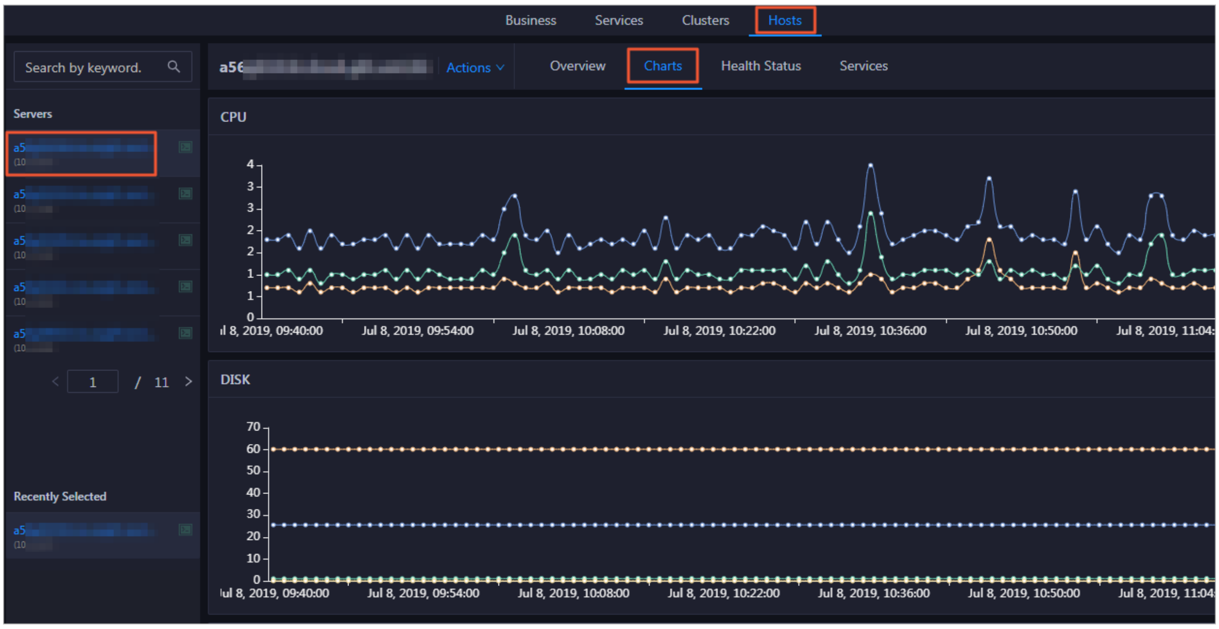
Details

Checker	Host	Status	Status Updated At
bcc_check_ntp	a[redacted]	WARNING	Dec 5, 2019, 17:00:04

11.2.5.5.3. Host charts

On the host chart page, you can view the enlarged trend charts of CPU usage, memory usage, storage usage, load, and packet transmission.

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Charts** tab. The **Charts** page for the host appears.



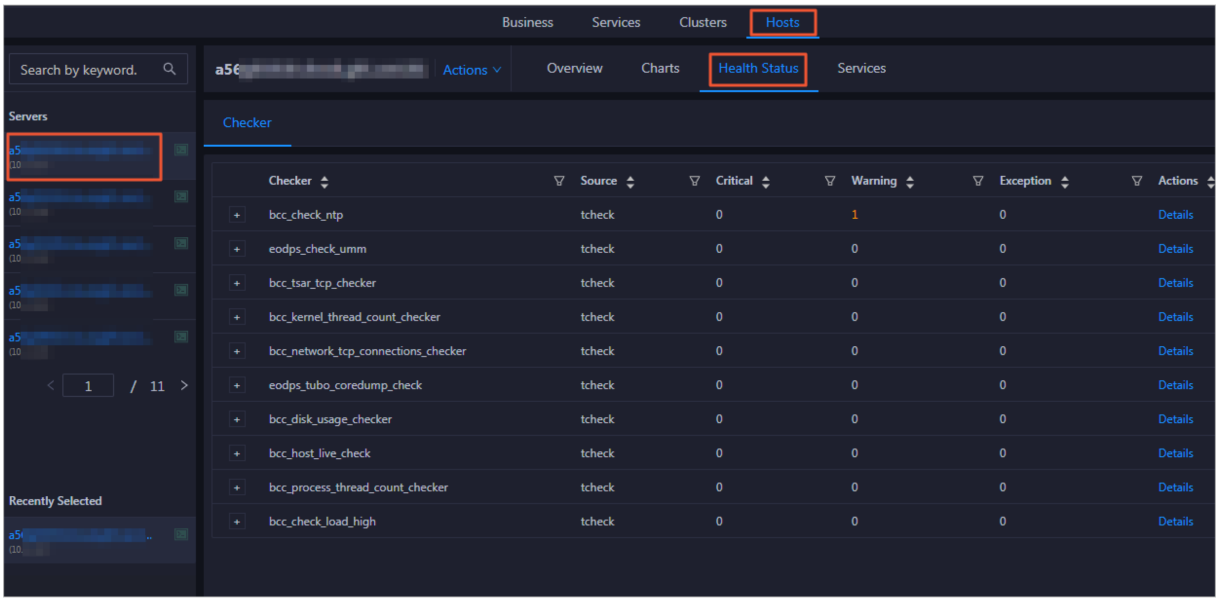
The **Charts** page displays trend charts of CPU usage, disk usage, memory usage, load, and packet transmission for the host. For more information, see Host overview.

11.2.5.5.4. Host health

On the Health Status page, you can view the checkers of the selected host, including the checker details, check results, and schemes to clear alerts (if any). In addition, you can log on to the host and perform manual checks on the host.

Entry

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Health Status** tab. The **Health Status** page for the host appears.

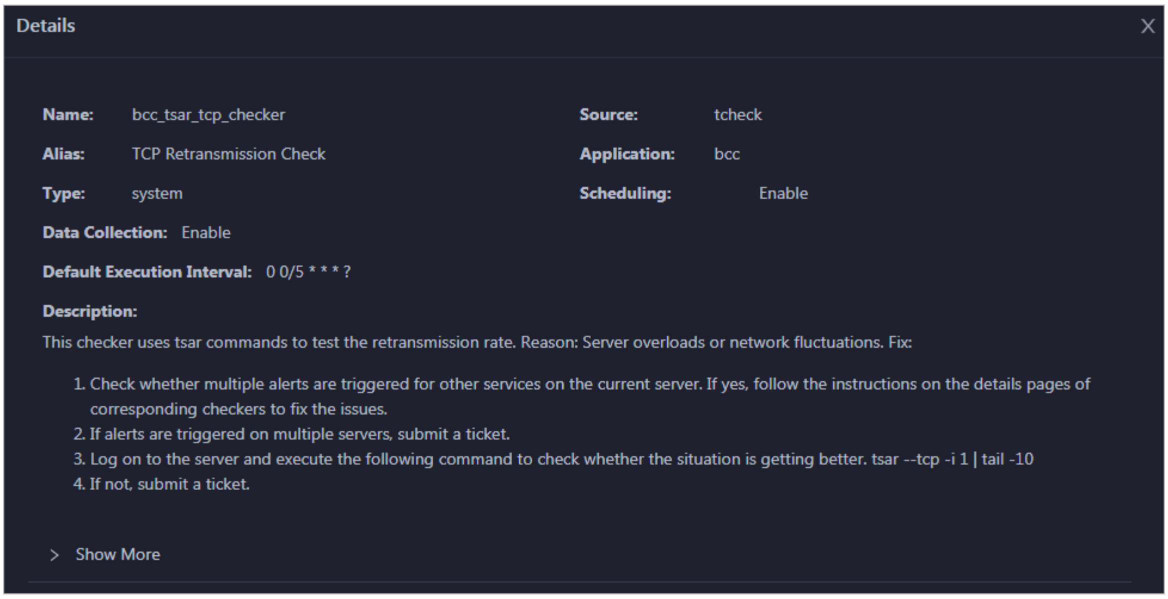


Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	1	0	Details
eodps_check_umm	tcheck	0	0	0	Details
bcc_tsar_tcp_checker	tcheck	0	0	0	Details
bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
bcc_network_tcp_connections_checker	tcheck	0	0	0	Details
eodps_tubo_coredump_check	tcheck	0	0	0	Details
bcc_disk_usage_checker	tcheck	0	0	0	Details
bcc_host_live_check	tcheck	0	0	0	Details
bcc_process_thread_count_checker	tcheck	0	0	0	Details
bcc_check_load_high	tcheck	0	0	0	Details

On the **Health Status** page, you can view all checkers and the check results for the host. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

View checker details

1. On the Health Status page, click **Details** in the Actions column of a checker. In the dialog box that appears, view the checker details.



Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

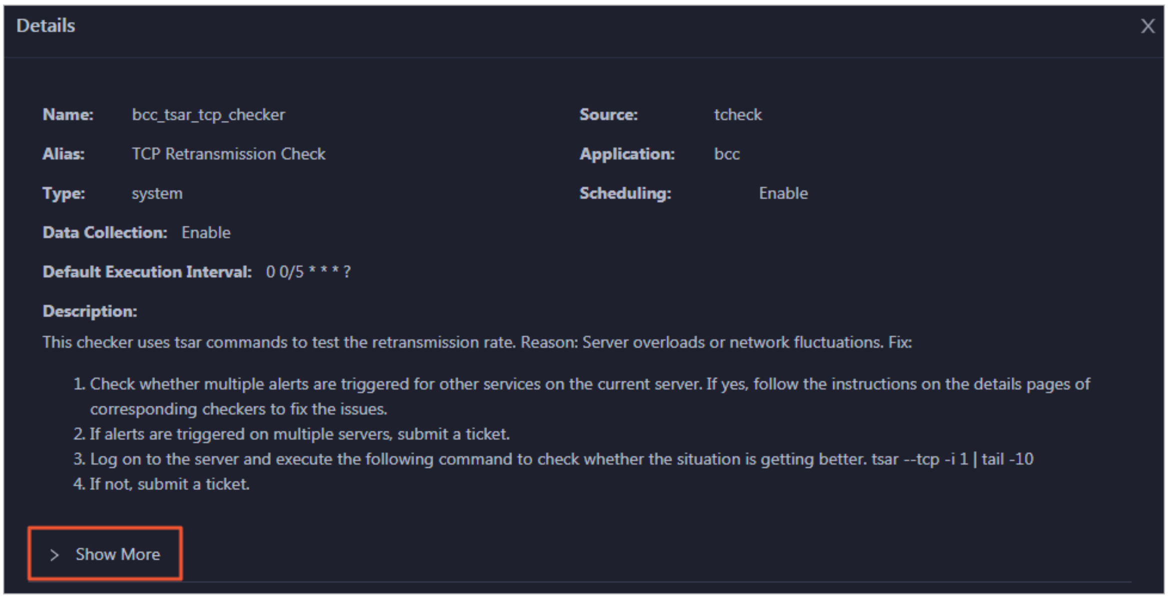
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include the name, source, alias, application, type, default execution interval, and description of the checker, whether scheduling is enabled, and whether data collection is enabled. The schemes to clear alerts are provided in the description.

2. Click **Show More** at the bottom to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker **Source:** tcheck

Alias: TCP Retransmission Check **Application:** bcc

Type: system **Scheduling:** Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

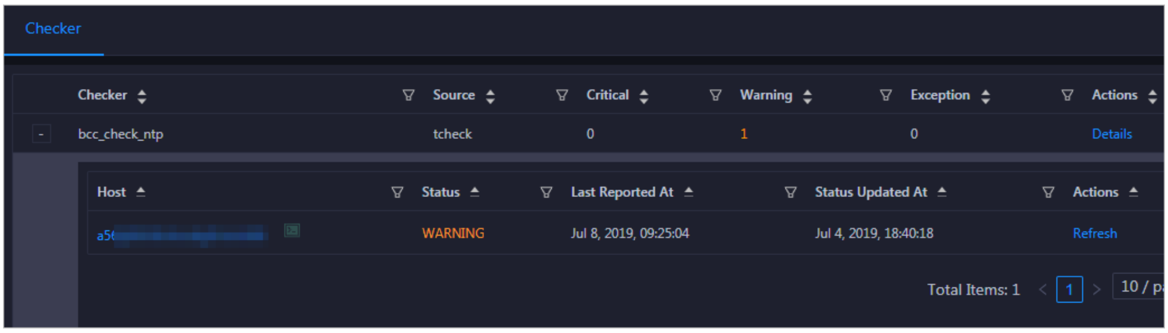
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about the execution script, execution target, default threshold, and mount point for data collection.

View alert causes

You can view the check history and check results of a checker.

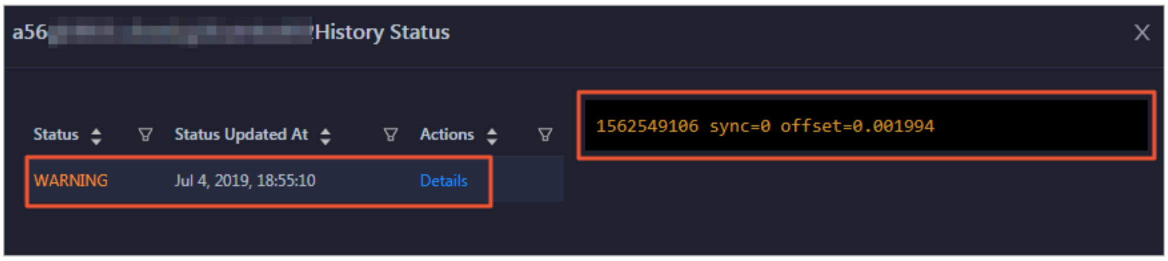
1. On the Health Status page, click **+** to expand a checker with alerts.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

2. Click the hostname. In the dialog box that appears, click **Details** in the Actions column of a check result to view the alert causes.



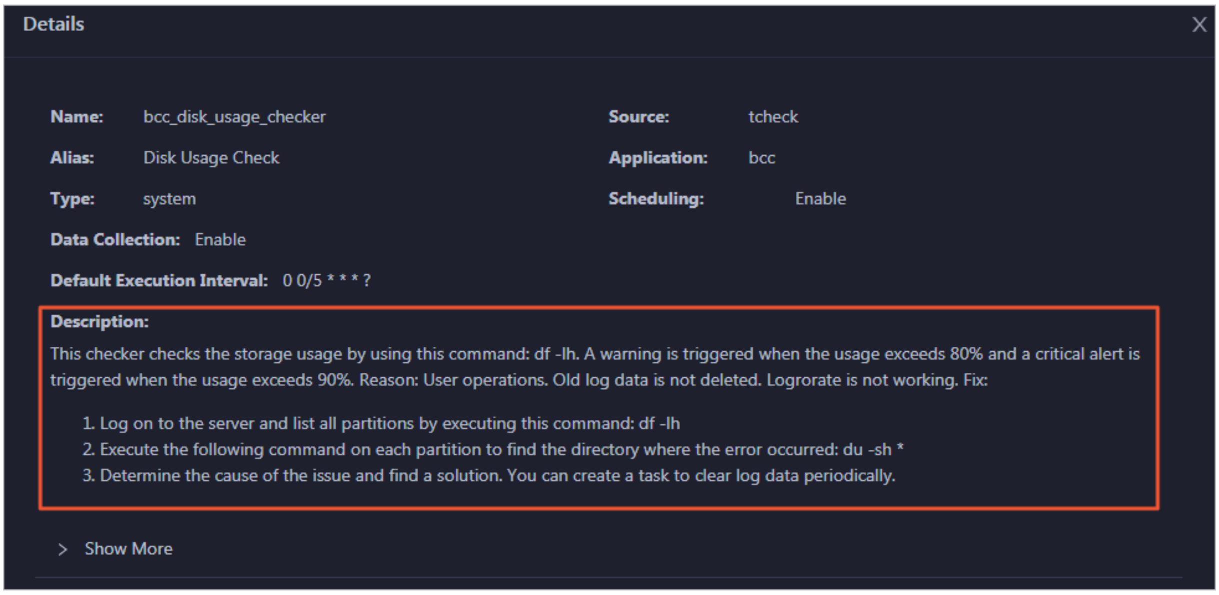
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status page, click **Details** in the Actions column of a checker with alerts. In the dialog box that appears, view the schemes to clear alerts.



Name: bcc_disk_usage_checker
Source: tcheck
Alias: Disk Usage Check
Application: bcc
Type: system
Scheduling: Enable
Data Collection: Enable
Default Execution Interval: 0 0/5 * * * ?

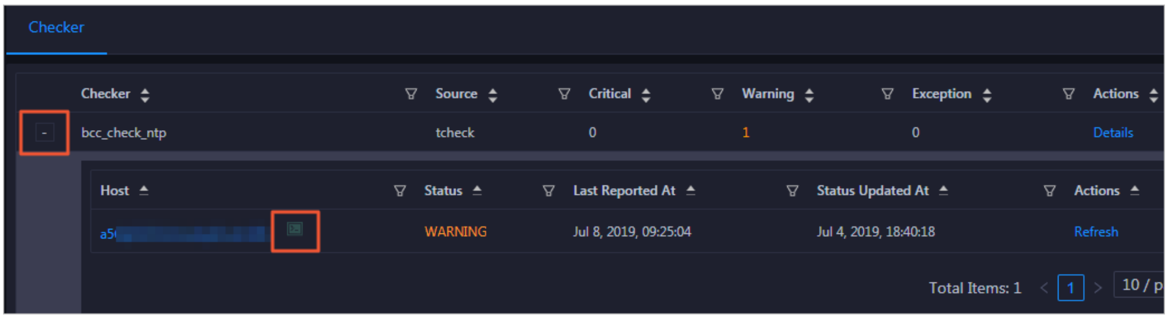
Description:
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

To log on to a host to clear alerts or perform other operations, follow these steps:

1. On the Health Status page, click **+** to expand a checker with alerts.

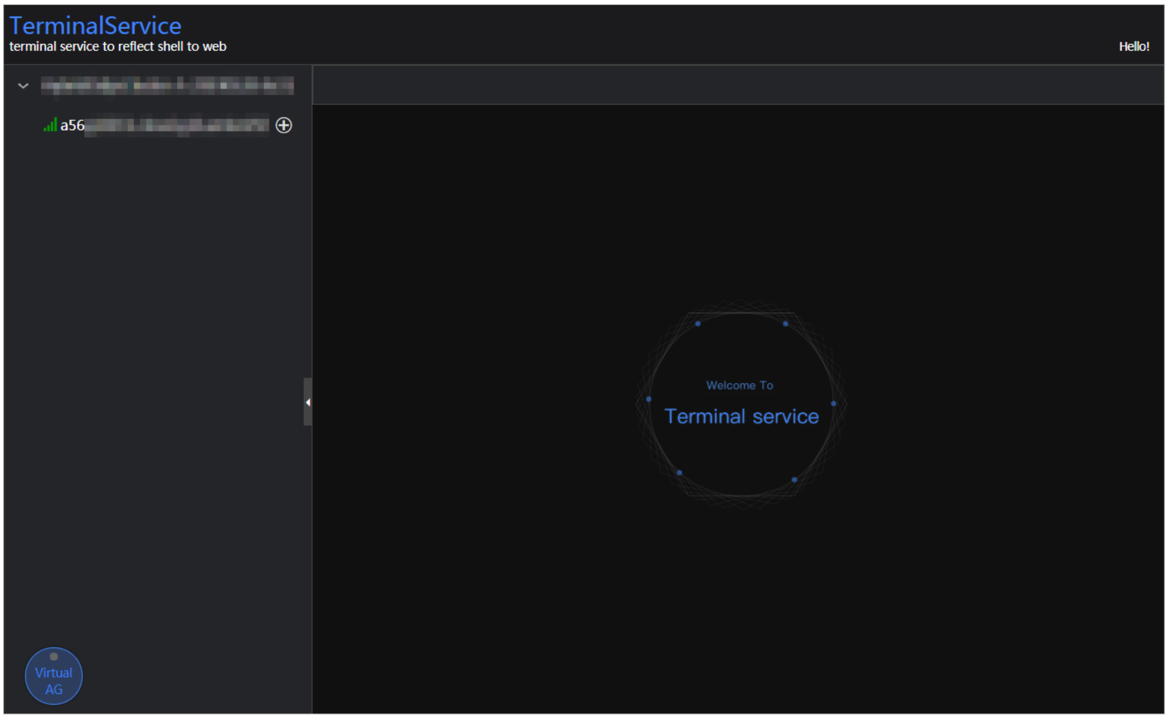


	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

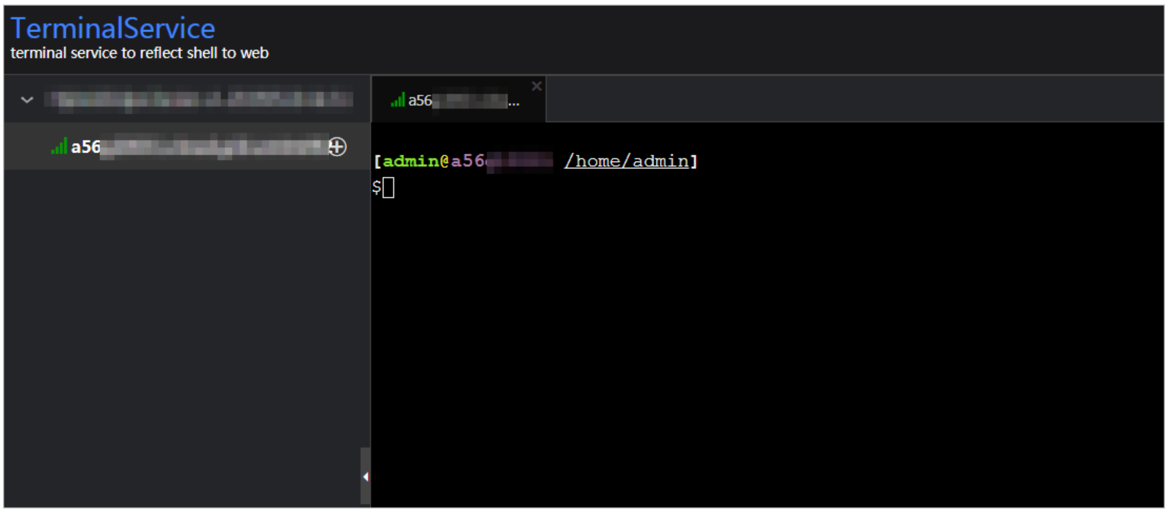
Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

2. Click the **Log On** icon of a host. The **TerminalService** page appears.



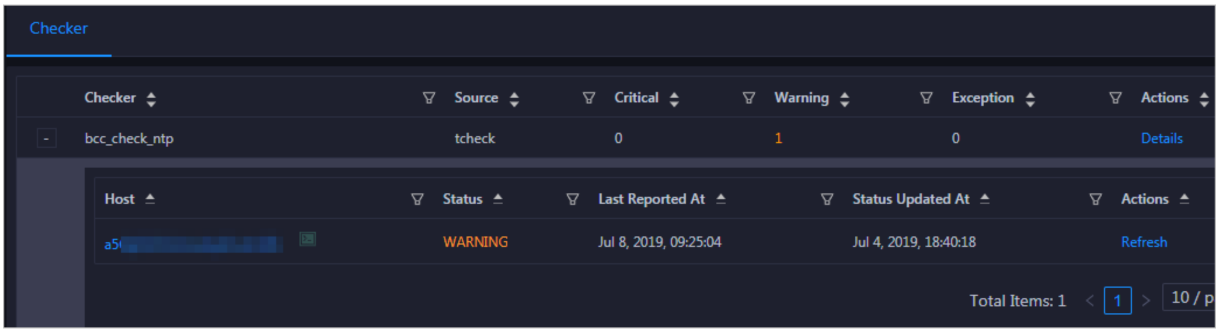
3. On the **TerminalService** page, click the hostname on the left to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. In this way, you can check whether the alert is cleared.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

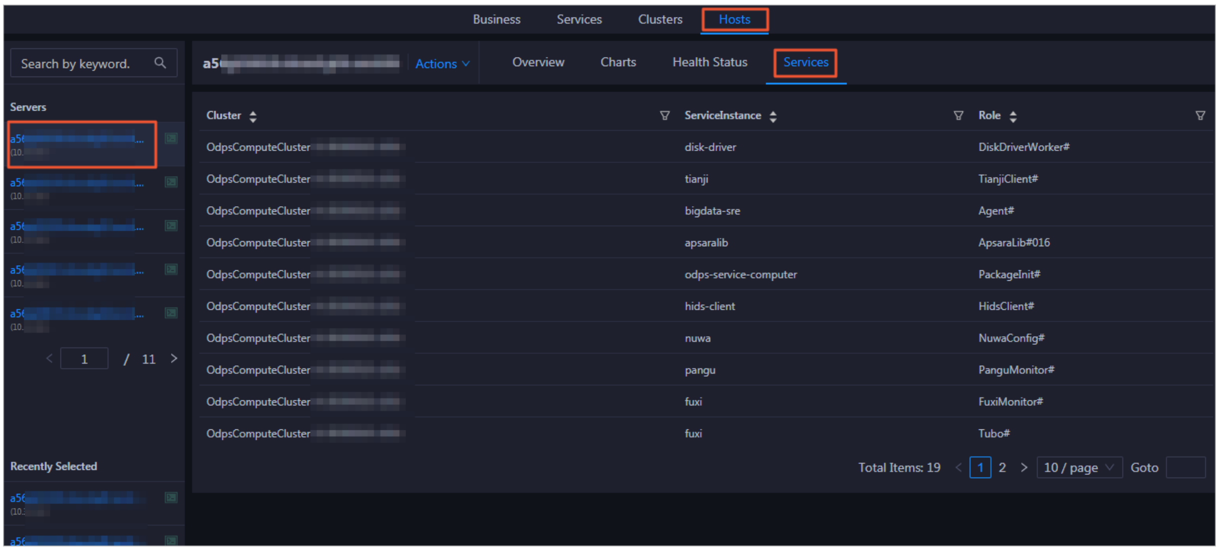
Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

11.2.5.5.5. Host services

On the Services page, you can view information about service instances and service instance roles of a host.

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Services** tab. The **Services** page for the host appears.



Cluster	ServiceInstance	Role
OdpsComputeCluster[redacted]	disk-driver	DiskDriverWorker#
OdpsComputeCluster[redacted]	tianji	TianjiClient#
OdpsComputeCluster[redacted]	bigdata-sre	Agent#
OdpsComputeCluster[redacted]	apsaralib	ApsaraLib#016
OdpsComputeCluster[redacted]	odps-service-computer	PackageInit#
OdpsComputeCluster[redacted]	hids-client	HidsClient#
OdpsComputeCluster[redacted]	nuwa	NuwaConfig#
OdpsComputeCluster[redacted]	pangu	PanguMonitor#
OdpsComputeCluster[redacted]	fuxi	FuxiMonitor#
OdpsComputeCluster[redacted]	fuxi	Tubo#

Total Items: 19 < 1 2 > 10 / page Goto

On the **Services** page, you can view the cluster, service instances, and service instance roles of the host.

11.3. DataWorks

11.3.1. Basic concepts and structure

11.3.1.1. What is DataWorks?

DataWorks is an end-to-end big data platform based on compute engines such as MaxCompute and E-MapReduce. It integrates all processes from data collection to data display and from data analysis to application running. DataWorks provides various features to help you complete the entire research and development (R&D) process in a quick and effective manner. The entire R&D process involves data integration, data development, data governance, data service provisioning, data quality control, and data security assurance.

DataWorks is an all-in-one solution for collecting, presenting, and analyzing data, and driving application development. It not only supports offline processing, analysis, and mining of large amounts of data, but also integrates core data-related technologies such as data development, data integration, production and operations and maintenance (O&M), real-time analysis, asset management, data quality control, data security assurance, and data sharing. In addition, it provides the DataService Studio and Machine Learning Platform for Artificial Intelligence (PAI) services.

In 2018, Forrester, a globally recognized market research company, named Alibaba Cloud DataWorks and MaxCompute as a world-leading cloud-based data warehouse solution. This solution is by far the only solution from a Chinese company to receive such an acknowledgment. Building on the success of the previous version, DataWorks V2.0 incorporates several new additions, such as workflows and script templates. DataWorks V2.0 supports dual workspaces for development, isolates the development environment from the production environment, adopts standard development processes, and uses a specific mechanism to reduce errors in code.

11.3.1.2. Benefits

This topic describes the benefits of DataWorks.

- Powerful computing capabilities

  DataWorks integrates with compute engines that can process large amounts of data.

  - DataWorks supports join operations for trillions of data records, millions of concurrent jobs, and petabytes (PB) of I/O throughput per day.
  - The offline scheduling system can run millions of concurrent jobs. You can configure rules and alerts to monitor the running statuses of nodes in real time.
  - DataWorks provides efficient and easy-to-use SQL and MapReduce engines, and supports most standard SQL syntax.
  - MaxCompute protects user data from loss, breach, or theft by using multi-layer data storage and access security mechanisms, including triplicate backups, read/write request authentication, application sandboxes, and system sandboxes.

- End-to-end platform

  DataWorks provides the graphical user interface (GUI) and allows multiple users to collaborate on a workspace.

  - DataWorks integrates all processes from data integration, processing, management, and monitoring to output.
  - You can create and edit workflows in a visual manner by using the workflow designer.
  - DataWorks provides a collaborative development environment. You can create and assign roles for varying nodes, such as development, online scheduling, maintenance, and data permission management, without locally processing data and nodes.

- Integration of heterogeneous data stores

  DataWorks supports batch synchronization of data among heterogeneous data stores at custom intervals in minutes, days, hours, weeks, or months. More than 400 pairs of heterogeneous data stores are supported.

- Web-based software

  DataWorks is an out-of-the-box service. You can use it on the Internet or an internal network without the need for installation and deployment.

- Multitenancy

  Data is isolated among different tenants. Each tenant controls permissions, processes data, allocates resources, and manages members in a unified and independent manner.

- Intelligent monitoring and alerting

By setting monitoring thresholds, you can control the entire process of all nodes as well as monitor the running status of each node.

- Easy-to-use SQL editor

  The SQL editor supports automatic code and metadata completion, code formatting and folding, and pre-compilation. It offers two editor themes. These features ensure a good user experience.

- Comprehensive data quality monitoring

  DataWorks allows you to control the quality of data in heterogeneous data stores, offline data, and real-time data. You can check data quality, configure alert notifications, and manage connections.

- Convenient API development and management

  The DataService Studio service of DataWorks interacts with API Gateway. This makes it easy for you to develop and publish APIs for data sharing.

- Secure data sharing

  DataWorks enables you to de-identify sensitive data before you share it with other tenants, which ensures the security of your big data assets and maximizes their value.

11.3.1.3. Introduction to data analytics

This topic describes two typical scenarios of data analytics.

Scenario 1: data synchronization and analysis

Scenario 1 shows a typical scenario of data analytics.

1. Collect data from various databases to MaxCompute by using DataWorks.
2. Log on to DataWorks, create SQL, MapReduce, and shell nodes, and commit the nodes to MaxCompute for data analysis.
3. Use DataWorks to synchronize the analysis results from MaxCompute to the databases from which you collect data.

Scenario 1

> **Note** Base is the name of DataWorks from the technical perspective.

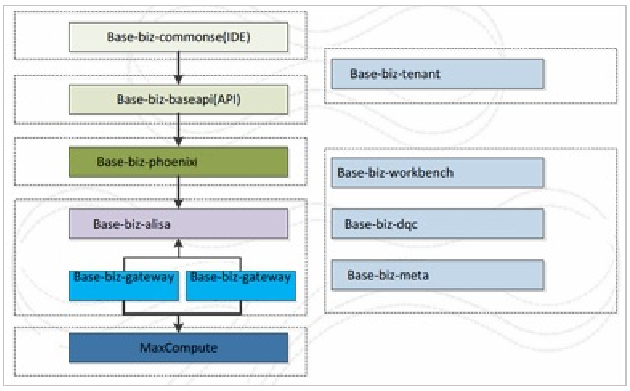
Scenario 2: data synchronization

DataWorks supports data synchronization between various databases. You can synchronize data by using DataWorks.

11.3.1.4. DataWorks architecture in Apsara Stack V3

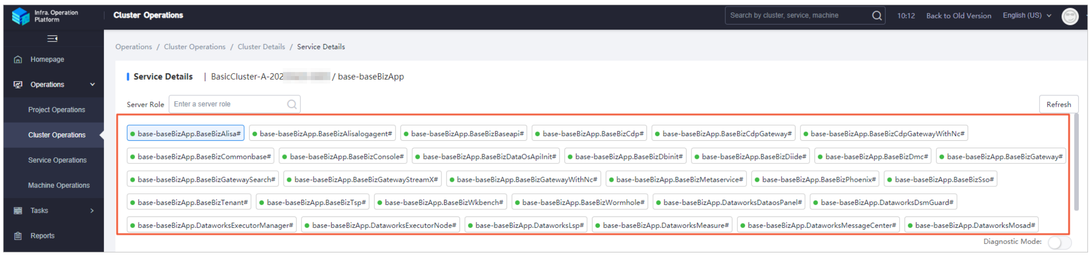
This topic describes the framework and services of DataWorks.

DataWorks framework



Services shown in the preceding figure play an important role for node scheduling and running. You can perform all O&M operations for DataWorks of Apsara Stack V3 in Apsara Infrastructure Management Framework. The following figure shows the services in DataWorks.

DataWorks services



Service Details | BasicCluster-A-202[redacted] / base-baseBizApp

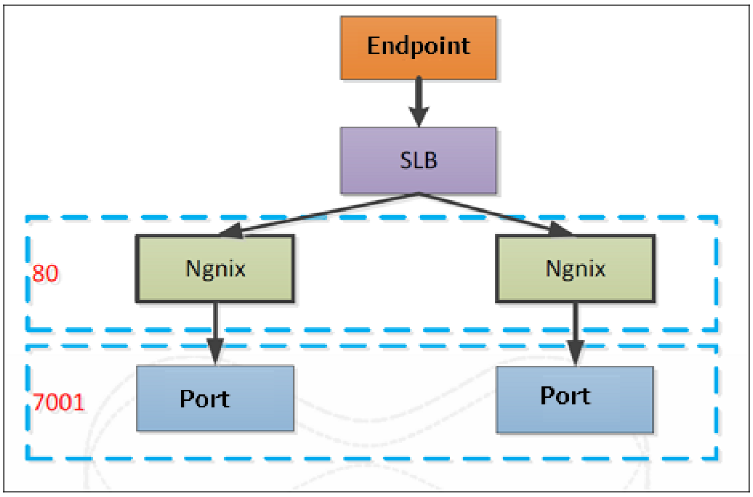
Server Role: Enter a server role

- base-baseBizApp.BaseBizAlisa#
- base-baseBizApp.BaseBizAlisalogagent#
- base-baseBizApp.BaseBizBaseapi#
- base-baseBizApp.BaseBizCdp#
- base-baseBizApp.BaseBizCdpGateway#
- base-baseBizApp.BaseBizCdpGatewayWithNc#
- base-baseBizApp.BaseBizCommonbase#
- base-baseBizApp.BaseBizConsole#
- base-baseBizApp.BaseBizDataOsApiInit#
- base-baseBizApp.BaseBizDbinit#
- base-baseBizApp.BaseBizDiide#
- base-baseBizApp.BaseBizDmc#
- base-baseBizApp.BaseBizGateway#
- base-baseBizApp.BaseBizGatewaySearch#
- base-baseBizApp.BaseBizGatewayStreamX#
- base-baseBizApp.BaseBizGatewayWithNc#
- base-baseBizApp.BaseBizMetaservice#
- base-baseBizApp.BaseBizPhoenix#
- base-baseBizApp.BaseBizSso#
- base-baseBizApp.BaseBizTenant#
- base-baseBizApp.BaseBizTsp#
- base-baseBizApp.BaseBizWkbench#
- base-baseBizApp.BaseBizWormhole#
- base-baseBizApp.DataworksDataosPanel#
- base-baseBizApp.DataworksDsmGuard#
- base-baseBizApp.DataworksExecutorManager#
- base-baseBizApp.DataworksExecutorNode#
- base-baseBizApp.DataworksLsp#
- base-baseBizApp.DataworksMeasure#
- base-baseBizApp.DataworksMessageCenter#
- base-baseBizApp.DataworksMosad#

All services in DataWorks are deployed in Docker containers. You can log on to a host and run the docker ps command to view the containers in which the services are deployed.

Service architecture shows the architecture of each service except base-biz-gateway.

Service architecture



11.3.1.5. Service directories

This topic describes the directory structure of each service.

base-biz-gateway service

The base-biz-gateway service receives and runs nodes from the DataWorks integrated development environment (IDE) and the scheduling system.

- Logs directory: stores the operational logs of the base-biz-gateway service.
- taskinfo directory: stores the code run by user nodes and the execution logs.
- target directory: the main directory of the base-biz-gateway service. This directory stores the service code, start script, stop script, and configuration files.

base-biz-cdp service

The base-biz-cdp service is used to synchronize data.

- Logs directory: stores the operational logs of the base-biz-cdp service.
- Conf directory: stores the configuration files of the base-biz-cdp service.
- Bin directory: stores the start script.

Other services

The base-biz-alisa service directory is used as an example.

- Logs directory: stores the operational logs of the base-biz-alisa service.
- Conf directory: stores the configuration files of the base-biz-alisa service.
- Bin directory: stores the start script.

11.3.2. O&M by using Apsara Big Data Manager

11.3.2.1. Log on to the ABM console

This topic describes how to log on to the Apsara Big Data Manager (ABM) console.

Prerequisites

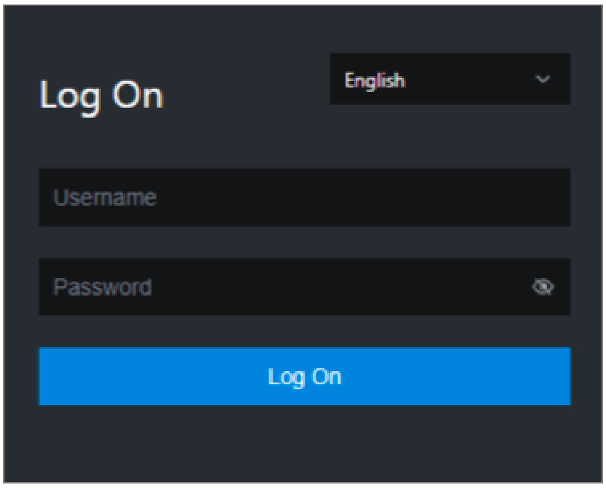
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.



> Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

> Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

For security reasons, your password must meet the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password must be 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Product Management > Products**.
7. In the **Big Data Services** section, choose **General-Purpose O&M > Apsara Big Data Manager**.

11.3.2.2. DataWorks O&M overview

This topic describes the features of DataWorks O&M supported by Apsara Big Data Manager (ABM) and how to access the DataWorks O&M page.

Modules

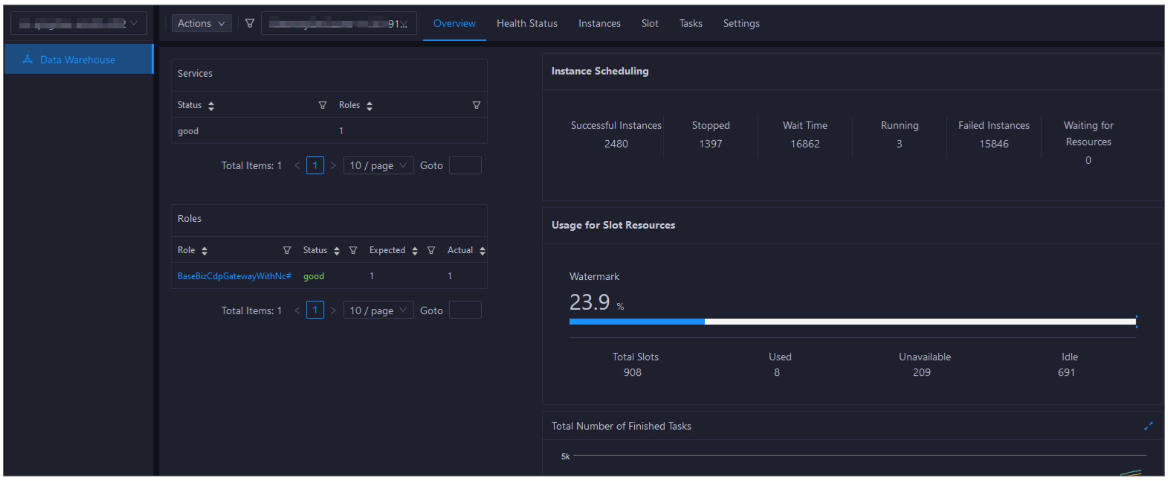
The modules provided by ABM for DataWorks O&M include the service, cluster, and host O&M modules. The following table describes them in detail.

Module	Sub-module	Description
Data Warehouse under Services	Overview	Displays the key operation metrics, including service overview, service status, instance scheduling information, and slot usage. On this page, you can also view the trend chart of the total number of finished nodes.
	Health Status	Displays all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.
	Instances	Displays the service roles of DataWorks.
	Slot	Displays the information about slot usage in DataWorks and allows you to change the number of slots in resource groups and hosts.
	Tasks	Displays the running status of DataWorks nodes.
	Settings	Allows you to change the values of configuration items for various service roles in DataWorks.
	Scale-up for Normal Hosts and Scale-down for Normal Hosts	Allows you to scale in or out a DataWorks cluster.
Data Integration under Services	Overview	Displays overall information about Data Integration in the **Task Scheduling Overview**, **Today's Tasks**, **Third-party Dependencies - Response Time (milliseconds)**, **Third-party Dependencies - Total Requests**, and **Third-party Dependencies - Request Error Rate** sections.
	Task	Displays information about Data Integration nodes on the **Instances** and **Multi-dimensional Analysis** tabs.
	Historical Analysis	Displays historical analysis information about Data Integration on the **Multi-dimensional Analysis**, **Execution Time Analysis**, and **Task Rankings** tabs.
Clusters	Overview	Displays the overall running and health check information about a cluster. On this page, you can view the health check result and health check history of the cluster. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the cluster.
	Health Status	Displays all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Module	Sub-module	Description
Hosts	Overview	Displays the overall running and health check information about a host. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.
	Health Status	Displays all checkers of a host, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Go to the DataWorks O&M page

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** tab under the **Data Warehouse** page appears.



Services

Status	Roles
good	1

Total Items: 1 < 1 > 10 / page Goto

Roles

Role	Status	Expected	Actual
BaseBizCdpGatewayWithNc#	good	1	1

Total Items: 1 < 1 > 10 / page Goto

Instance Scheduling

Successful Instances	Stopped	Wait Time	Running	Failed Instances	Waiting for Resources
2480	1397	16862	3	15846	0

Usage for Slot Resources

Watermark
23.9 %

Total Slots	Used	Unavailable	Idle
908	8	209	691

The **O&M** page includes three modules: **Services**, **Clusters**, and **Hosts**.

11.3.2.3. Service O&M

11.3.2.3.1. Data Warehouse

11.3.2.3.1.1. Service overview

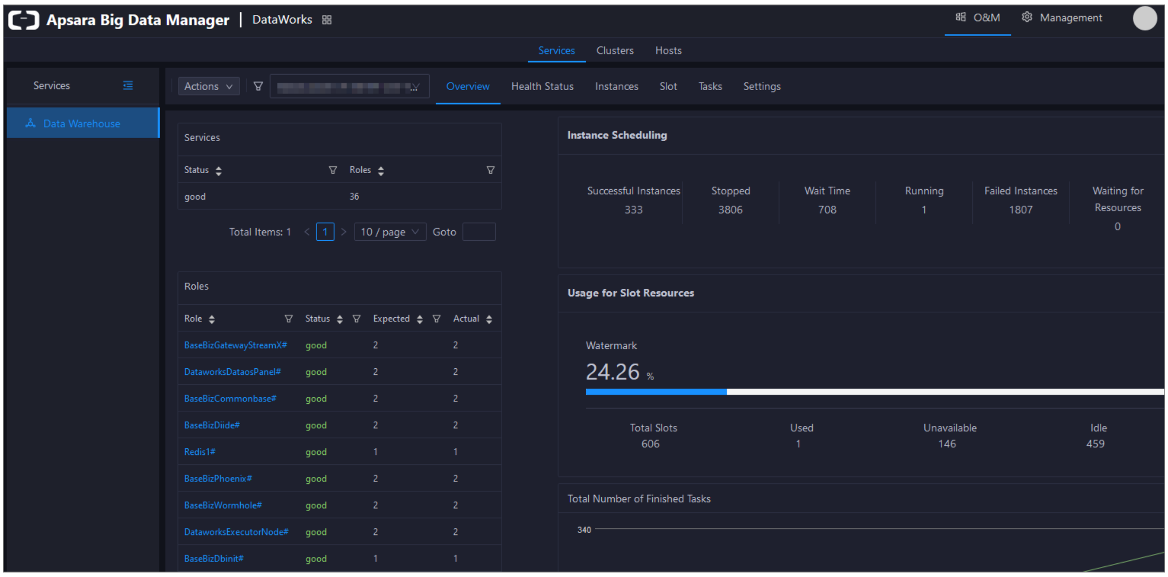
The DataWorks Overview page displays the key operation metrics, including service overview, service status, instance scheduling information, and slot usage. On this page, you can also view the trend chart of the total number of finished tasks.

Go to the Overview page under Services

1. Log on to the ABM console.

2. Click ⊞ in the upper-left corner and select **DataWorks**.

3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** tab under the **Data Warehouse** page appears.



Services

Status	Roles
good	36

Total Items: 1 < 1 > 10 / page Goto

Roles

Role	Status	Expected	Actual
BaseBizGatewayStreamX#	good	2	2
DataworksDataosPanel#	good	2	2
BaseBizCommonbase#	good	2	2
BaseBizDiide#	good	2	2
Redis1#	good	1	1
BaseBizPhoenix#	good	2	2
BaseBizWormhole#	good	2	2
DataworksExecutorNode#	good	2	2
BaseBizDbinit#	good	1	1

Instance Scheduling

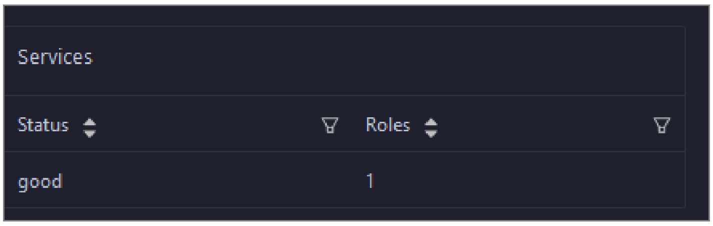
Successful Instances	Stopped	Wait Time	Running	Failed Instances	Waiting for Resources
333	3806	708	1	1807	0

Usage for Slot Resources

Total Slots	Used	Unavailable	Idle
606	1	146	459

Services

This section displays the numbers of available services, unavailable services, and services that are being respectively upgraded.

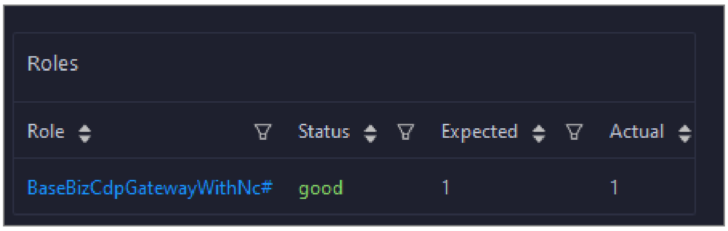


Services

Status	Roles
good	1

Roles

This section displays all DataWorks service roles and their statuses. You can also view the expected and actual numbers of hosts in the desired state for each service role.

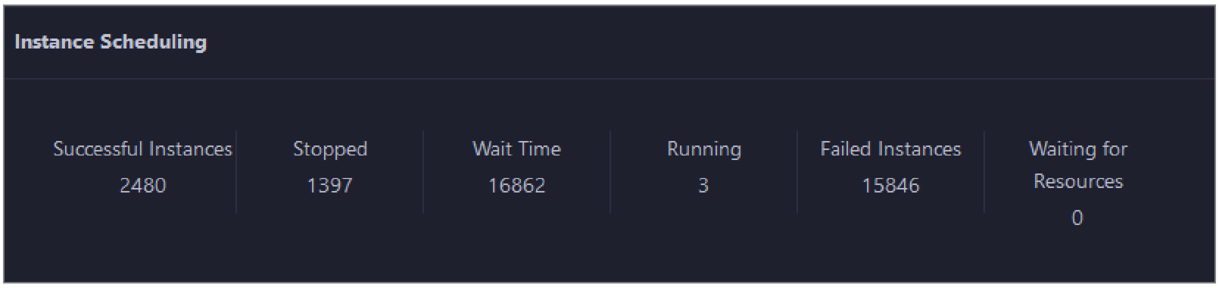


Roles

Role	Status	Expected	Actual
BaseBizCdpGatewayWithNc#	good	1	1

Instance Scheduling

This section displays the number of successful instances, number of instances not running, waiting duration, number of running instances, number of failed instances, and number of instances waiting for resources.

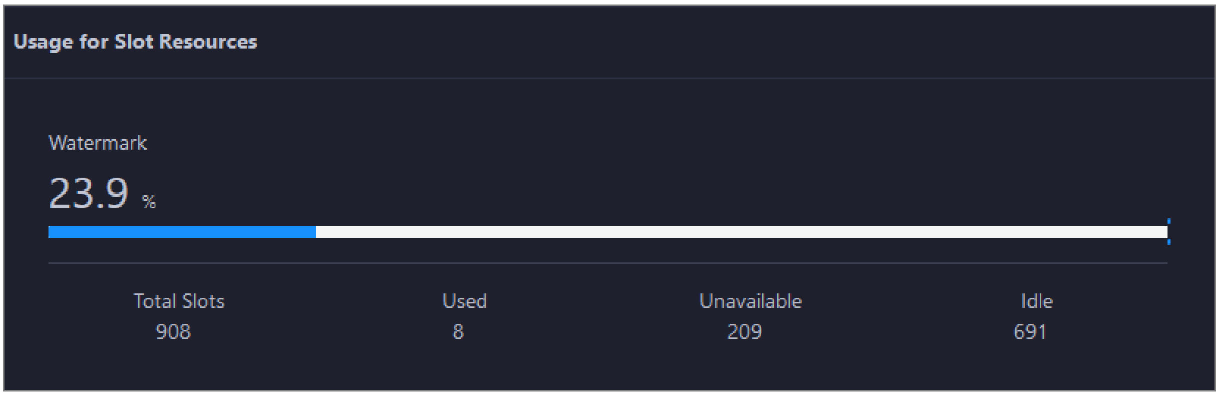


Instance Scheduling

Successful Instances	Stopped	Wait Time	Running	Failed Instances	Waiting for Resources
2480	1397	16862	3	15846	0

Usage for Slot Resources

This section displays the total number of slots, the number of used slots, the number of unavailable slots, and the number of idle slots for DataWorks.



Usage for Slot Resources

Watermark

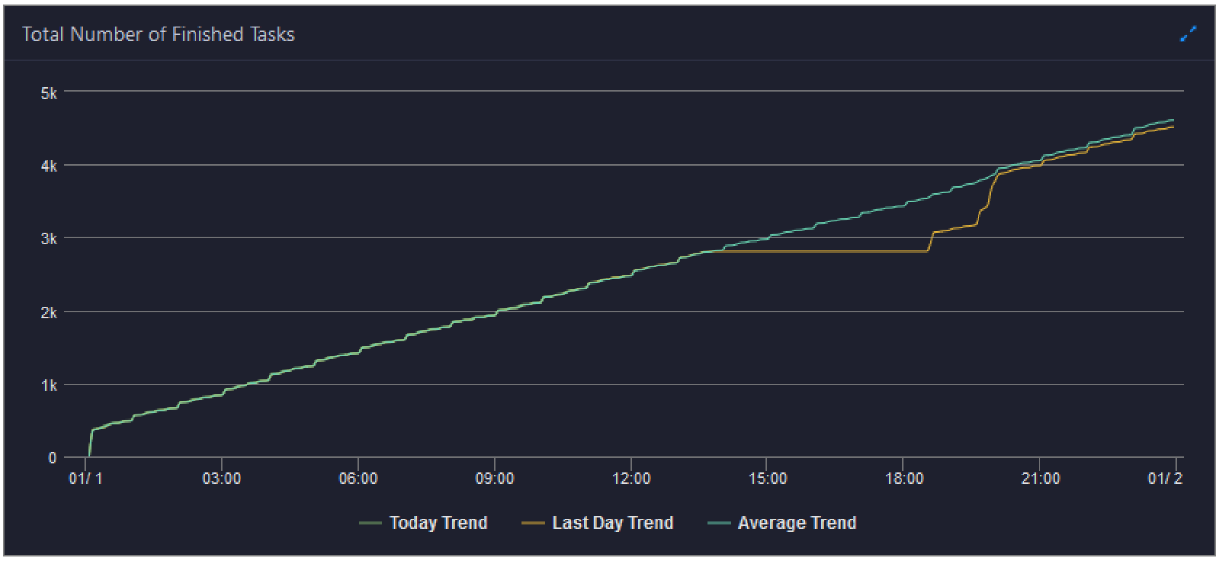
23.9 %

Total Slots	Used	Unavailable	Idle
908	8	209	691

Note Slots are resources that can be used by DataWorks for instance scheduling.

Total Number of Finished Tasks

This section displays the trend chart of the total number of finished nodes. The trend chart displays the trend lines of the number of nodes finished yesterday, the number of nodes finished today, and the average number of nodes finished each day over time in different colors.

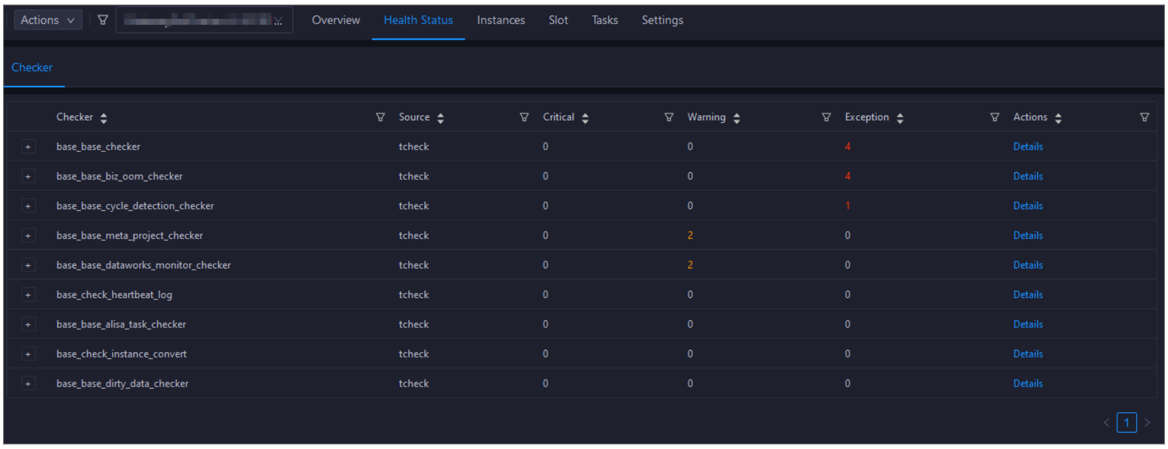


11.3.2.3.1.2. Service health

On the Health Status page for DataWorks, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Entry

1. Log on to the ABM console.
2. Click ▦ in the upper-left corner, and then click **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** page under the **Data Warehouse** page appears.
4. Select a cluster from the drop-down list, and then click the **Health Status** tab. The **Health Status** page appears.



	Checker	Source	Critical	Warning	Exception	Actions
+	base_base_checker	tcheck	0	0	4	Details
+	base_base_biz_oom_checker	tcheck	0	0	4	Details
+	base_base_cycle_detection_checker	tcheck	0	0	1	Details
+	base_base_meta_project_checker	tcheck	0	2	0	Details
+	base_base_dataworks_monitor_checker	tcheck	0	2	0	Details
+	base_check_heartbeat_log	tcheck	0	0	0	Details
+	base_base_alisa_task_checker	tcheck	0	0	0	Details
+	base_check_instance_convert	tcheck	0	0	0	Details
+	base_base_dirty_data_checker	tcheck	0	0	0	Details

The **Health Status** page displays all checkers of the cluster and the check results for the hosts in the cluster. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

Supported operations

On the **Health Status** page, you can view checker details, hosts with alerts, and alert causes. You can also log on to hosts with alerts, clear alerts, and run checkers again. For more information, see Cluster health.

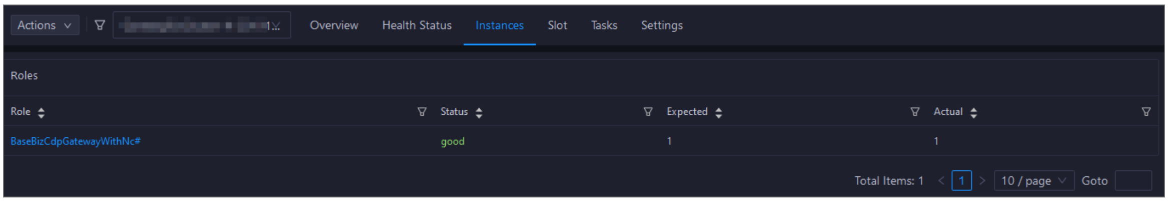
11.3.2.3.1.3. Service instances

The Instances page displays information about all DataWorks service roles, including the name, status, and expected and actual numbers of hosts in the desired state.

Go to the Instances page under Services

1. Log on to the ABM console.
2. Click ▦ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** tab under the **Data Warehouse** page appears.

4. Select a cluster from the drop-down list, and click the **Instances** tab. The **Instances** page appears.



Roles

Role	Status	Expected	Actual
BaseBizCdpGatewayWithNc#	good	1	1

Total Items: 1 < 1 > 10 / page Goto

The **Instances** page displays information about all DataWorks service roles, including the status and the expected and actual numbers of hosts in the desired state. The statuses include **good**, **bad**, and **upgrading**.

Supported operations

You can filter or sort service roles based on a column to facilitate information retrieval on the **Instances** page.

11.3.2.3.1.4. Service slots

Slots are resources used to process tasks. Apsara Big Data Manager (ABM) allows you to view the slot information of DataWorks clusters, resource groups, and hosts. The information includes the maximum number of slots, the number of used slots, and slot usage. You can also migrate resource groups, modify the number of slots for resource groups or hosts, and modify the host status.

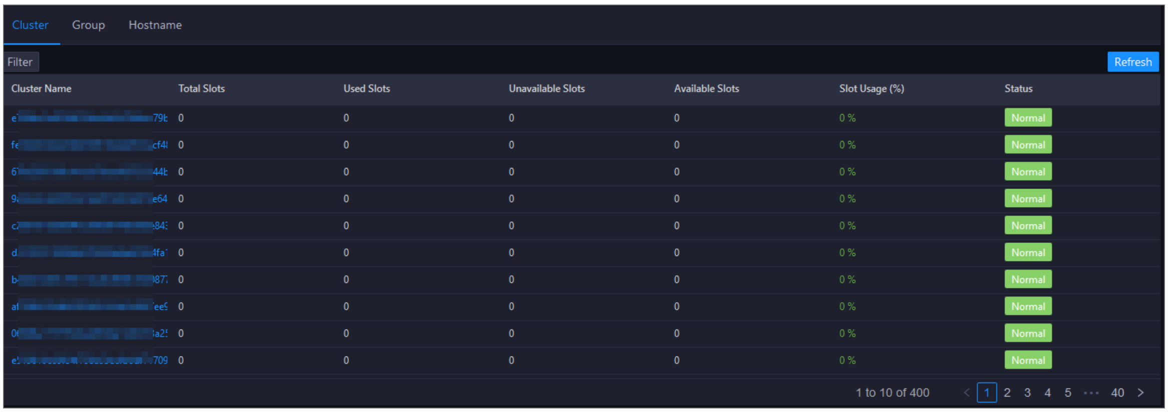
Terms

A data migration unit (DMU) represents the minimum operating capability required by a Data Integration task. This capability indicates the data synchronization processing capability in the case of limited CPU, memory, and network resources.

Resources measured by DMU are allocated by slot. Each DMU occupies two slots.

Entry

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** page appears.
4. Select a cluster from the drop-down list and click the **Slot** tab.



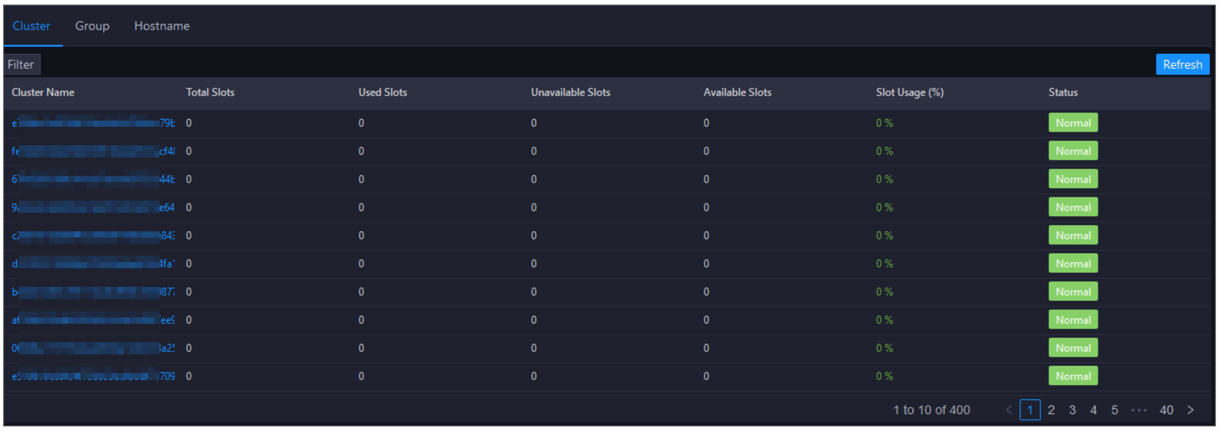
Cluster Name	Total Slots	Used Slots	Unavailable Slots	Available Slots	Slot Usage (%)	Status
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal

1 to 10 of 400 < 1 2 3 4 5 ··· 40 >

Cluster slots

Click the **Cluster** tab on the **Slot** tab.

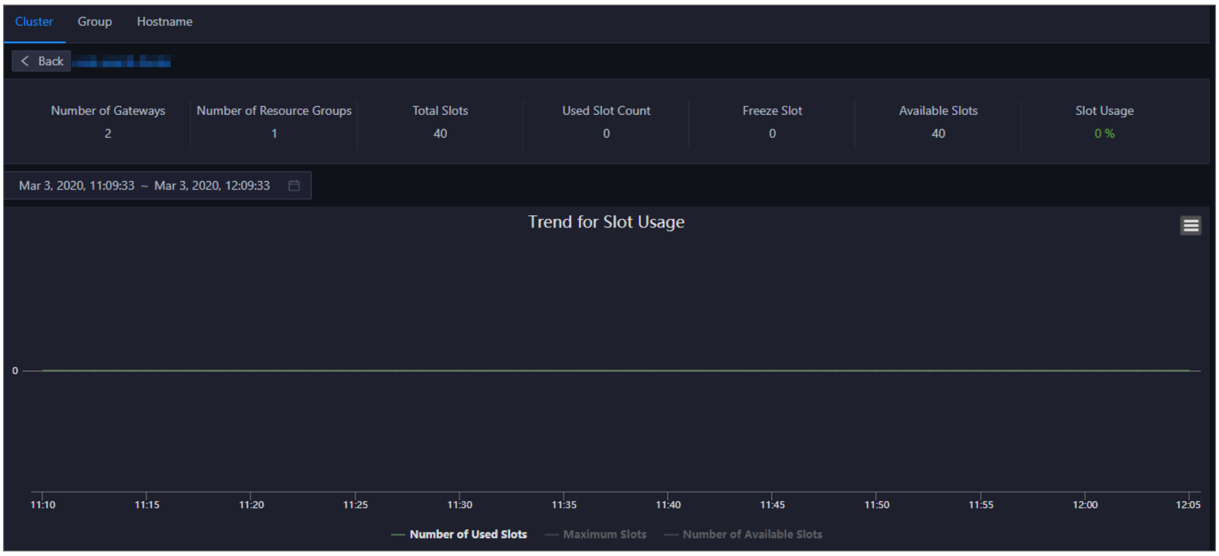
The **Cluster** tab displays the slot overview of all DataWorks clusters, including the total number of slots, the numbers of used slots and available slots, and slot usage. It also displays the cluster running status.



Cluster Name	Total Slots	Used Slots	Unavailable Slots	Available Slots	Slot Usage (%)	Status
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal
[redacted]	0	0	0	0	0 %	Normal

1 to 10 of 400

To view more information about the slots of a specified cluster, click the name of the cluster in the **Cluster Name** column.



[redacted]

Number of Gateways	Number of Resource Groups	Total Slots	Used Slot Count	Freeze Slot	Available Slots	Slot Usage
2	1	40	0	0	40	0 %

Mar 3, 2020, 11:09:33 ~ Mar 3, 2020, 12:09:33

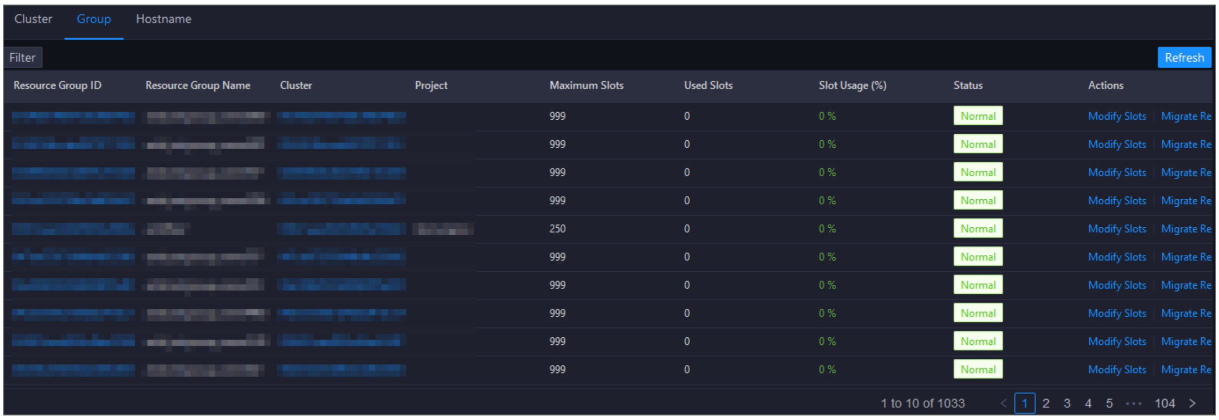
In the upper part of the page that appears, you can view the numbers of gateways, resource groups, slots, used slots, frozen slots, and available slots, and the slot usage of the cluster. You can also view the trend chart of slot usage over time in the lower part of the page. The trend chart displays trend lines for the number of used slots, the maximum number of slots, and the number of available slots in different colors.

You can click the name of a metric under the chart to determine whether to display the related trend line in the chart. A highlighted metric name indicates that the related trend line is displayed, whereas a dimmed metric name indicates that the related trend line is not displayed.

Resource group slots

Click the **Group** tab on the **Slot** tab.

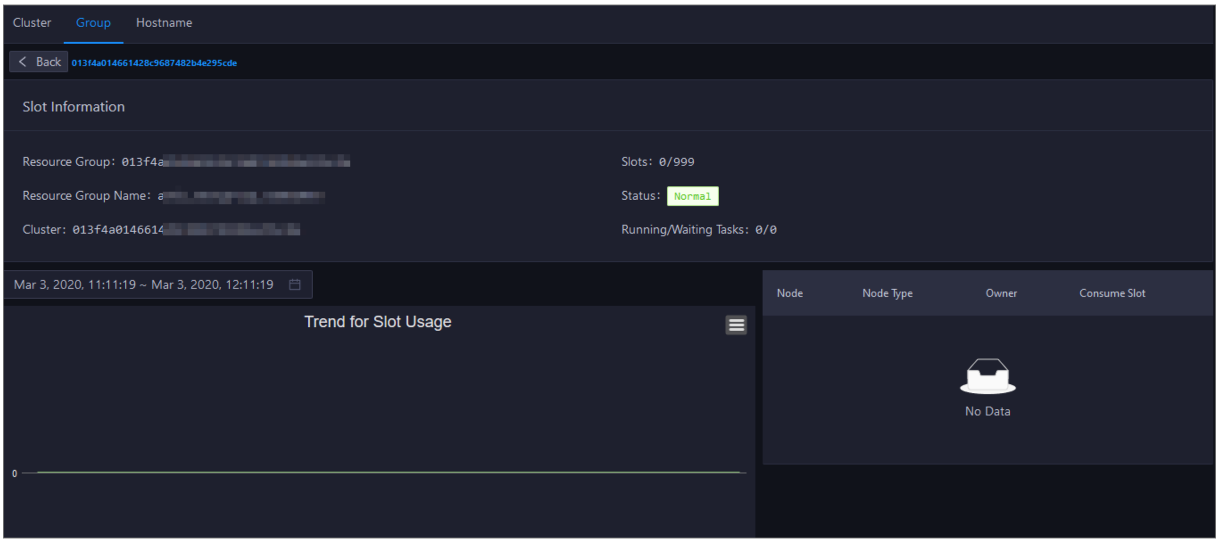
The **Group** tab displays the slot overview of all DataWorks resource groups, including the maximum number of slots, the numbers of used slots and available slots, and slot usage. The tab also displays the name, cluster, project, and running status of each resource group.



Resource Group ID	Resource Group Name	Cluster	Project	Maximum Slots	Used Slots	Slot Usage (%)	Status	Actions
[redacted]	[redacted]	[redacted]		999	0	0 %	Normal	Modify Slots | Migrate Re
[redacted]	[redacted]	[redacted]		999	0	0 %	Normal	Modify Slots | Migrate Re
[redacted]	[redacted]	[redacted]		999	0	0 %	Normal	Modify Slots | Migrate Re
[redacted]	[redacted]	[redacted]		999	0	0 %	Normal	Modify Slots | Migrate Re
[redacted]	[redacted]	[redacted]	[redacted]	250	0	0 %	Normal	Modify Slots | Migrate Re
[redacted]	[redacted]	[redacted]		999	0	0 %	Normal	Modify Slots | Migrate Re
[redacted]	[redacted]	[redacted]		999	0	0 %	Normal	Modify Slots | Migrate Re
[redacted]	[redacted]	[redacted]		999	0	0 %	Normal	Modify Slots | Migrate Re
[redacted]	[redacted]	[redacted]		999	0	0 %	Normal	Modify Slots | Migrate Re
[redacted]	[redacted]	[redacted]		999	0	0 %	Normal	Modify Slots | Migrate Re

1 to 10 of 1033 < 1 2 3 4 5 ··· 104 >

To view more information about slots of a specified resource group, click the ID of the resource group in the **Resource Group ID** column.



Slot Information

Resource Group: 013f4a[redacted]
Resource Group Name: a[redacted]
Cluster: 013f4a0146614[redacted]
Slots: 0/999
Status: Normal
Running/Waiting Tasks: 0/0

Mar 3, 2020, 11:11:19 ~ Mar 3, 2020, 12:11:19

Node	Node Type	Owner	Consume Slot

In the upper part of the page that appears, you can view the current slot information of the resource group, such as the number of used slots and the maximum number of slots. You can also view the trend chart of slot usage over time, the nodes that occupy the slots, and the owners in the lower part. The trend chart displays trend lines for the number of used slots, the maximum number of slots, and the number of available slots in different colors.

You can click the name of a metric under the chart to determine whether to display the related trend line in the chart. A highlighted metric name indicates that the related trend line is displayed, whereas a dimmed metric name indicates that the related trend line is not displayed.

Change the number of slots for a resource group

If the number of slots for a resource group is insufficient or excessive, you can change the number of slots to add or remove resources for the resource group.

1. On the **Group** tab, find the resource group for which you want to change the number of slots, and click **Change Maximum Slots** in the Actions column.
2. In the dialog box that appears, change the value of **Maximum Slots**.
3. Click **Run**. A message appears, indicating that the action is submitted.

Migrate a resource group

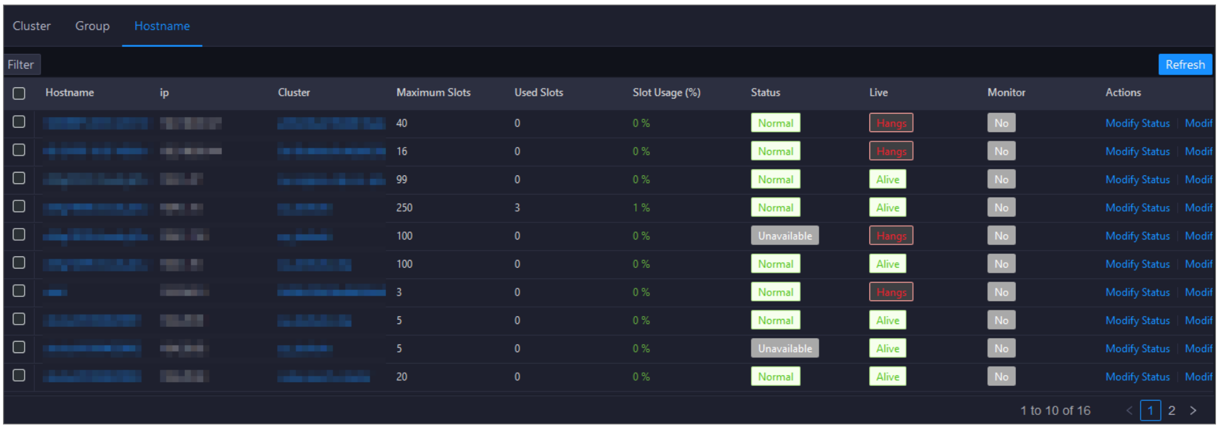
If the slots in a cluster that is associated with a resource group are insufficient and slots cannot be added for the cluster, you can associate the resource group with another cluster.

1. On the **Group** tab, find the resource group that you want to manage. Then, move the pointer over Change Maximum Slots in the Actions column and click **Bind Resource Group**.
2. In the dialog box that appears, change the value of **Target Cluster**.
3. Click **Run**. A message appears, indicating that the action is submitted.

Host slots

Click the **Hostname** tab on the **Slot** tab.

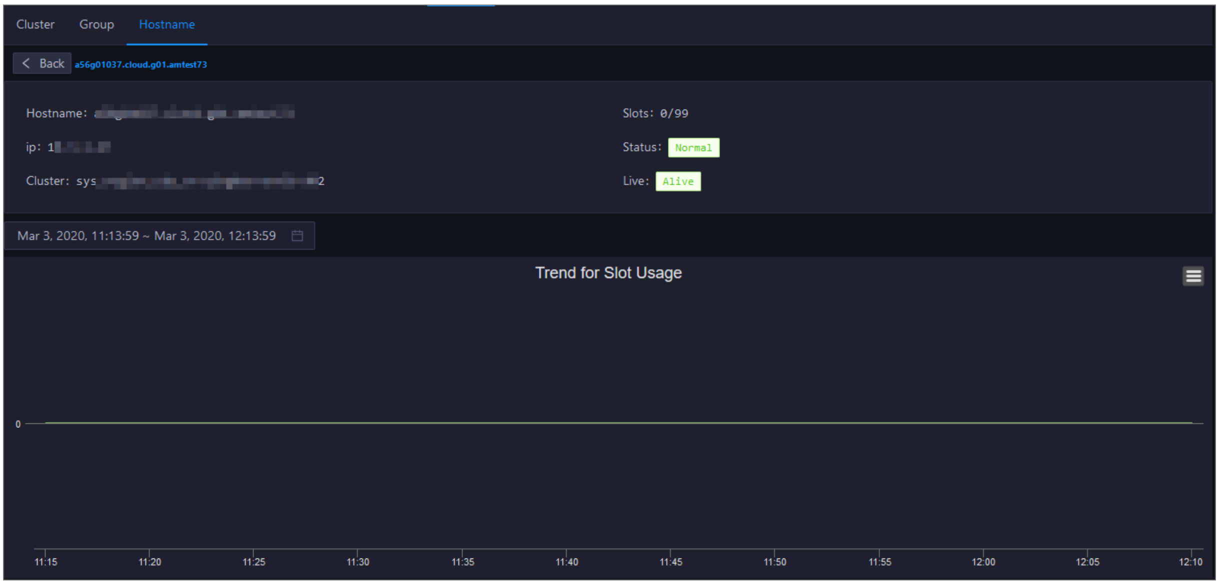
The **Hostname** tab displays the slot overview of all DataWorks hosts, including the maximum number of slots, the number of used slots, and the slot usage. The tab also displays the IP address, cluster, running status, activeness, and monitoring status of each host.



□	Hostname	ip	Cluster	Maximum Slots	Used Slots	Slot Usage (%)	Status	Live	Monitor	Actions
□	[redacted]	[redacted]	[redacted]	40	0	0 %	Normal	Hangs	No	Modify Status Modif
□	[redacted]	[redacted]	[redacted]	16	0	0 %	Normal	Hangs	No	Modify Status Modif
□	[redacted]	[redacted]	[redacted]	99	0	0 %	Normal	Alive	No	Modify Status Modif
□	[redacted]	[redacted]	[redacted]	250	3	1 %	Normal	Alive	No	Modify Status Modif
□	[redacted]	[redacted]	[redacted]	100	0	0 %	Unavailable	Hangs	No	Modify Status Modif
□	[redacted]	[redacted]	[redacted]	100	0	0 %	Normal	Alive	No	Modify Status Modif
□	[redacted]	[redacted]	[redacted]	3	0	0 %	Normal	Hangs	No	Modify Status Modif
□	[redacted]	[redacted]	[redacted]	5	0	0 %	Normal	Alive	No	Modify Status Modif
□	[redacted]	[redacted]	[redacted]	5	0	0 %	Unavailable	Alive	No	Modify Status Modif
□	[redacted]	[redacted]	[redacted]	20	0	0 %	Normal	Alive	No	Modify Status Modif

1 to 10 of 16 ‹ 1 2 ›

To view more information about the slots of a specified host, click the name of the host in the **Hostname** column.



Hostname: [redacted]

ip: 1[redacted]

Cluster: sys[redacted]2

Slots: 0/99

Status: Normal

Live: Alive

Mar 3, 2020, 11:13:59 ~ Mar 3, 2020, 12:13:59

In the upper part of the host details page, you can view the current slot information of the host, such as the number of used slots and the maximum number of slots. You can also view the trend chart of slot usage over time in the lower part of the page. The trend chart displays trend lines for the number of used slots, the maximum number of slots, and the number of available slots in different colors.

You can click the name of a metric under the chart to determine whether to display the related trend line in the chart. A highlighted metric name indicates that the related trend line is displayed, whereas a dimmed metric name indicates that the related trend line is not displayed.

Modify the host status

A host can be in the normal, unavailable, or suspended state. You can modify the host status based on your business requirements.

1. On the **Hostname** tab, find the host whose status you want to modify and click **Change Status** in the Actions column.
2. In the dialog box that appears, set **Status**.
3. Click **Run**. A message appears, indicating that the action is submitted.

Change the number of slots for a host

If the number of slots for a host is insufficient or excessive, you can change the number of slots to add or remove resources for the host.

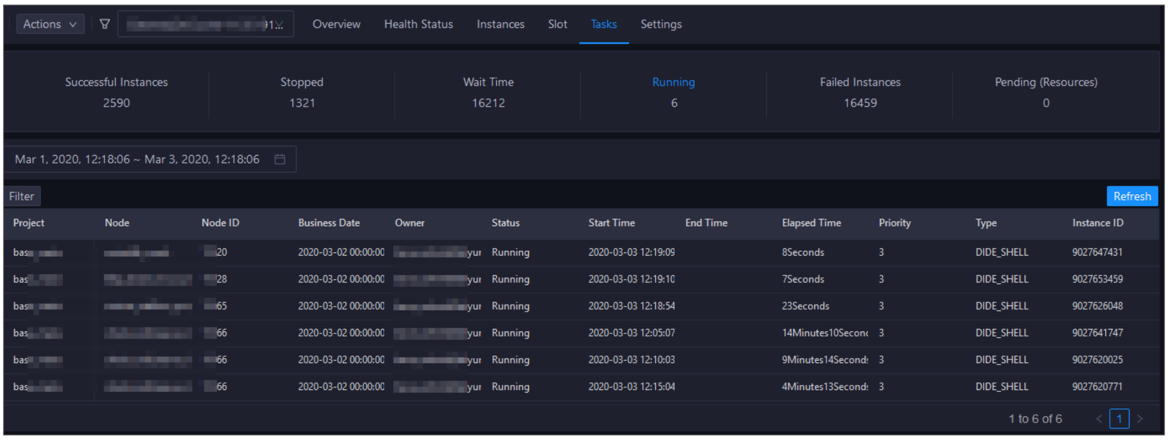
1. On the **Hostname** tab, find the host that you want to manage and click **Change Maximum Slots** in the Actions column.
2. In the dialog box that appears, change the value of **Maximum Slots**.
3. Click **Run**. A message appears, indicating that the action is submitted.

11.3.2.3.1.5. Service nodes

The Tasks page displays nodes created by users in DataWorks. You can filter or sort nodes based on a column to facilitate information retrieval.

Go to the Tasks page under Services

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** tab under the **Data Warehouse** page appears.
4. Select a cluster from the drop-down list, and click the **Tasks** tab. The **Tasks** page appears.



Successful Instances	Stopped	Wait Time	Running	Failed Instances	Pending (Resources)
2590	1321	16212	6	16459	0

Mar 1, 2020, 12:18:06 ~ Mar 3, 2020, 12:18:06

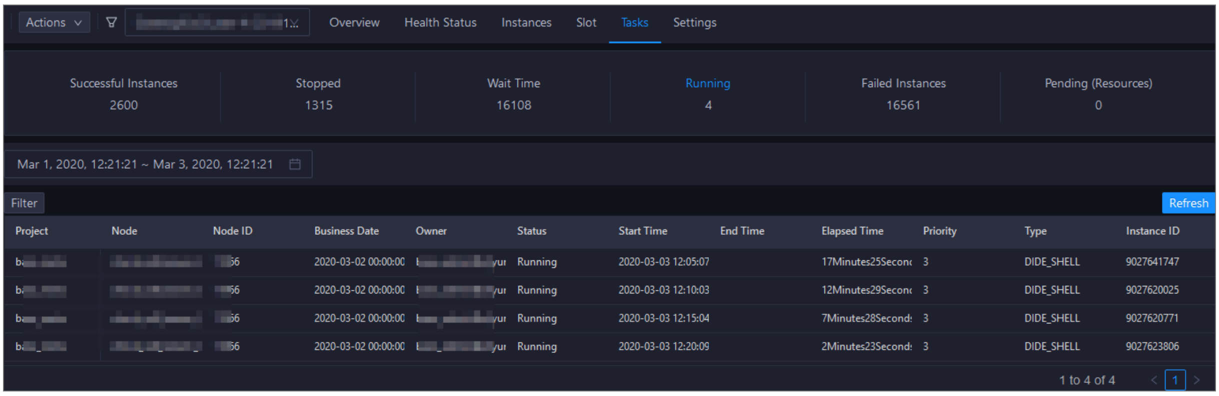
Project	Node	Node ID	Business Date	Owner	Status	Start Time	End Time	Elapsed Time	Priority	Type	Instance ID
bas[redacted]	[redacted]	[redacted]20	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:19:09		8Seconds	3	DIDE_SHELL	9027647431
bas[redacted]	[redacted]	[redacted]28	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:19:10		7Seconds	3	DIDE_SHELL	9027653459
bas[redacted]	[redacted]	[redacted]65	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:18:54		23Seconds	3	DIDE_SHELL	9027626048
bas[redacted]	[redacted]	[redacted]66	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:05:07		14Minutes10Second	3	DIDE_SHELL	9027641747
bas[redacted]	[redacted]	[redacted]66	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:10:03		9Minutes14Second:	3	DIDE_SHELL	9027620025
bas[redacted]	[redacted]	[redacted]66	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:15:04		4Minutes13Second:	3	DIDE_SHELL	9027620771

1 to 6 of 6

The **Tasks** page displays the node information of the current cluster, including the project name, node name, node ID, data timestamp, owner, running status, start time, end time, running duration, priority, type, and instance ID.

Filter nodes by status

On the **Tasks** page, the respective number of nodes in all statuses is displayed at the top. Click a node state to view corresponding nodes in the list. By default, nodes in the **Running** state appear.



Successful Instances	Stopped	Wait Time	Running	Failed Instances	Pending (Resources)
2600	1315	16108	4	16561	0

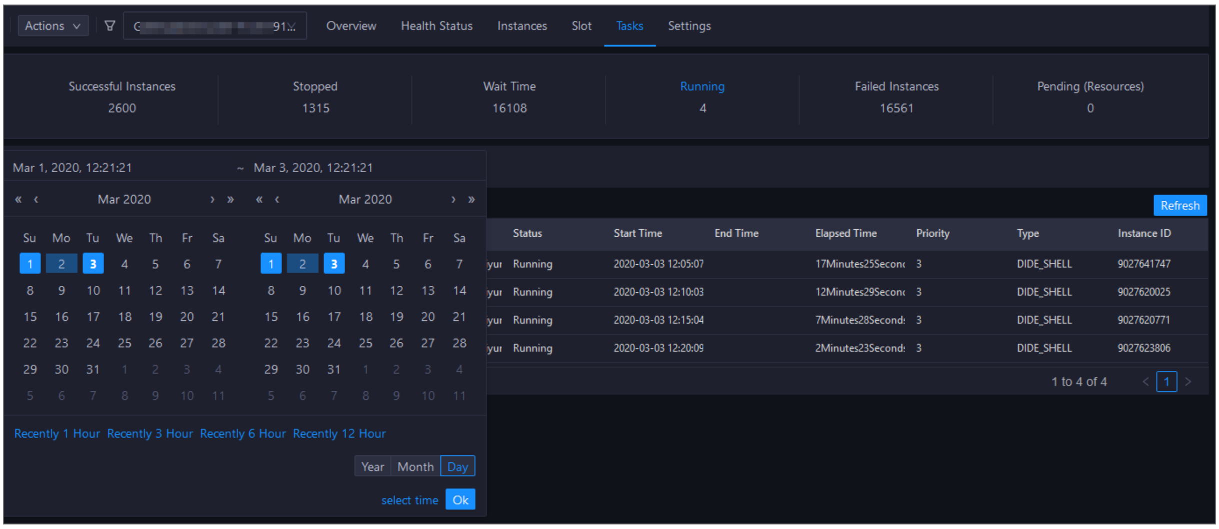
Mar 1, 2020, 12:21:21 ~ Mar 3, 2020, 12:21:21

Project	Node	Node ID	Business Date	Owner	Status	Start Time	End Time	Elapsed Time	Priority	Type	Instance ID
b[redacted]	[redacted]	[redacted]66	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:05:07		17Minutes25Second	3	DIDE_SHELL	9027641747
b[redacted]	[redacted]	[redacted]66	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:10:03		12Minutes29Second	3	DIDE_SHELL	9027620025
b[redacted]	[redacted]	[redacted]66	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:15:04		7Minutes28Second:	3	DIDE_SHELL	9027620771
b[redacted]	[redacted]	[redacted]66	2020-03-02 00:00:00	[redacted]yur	Running	2020-03-03 12:20:09		2Minutes23Second:	3	DIDE_SHELL	9027623806

1 to 4 of 4

Filter nodes by time

Select a time period, including both the date and time, in the upper-left corner of the node list to view the nodes in the corresponding time period.



Successful Instances	Stopped	Wait Time	Running	Failed Instances	Pending (Resources)
2600	1315	16108	4	16561	0

Mar 1, 2020, 12:21:21 ~ Mar 3, 2020, 12:21:21

	Status	Start Time	End Time	Elapsed Time	Priority	Type	Instance ID
yur	Running	2020-03-03 12:05:07		17Minutes25Second	3	DIDE_SHELL	9027641747
yur	Running	2020-03-03 12:10:03		12Minutes29Second	3	DIDE_SHELL	9027620025
yur	Running	2020-03-03 12:15:04		7Minutes28Second:	3	DIDE_SHELL	9027620771
yur	Running	2020-03-03 12:20:09		2Minutes23Second:	3	DIDE_SHELL	9027623806

1 to 4 of 4

Other operations

You can filter nodes, sort nodes based on a column, and customize columns on the Tasks page.

11.3.2.3.1.6. Service settings

The Settings page allows you to change the values of configuration items for various service roles in DataWorks.

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner, and then click **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** page under the **Data Warehouse** page appears.
4. Select a cluster from the drop-down list, and then click the **Settings** tab. The **Settings** page appears.

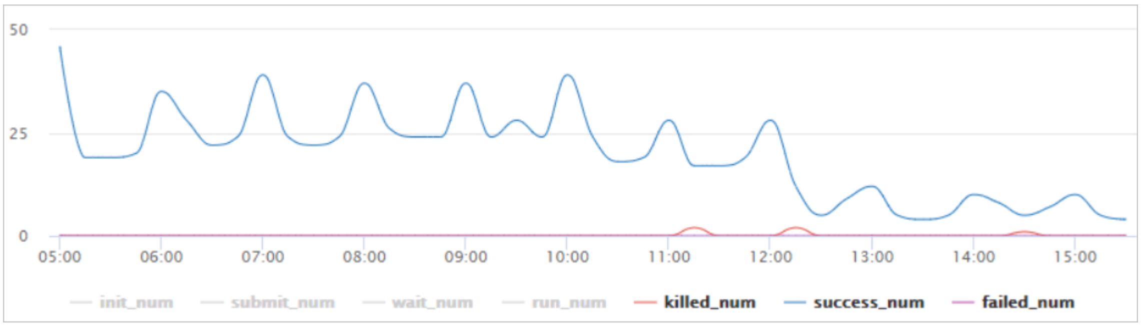
11.3.2.3.2. Data Integration

11.3.2.3.2.1. Data integration overview

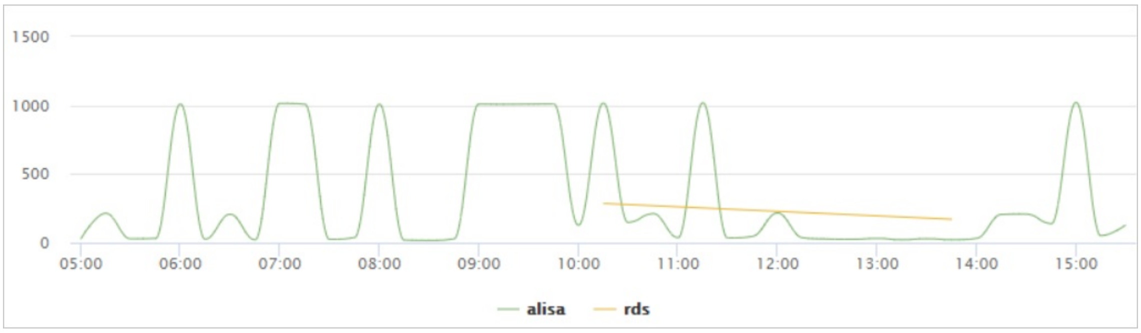
The Overview page of Data Integration displays information in the Task Scheduling Overview, Today's Tasks, Third-party Dependencies - Response Time (milliseconds), Third-party Dependencies - Total Requests, and Third-party Dependencies - Request Error Rate sections.

Procedure

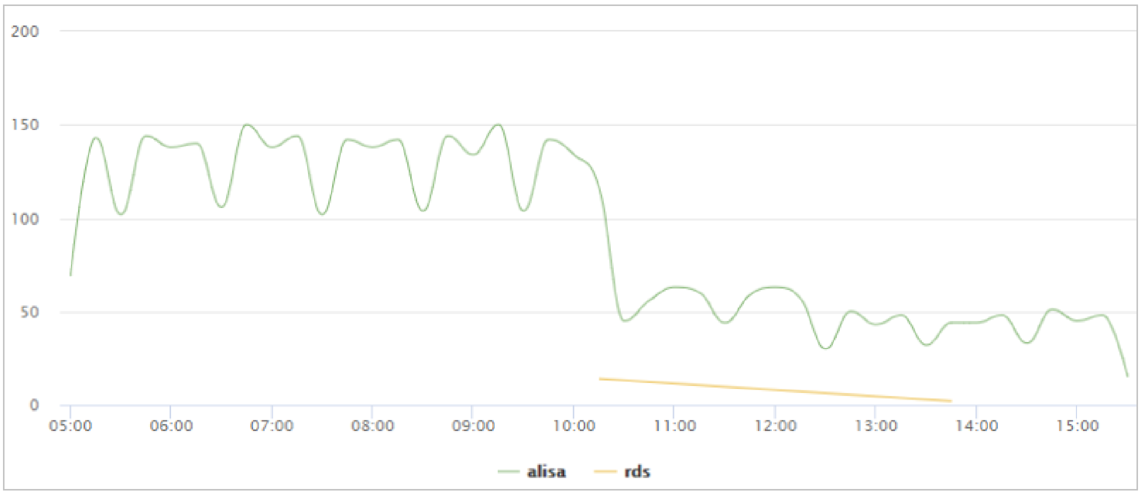
1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** tab under the **Data Warehouse** page appears.
4. In the left-side navigation pane, click **Data Integration**. The **Overview** page appears.After you set the **Aggregation Period** parameter and select a time period, you can view the desired information in the following sections:
    - **Task Scheduling Overview**
    - **Today's Tasks**



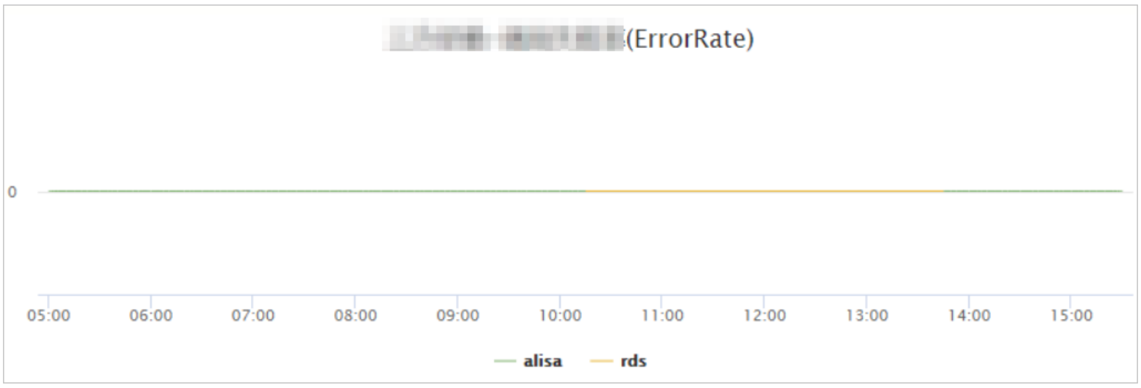
    - **Third-party Dependencies - Response Time (milliseconds)**



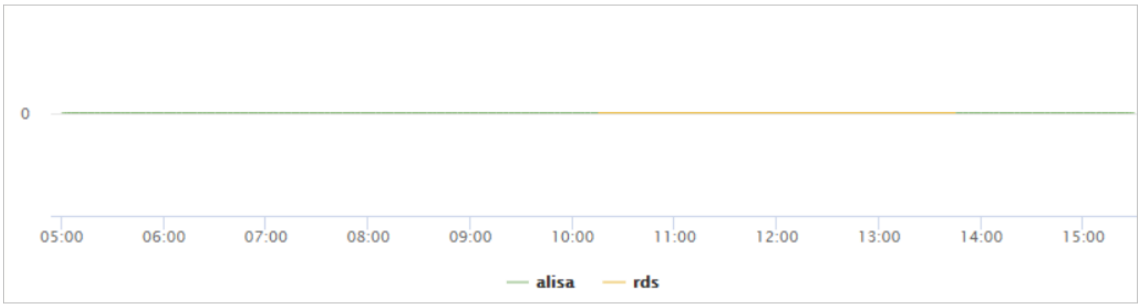
- Third-party Dependencies - Total Requests



- Third-party Dependencies - Request Error Rate



- Third-party Dependencies - Failed Requests



11.3.2.3.2.2. View Data Integration nodes

This topic describes how to view node information on the Tasks page of Data Integration, and obtain the required data such as the amount of synchronized data, synchronization speed, and node data volume.

Go to the Tasks page

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** tab under the **Data Warehouse** page appears.
4. In the left-side navigation pane, click **Data Integration**. The **Overview** page appears.
5. Click the **Tasks** tab. The **Instances** tab appears by default.

View instance information

On the **Instances** tab, you can filter instances by **Project Name**, **Resource Group**, **Host**, **Status**, **Read Plug-in Type**, **Write Plug-in Type**, and **Data Source**. If you need to customize more filter criteria, click **Advanced Search**.

You can also click the request ID, synchronization script number, or resource group name to view the corresponding details.

- After you click the request ID, you can view the event type, IP address from which the request is submitted, and start time of the instance.
- After you click the synchronization script number, you can view the following information:
  - On the **Job Statistics by Day** page, you can view the trends of the synchronized data volume, synchronization speed, and consumed time.
  - On the **Job Statistics by Run** page, you can view the trends of the synchronized data volume, synchronization speed, and consumed time.
  - On the **Jobs in the Final Status** page, you can view the trends of successful nodes, failed nodes, and killed nodes.
- After you click the resource group name, you can view the slot usage of the resource group.

After you view the corresponding details, you can click **Back** to return to the **Instances** page under **Task**.

On the Task page, you can also view the number of initialized nodes, submitted nodes, running nodes, failed, nodes, successful nodes, and nodes waiting to be scheduled.

View multi-dimensional analysis information

On the **Multi-dimensional Analysis** tab, you can filter historical analysis information by **Project Name**, **Resource Group**, **Host**, **Status**, **Read Plug-in Type**, **Write Plug-in Type**, or **Data Source** from the perspective of **Sync Data Size**, **Sync Speed**, or **Tasks**.

11.3.2.3.2.3. View historical analysis information

On the Historical Analysis page, you can view information about multi-dimensional analysis, execution time analysis, and nodes rankings.

Go to the Historical Analysis page

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** tab under the **Data Warehouse** page appears.
4. In the left-side navigation pane, click **Data Integration**. The **Overview** page appears.
5. Click the **Historical Analysis** tab. The **Multi-dimensional Analysis** page appears.

View multi-dimensional analysis information

On the **Multi-dimensional Analysis** tab, you can filter historical analysis information by **Project Name**, **Resource Group**, **Host**, **Status**, **Read Plug-in Type**, **Write Plug-in Type**, or **Data Source** from the perspective of **Sync Data Size**, **Sync Speed**, **Time**, or **Tasks**.

View execution time analysis information

On the **Execution Time Analysis** tab, you can filter required execution time information by **Project Name**, **Resource Group**, **Host**, **Status**, **Read Plug-in Type**, **Write Plug-in Type**, or **Data Source**.

View top 10 nodes

On the **Task Rankings** tab, you can filter top 10 nodes by **Project Name**, **Resource Group**, **Host**, **Status**, **Read Plug-in Type**, **Write Plug-in Type**, or **Data Source**.

11.3.2.3.3. Cluster scaling

Apsara Big Data Manager (ABM) supports DataWorks cluster scaling. To scale out a DataWorks cluster, add physical hosts in the default cluster of Apsara Infrastructure Management Framework to the DataWorks cluster. To scale in a DataWorks cluster, remove physical hosts from the DataWorks cluster to the default cluster of Apsara Infrastructure Management Framework.

Background information

In Apsara Stack, scaling out a cluster involves complex operations. You must configure new physical hosts on Deployment Planner so that they can be added to the default cluster of Apsara Infrastructure Management Framework. The default cluster of Apsara Infrastructure Management Framework is considered as a resource pool that can provide resources for scaling out business clusters. To scale out a cluster, add physical hosts in the default cluster of Apsara Infrastructure Management Framework to the cluster. To scale in a cluster, remove physical hosts from the cluster to the default cluster of Apsara Infrastructure Management Framework.

When you scale out a DataWorks cluster, ABM adds physical hosts in the default cluster to the DataWorks cluster. When you scale in a DataWorks cluster, ABM removes physical hosts from the DataWorks cluster to the default cluster. The server roles of physical hosts in DataWorks include **BaseBizCdpGatewayWithNc#** and **BaseBizGatewayWithNc#**. DataWorks cluster scaling supports only the two server roles.

Prerequisites

- Scale-out
  - The physical hosts that you want to add to your DataWorks cluster are in the default cluster of Apsara Infrastructure Management Framework.

- ○ The server role of the template host is **BaseBizCdpGatewayWithNc#** or **BaseBizGatewayWithNc#**.

- Scale-in

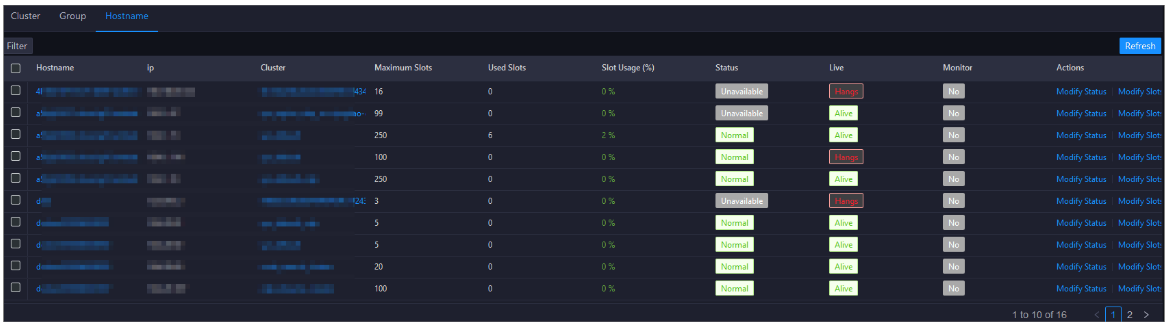
  The server role of the template host is **BaseBizCdpGatewayWithNc#** or **BaseBizGatewayWithNc#**.

> ? **Note** You can go to the **DataWorks** page. Then, click **O&M** in the upper-right corner, and click the **Services** tab. In the left-side navigation pane, click **Data Warehouse**. On the page that appears, click the **Instances** tab. In the server role list, find the server role **BaseBizCdpGatewayWithNc#** or **BaseBizGatewayWithNc#**, and click the server role name to go to the Apsara Infrastructure Management Framework console and view the hosts with the server role **BaseBizCdpGatewayWithNc#** or **BaseBizGatewayWithNc#**.

Scale out a DataWorks cluster

You can add multiple hosts to a DataWorks cluster at a time to scale out the cluster. To achieve this, you must specify an existing host as the template host. During the scale-out, the configurations of the template host are copied to the hosts so that the hosts can be added to the cluster at a time.

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** tab appears.
4. Select a cluster from the drop-down list and click the **Slot** tab.
5. On the **Slot** tab, click the **Hostname** tab. Then, select a physical host whose server role is **BaseBizCdpGatewayWithNc#** or **BaseBizGatewayWithNc#** in the host list as the template host.



☐	Hostname	ip	Cluster	Maximum Slots	Used Slots	Slot Usage (%)	Status	Live	Monitor	Actions
☐	[redacted]	[redacted]	[redacted]	16	0	0 %	Unavailable	Hangs	No	Modify Status | Modify Slots
☐	[redacted]	[redacted]	[redacted]	99	0	0 %	Unavailable	Alive	No	Modify Status | Modify Slots
☐	[redacted]	[redacted]	[redacted]	250	6	2 %	Normal	Alive	No	Modify Status | Modify Slots
☐	[redacted]	[redacted]	[redacted]	100	0	0 %	Normal	Hangs	No	Modify Status | Modify Slots
☐	[redacted]	[redacted]	[redacted]	250	0	0 %	Normal	Alive	No	Modify Status | Modify Slots
☐	[redacted]	[redacted]	[redacted]	3	0	0 %	Unavailable	Hangs	No	Modify Status | Modify Slots
☐	[redacted]	[redacted]	[redacted]	5	0	0 %	Normal	Alive	No	Modify Status | Modify Slots
☐	[redacted]	[redacted]	[redacted]	5	0	0 %	Normal	Alive	No	Modify Status | Modify Slots
☐	[redacted]	[redacted]	[redacted]	20	0	0 %	Normal	Alive	No	Modify Status | Modify Slots
☐	[redacted]	[redacted]	[redacted]	100	0	0 %	Normal	Alive	No	Modify Status | Modify Slots

1 to 10 of 16 < 1 2 >

6. Move the pointer over **Actions** in the upper-right corner and click **Scale-up for Normal Hosts**. In the **Scale-up for Normal Hosts** panel, configure the parameters

   Parameters:

   - ○ **Refer Hostname**: the name of the template host. By default, the name of the selected host is used.
   - ○ **Hostname**: the name of the host that you want to add to the DataWorks cluster. Enter the name of an available host in the default cluster for scale-out. If you want to add multiple hosts, enter multiple hostnames and separate the hostnames with commas (,).
7. Click **Run**. A message appears, indicating that the action is submitted.
8. View the scale-out status.

Move the pointer over **Actions** in the upper-right corner and click **Execution History** next to **Scale-up for Normal Hosts** to view the scale-out history.

The scale-out may require a long period. In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.

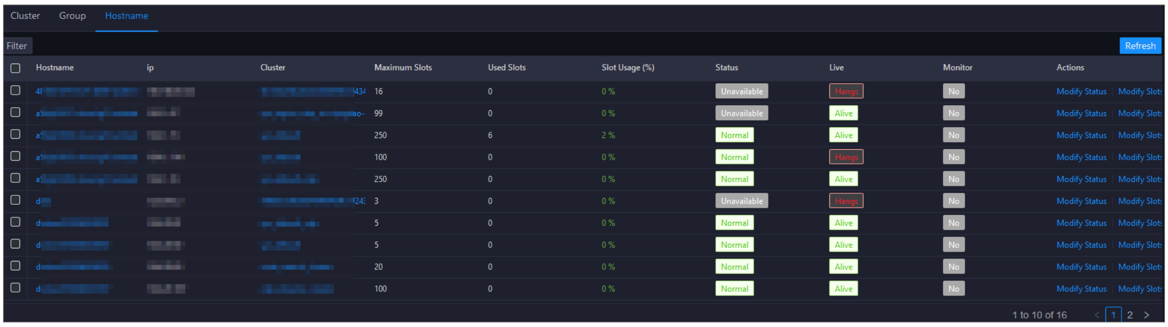
If **RUNNING** is displayed in the Current Status column, you can click **Details** in the Details column to view the steps and progress of the scale-out.

If **FAILED** is displayed in the Current Status column, click **Details** in the Details column to locate the failure cause. For more information, see Locate the cause of a scaling failure.

Scale in a DataWorks cluster

You can remove physical hosts from a DataWorks cluster to the default cluster of Apsara Infrastructure Management Framework to scale in the DataWorks cluster.

1. Log on to the ABM console.
2. Click ▦ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** page appears.
4. Select a cluster from the drop-down list and click the **Slot** tab.
5. On the **Slot** tab, click the **Hostname** tab. Then, select a physical host whose server role is **BaseBizCdpGatewayWithNc#** or **BaseBizGatewayWithNc#** in the host list as the template host.



□	Hostname	ip	Cluster	Maximum Slots	Used Slots	Slot Usage (%)	Status	Live	Monitor	Actions
□	[redacted]	[redacted]	[redacted]	16	0	0 %	Unavailable	Hangs	No	Modify Status | Modify Slots
□	[redacted]	[redacted]	[redacted]	99	0	0 %	Unavailable	Alive	No	Modify Status | Modify Slots
□	[redacted]	[redacted]	[redacted]	250	6	2 %	Normal	Alive	No	Modify Status | Modify Slots
□	[redacted]	[redacted]	[redacted]	100	0	0 %	Normal	Hangs	No	Modify Status | Modify Slots
□	[redacted]	[redacted]	[redacted]	250	0	0 %	Normal	Alive	No	Modify Status | Modify Slots
□	[redacted]	[redacted]	[redacted]	3	0	0 %	Unavailable	Hangs	No	Modify Status | Modify Slots
□	[redacted]	[redacted]	[redacted]	5	0	0 %	Normal	Alive	No	Modify Status | Modify Slots
□	[redacted]	[redacted]	[redacted]	5	0	0 %	Normal	Alive	No	Modify Status | Modify Slots
□	[redacted]	[redacted]	[redacted]	20	0	0 %	Normal	Alive	No	Modify Status | Modify Slots
□	[redacted]	[redacted]	[redacted]	100	0	0 %	Normal	Alive	No	Modify Status | Modify Slots

1 to 10 of 16 < 1 2 >

6. Move the pointer over **Actions** in the upper-right corner and click **Scale-down for Normal Hosts**. In the **Scale-up for Normal Hosts** panel, configure the parameters.

   Parameters:

   - **Hostname**: the name of the host that you want to remove from the DataWorks cluster. By default, the name of the selected host is used.
   - **Biz Name**: the server role of the host that you want to remove from the DataWorks cluster. Select the actual server role from the drop-down list. Valid values: **base-biz-cdpgatewaywithnc#** and **base-biz-gatewaywithnc#**.
7. Click **Run**. A message appears, indicating that the action is submitted.
8. View the scale-in status.

   Move the pointer over **Actions** in the upper-left corner and click **Execution History** next to **Scale-down for Normal Hosts** to view the scale-in history.

The scale-in may require a long period. In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.

If **RUNNING** is displayed in the Current Status column, you can click **Details** in the Details column to view the steps and progress of the scale-in.

If **FAILED** is displayed in the Current Status column, click **Details** in the Details column to locate the failure cause. For more information, see Locate the cause of a scaling failure.

Locate the cause of a scaling failure

The method for locating the cause of a scale-out failure and that of a scale-in failure are similar. This section describes how to locate the cause of a scale-out failure.

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Overview** page appears.
4. Move the pointer over **Actions** in the upper-right corner and click **Execution History** next to **Scale-up for Normal Hosts** to view the scale-out history.
5. In the panel that appears, click **Details** in the Details column of a failed execution to locate the failure cause.

   You can locate the failure cause based on the following information: parameter settings, host details, scripts, and execution parameters.

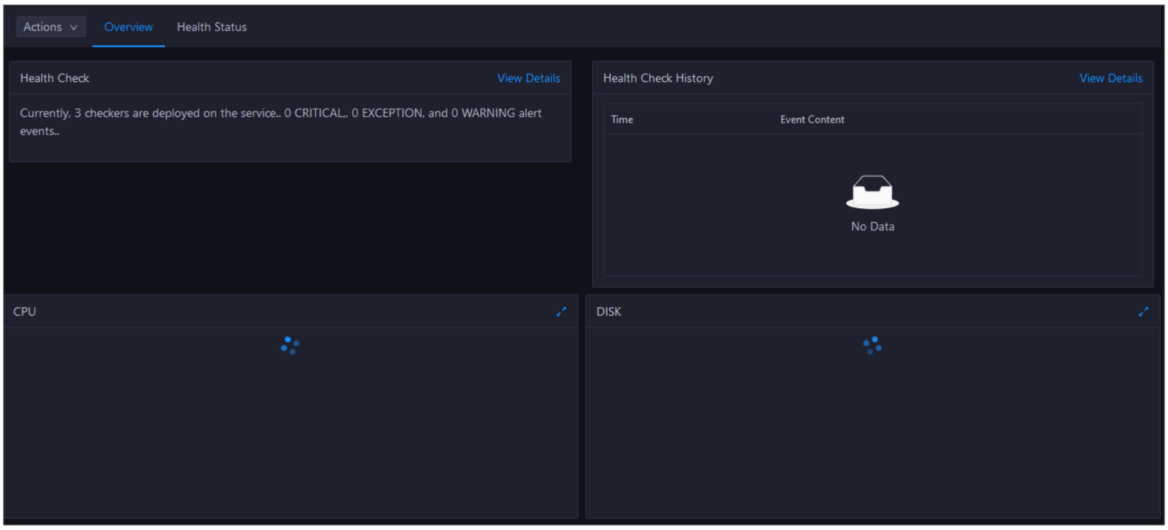
11.3.2.4. Cluster O&M

11.3.2.4.1. Cluster overview

The cluster overview page displays the overall running and health check information about a cluster. On this page, you can view the health check result and health check history of the cluster. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the cluster.

Entry

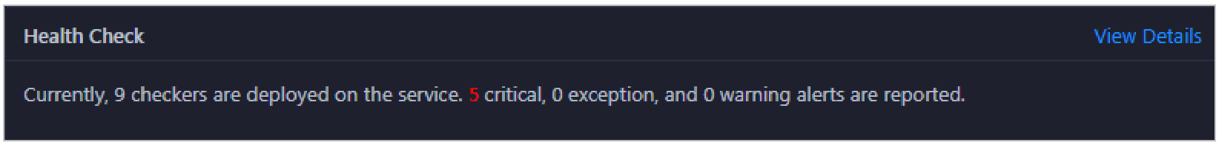
1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner, and then click **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner.
4. Click the **Clusters** tab at the top of the **O&M** page.
5. On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Overview** tab. The **Overview** page appears.



Currently, 3 checkers are deployed on the service.. 0 CRITICAL,, 0 EXCEPTION, and 0 WARNING alert events..

Health Check

This section displays the number of checkers deployed for the cluster and the respective number of Critical, Warning, and Exception alerts.



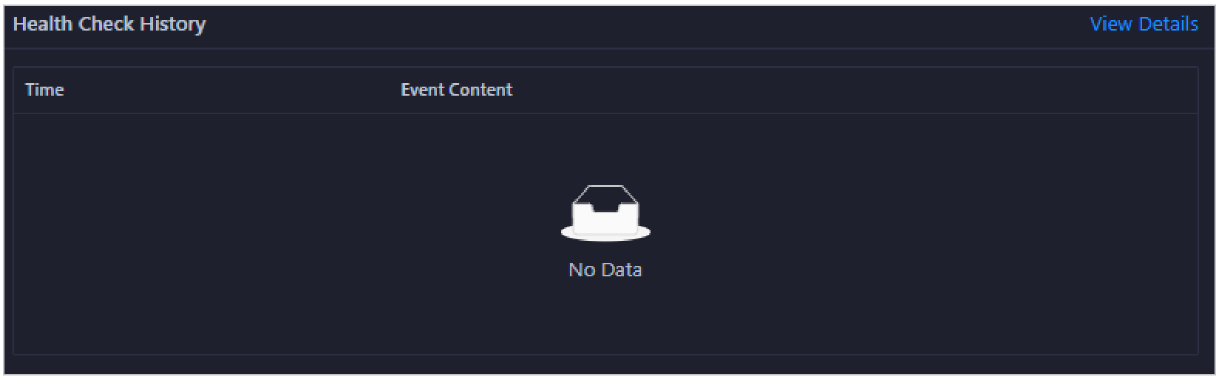
Currently, 9 checkers are deployed on the service. 5 critical, 0 exception, and 0 warning alerts are reported.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Cluster health.

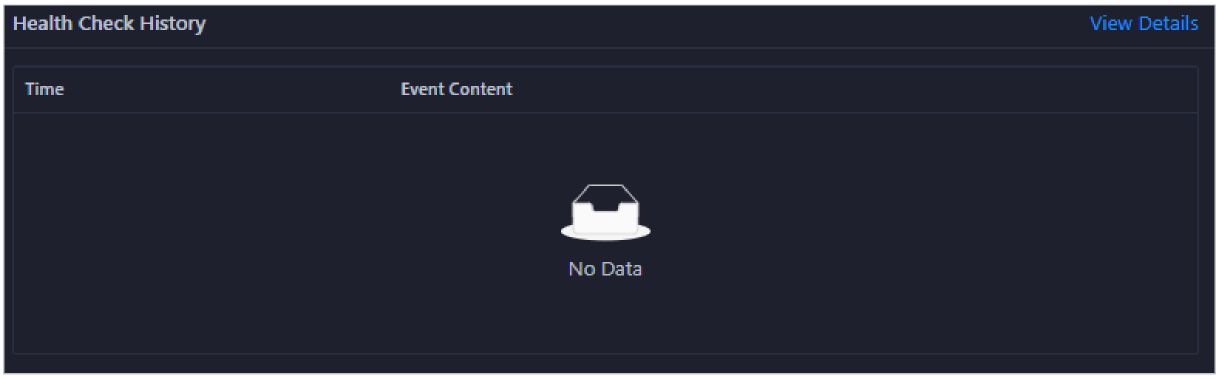
Health Check History

This section displays a record of the health checks performed on the cluster.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Cluster health.



You can click the event content of a check to view the exception items.



Health Check History

View Details

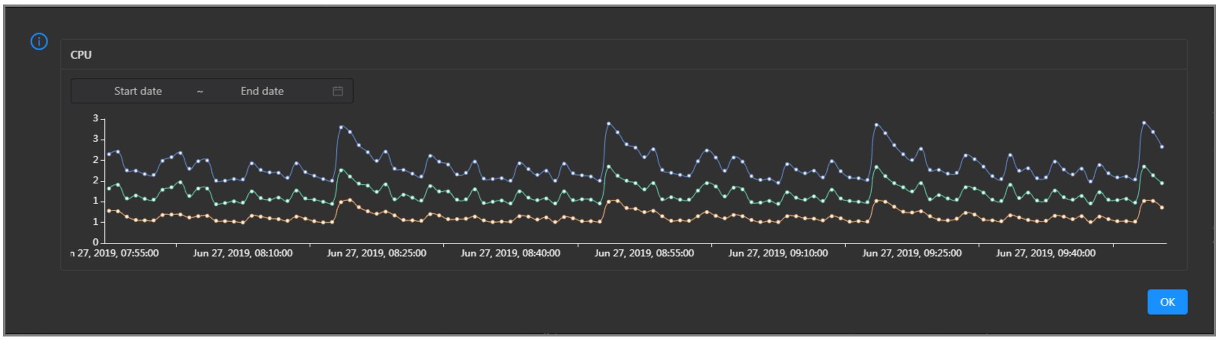
Time	Event Content
No Data	

CPU

This chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

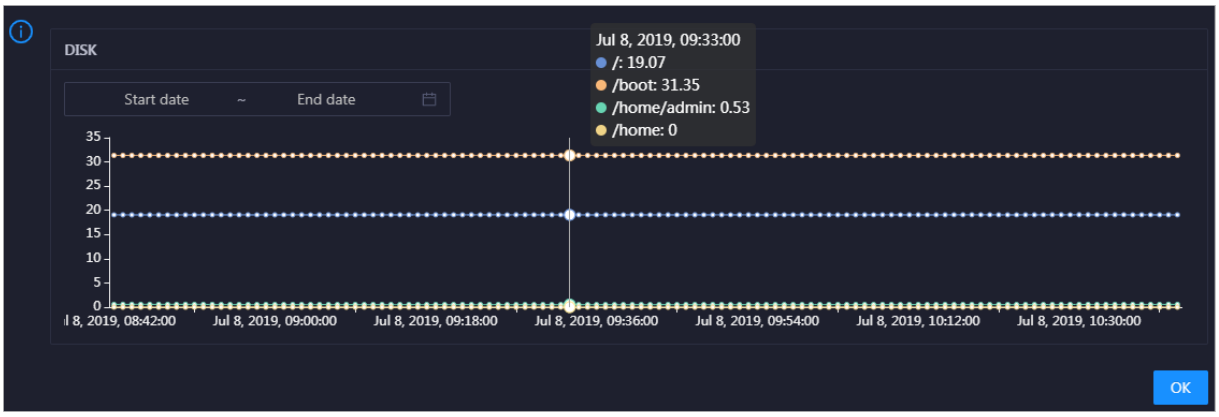
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the cluster in the specified period.



DISK

This chart shows the trend lines of the storage usage on the */*, */boot*, */home/admin*, and */home* directories for the cluster over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

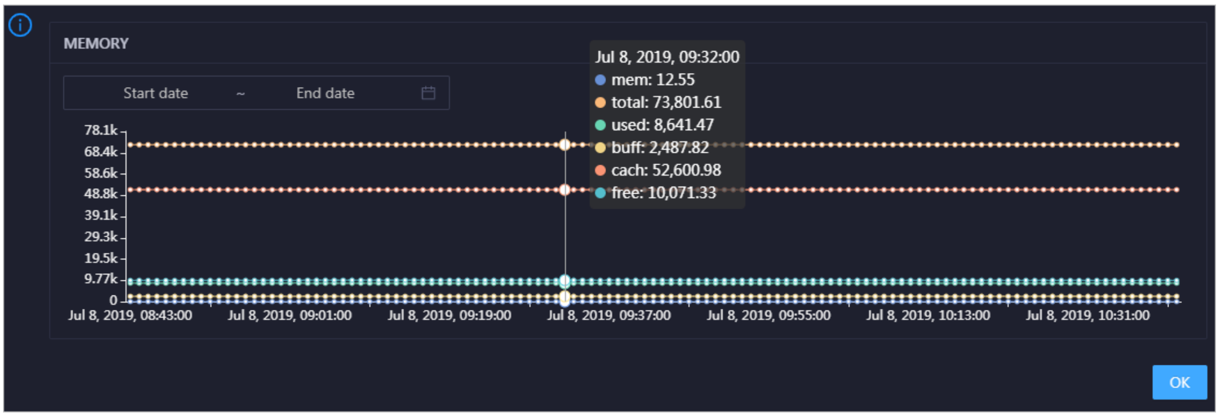


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

MEMORY

This chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

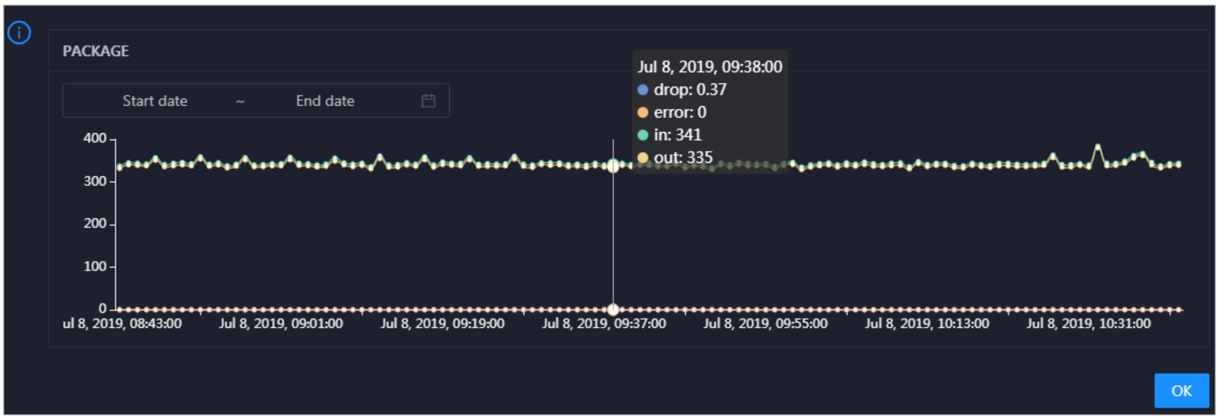


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the cluster in the specified period.

PACKAGE

This chart shows the trend lines of the numbers of dropped packets (drop), error packets (error), received packets (in), and sent packets (out) for the cluster in different colors. These trend lines reflect the data transmission status of the cluster.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

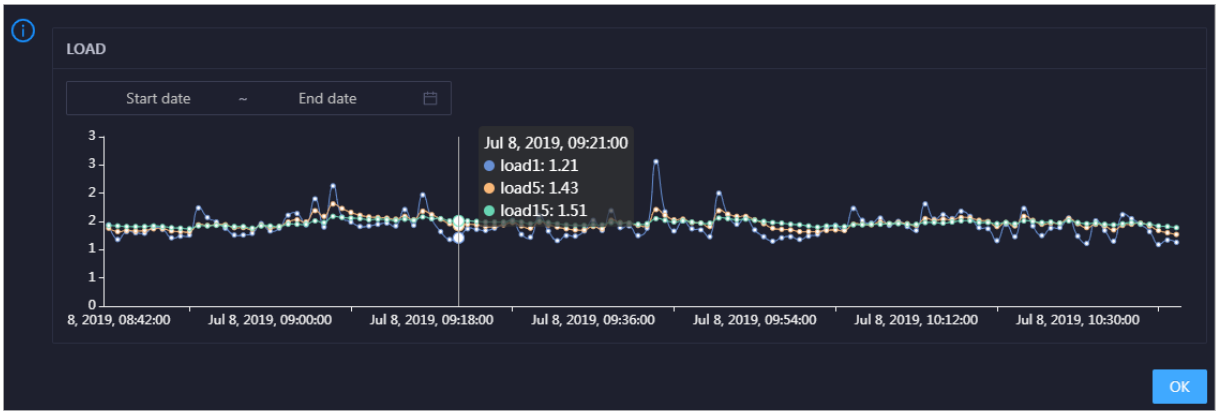


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the cluster in the specified period.

LOAD

This chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



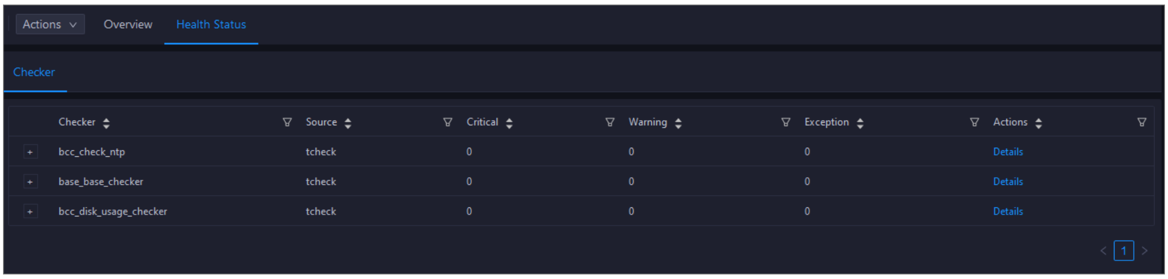
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the cluster in the specified period.

11.3.2.4.2. Cluster health

On the Health Status page, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Go to the Health Status page under Clusters

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner.
4. Click the **Clusters** tab at the top of the **O&M** page.
5. On the **Clusters** page, select a cluster in the left-side navigation pane, and click the **Health Status** tab. The **Health Status** page appears.

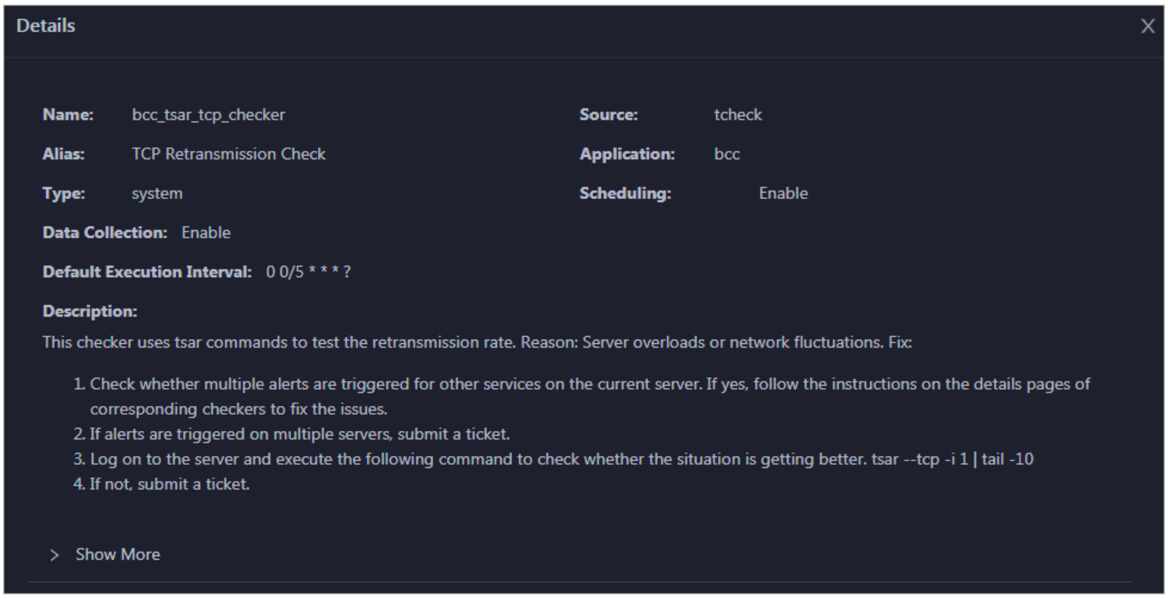


	Checker	Source	Critical	Warning	Exception	Actions
+	bcc_check_ntp	tcheck	0	0	0	Details
+	base_base_checker	tcheck	0	0	0	Details
+	bcc_disk_usage_checker	tcheck	0	0	0	Details

On the **Health Status** tab, you can view all checkers for the cluster and the check results for the hosts in the cluster. The following alerts may be reported on a host: **CRITICAL**, **WARNING**, and **EXCEPTION**. The alerts are represented in different colors. You must handle the alerts in a timely manner, especially the **CRITICAL** and **WARNING** alerts.

View checker details

1. On the Health Status tab, click **Details** in the Actions column of a checker. On the Details page, view checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

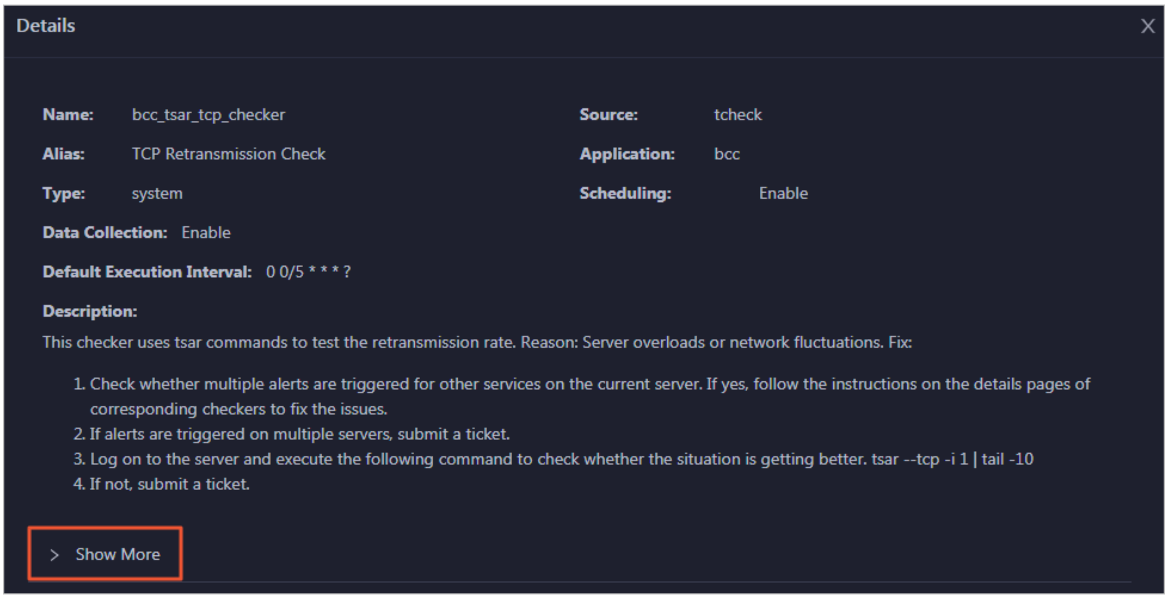
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include **Name**, **Source**, **Alias**, **Application**, **Type**, **Scheduling**, **Data Collection**, **Default Execution Interval**, and **Description**. The schemes to clear alerts are provided in the description.

2. Click **Show More** to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

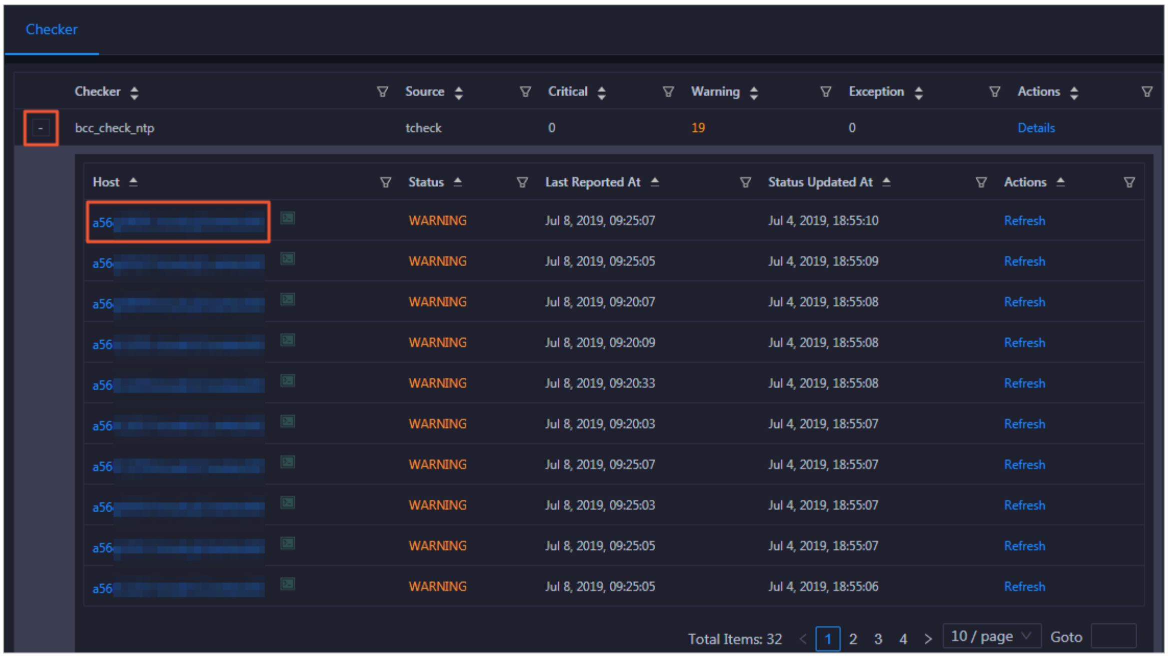
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about **Script**, **Target (TianJi)**, **Default Threshold**, and **Mount Point**.

View the hosts for which alerts are reported and causes for the alerts

You can view the check history and check results of a checker on a host.

1. On the Health Status tab, click **+** to expand a checker for which alerts are reported. You can view all hosts where the checker is run.



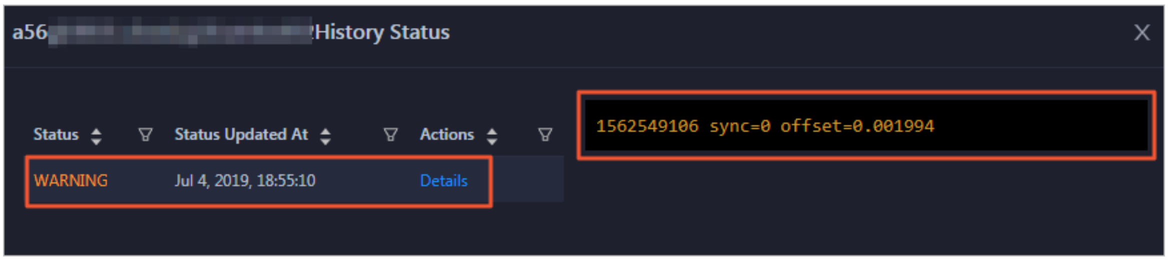
Checker

	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:06	Refresh

Total Items: 32 < 1 2 3 4 > 10 / page Goto

2. Click a hostname. In the panel that appears, click **Details** in the Actions column of a check result to view the cause of the alert.



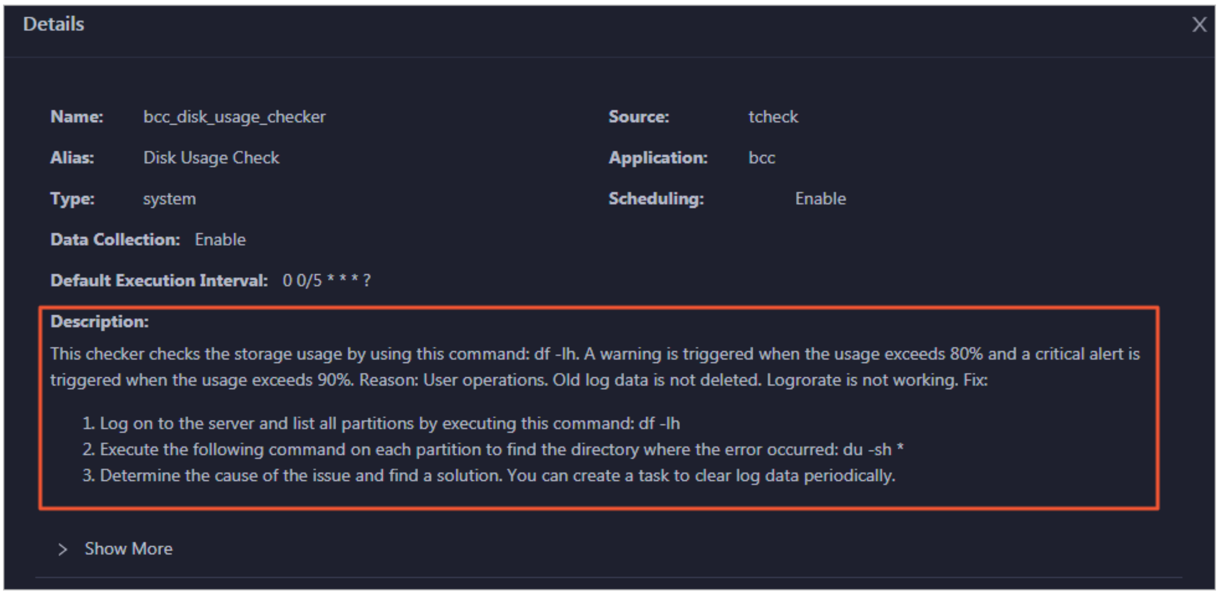
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status tab, click **Details** in the Actions column of a checker for which alerts are reported. On the Details page, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

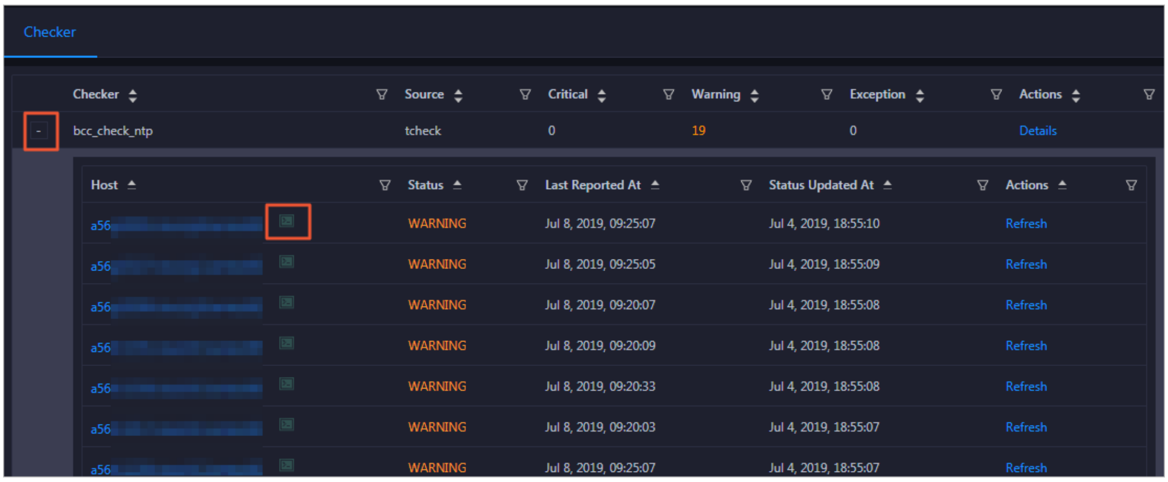
1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

> Show More

Log on to a host

You may need to log on to a host to handle alerts or other issues that occurred on the host.

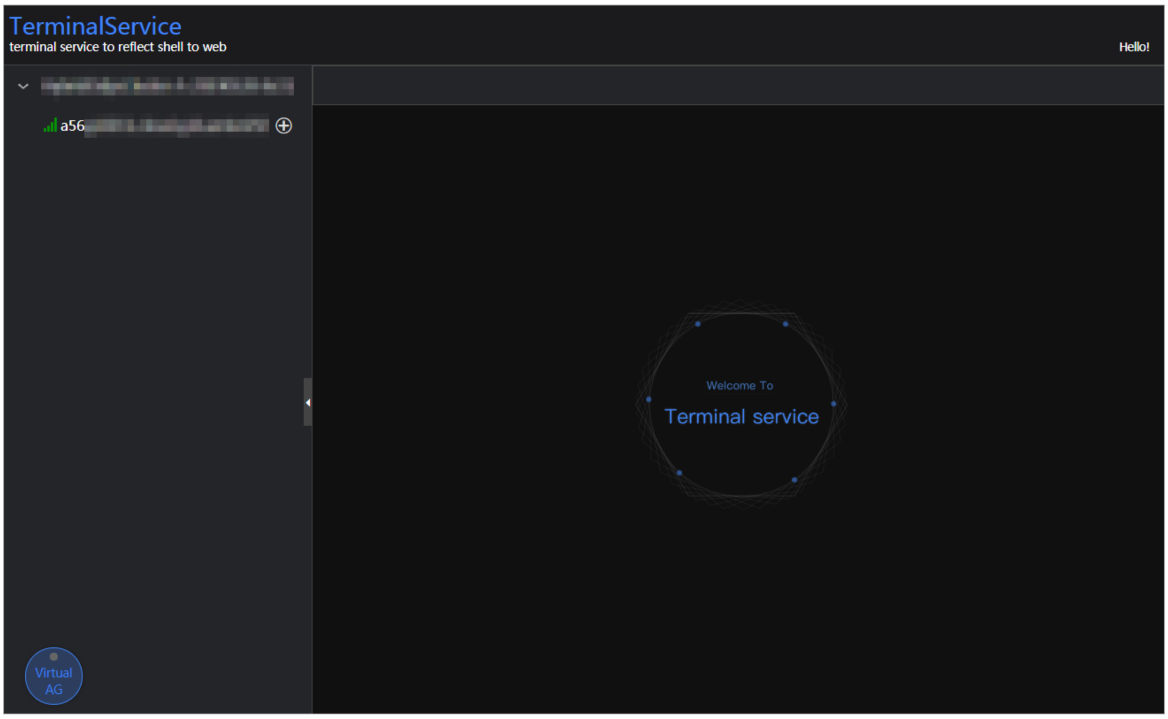
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported.



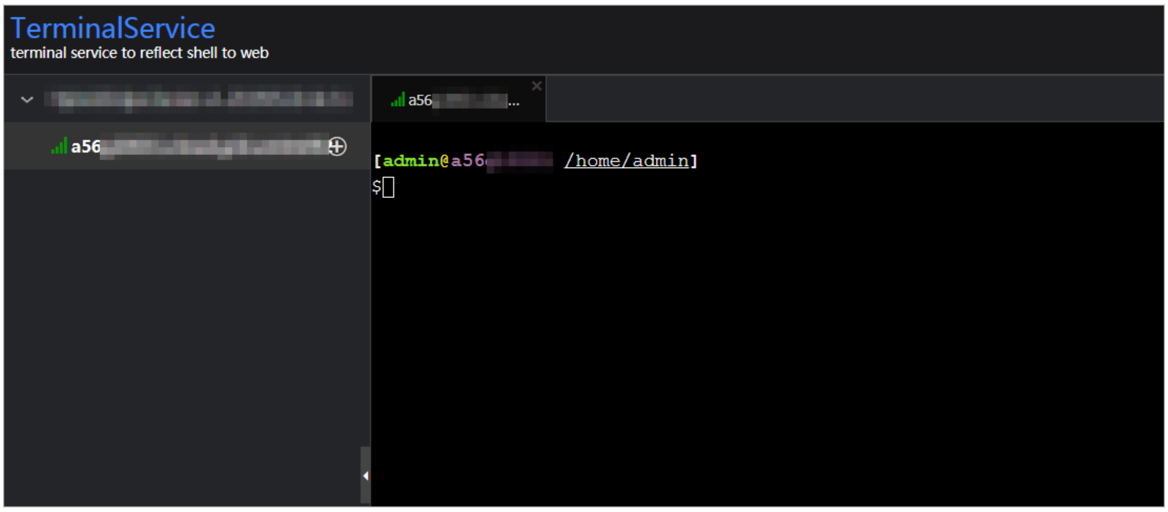
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

2. Click the **Login in** icon of a host. The **TerminalService** page appears.



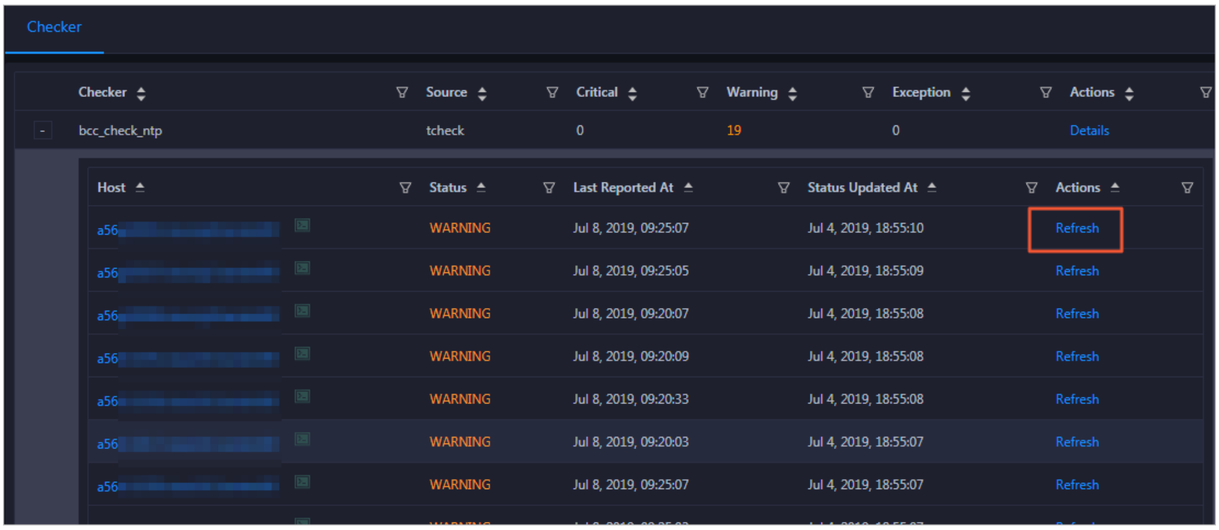
3. On the **TerminalService** page, click the hostname in the left-side navigation pane to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. This way, you can check whether the alert is cleared.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

11.3.2.5. Host O&M

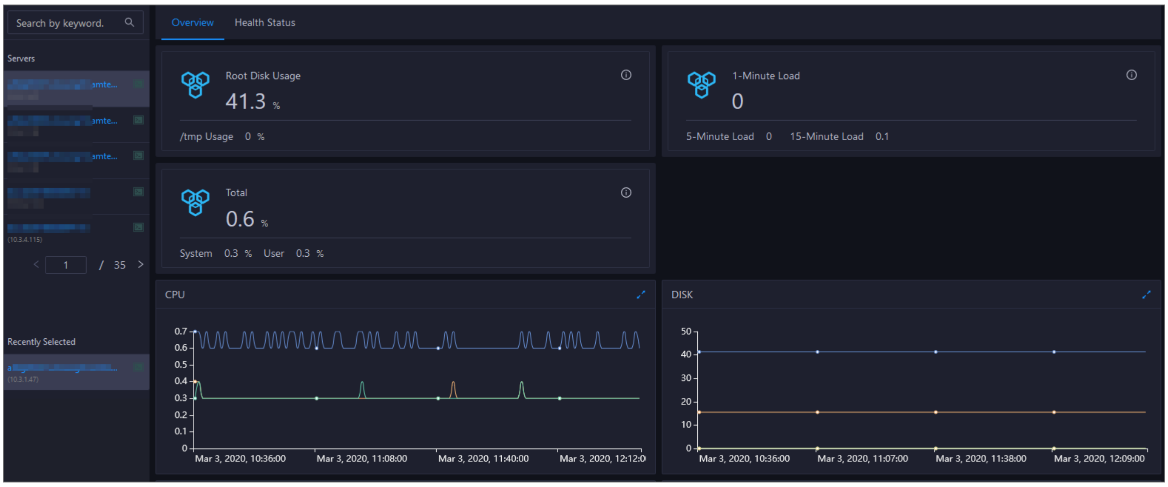
11.3.2.5.1. Host overview

The host overview page displays the overall running information about a host in a DataWorks cluster. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.

Entry

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner, and then click **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner.

4. Click the **Hosts** tab at the top of the **O&M** page.
5. On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Overview** tab. The **Overview** page appears.



Search by keyword.

Servers

[redacted]

1 / 35

Recently Selected

[redacted]

Overview | Health Status

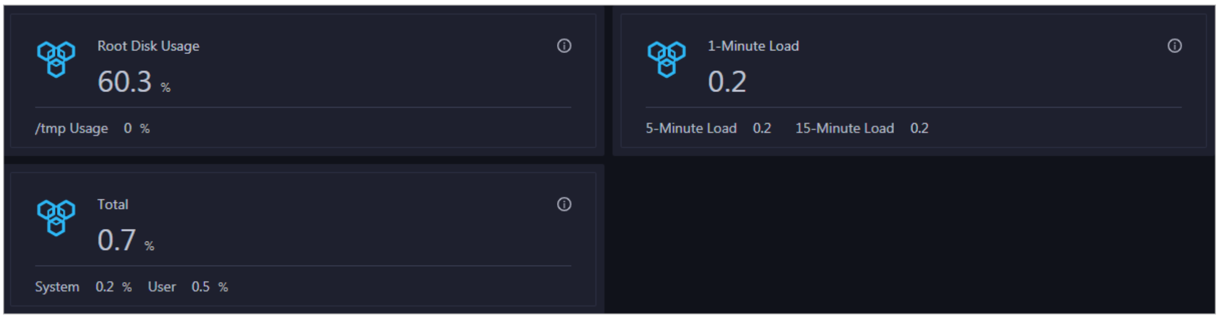
Root Disk Usage 41.3 %
/tmp Usage 0 %

1-Minute Load 0
5-Minute Load 0 15-Minute Load 0.1

Total 0.6 %
System 0.3 % User 0.3 %

Root Disk Usage, Total, and 1-Minute Load

These sections display the root disk usage, total usage, and 1-minute load for the selected host. The Root Disk Usage section provides the usage of the */tmp* directory. The Total section provides the system usage and user usage. The 1-Minute Load section provides the 1-minute, 5-minute, and 15-minute load averages.



Root Disk Usage 60.3 %
/tmp Usage 0 %

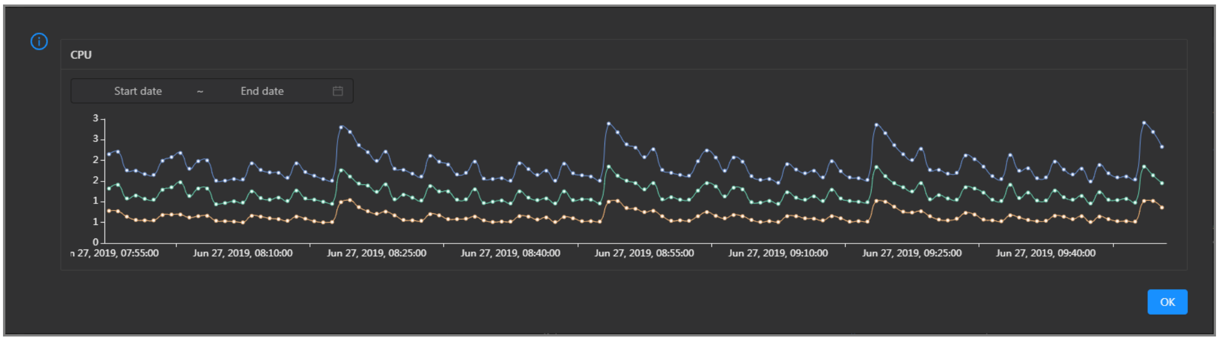
1-Minute Load 0.2
5-Minute Load 0.2 15-Minute Load 0.2

Total 0.7 %
System 0.2 % User 0.5 %

CPU

The CPU chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) of the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

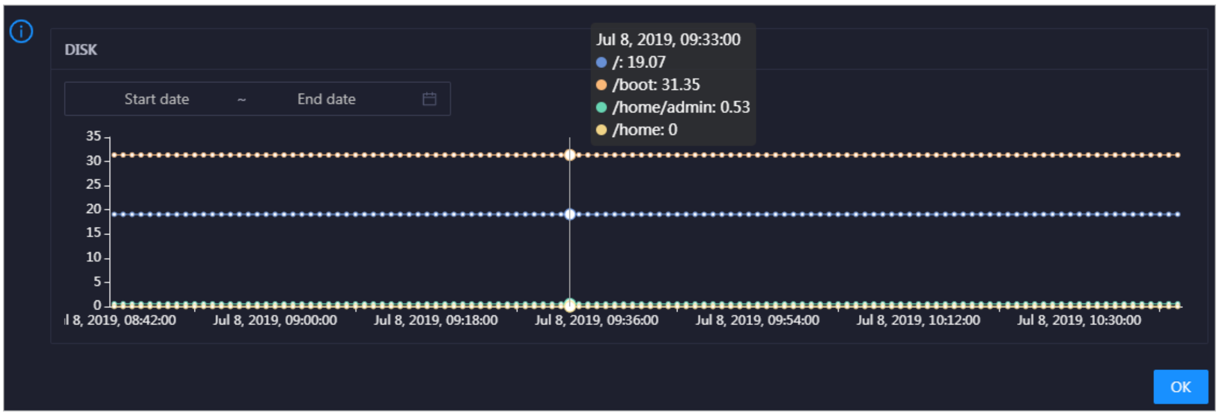


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the host in the specified period.

DISK

The DISK chart shows the trend lines of the storage usage in the */*, */boot*, */home/admin*, and */home* directories for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

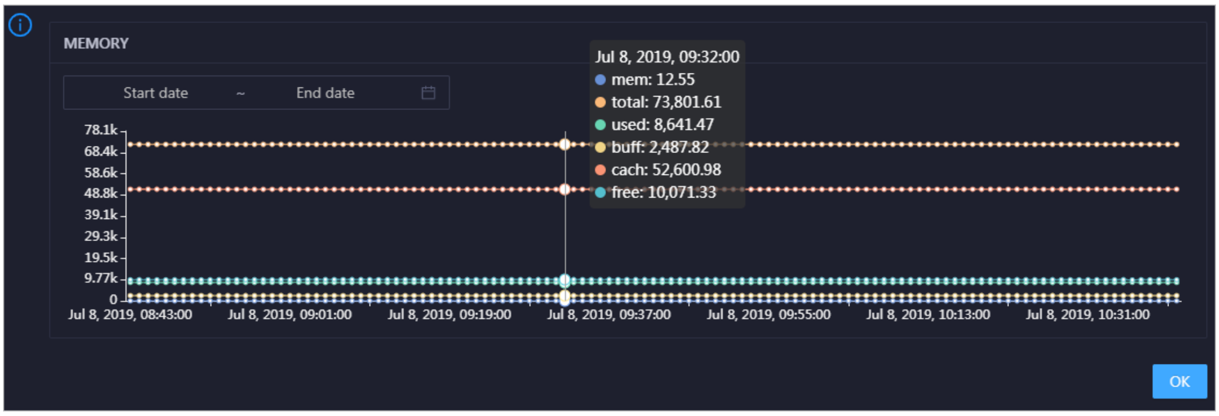


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the host in the specified period.

MEMORY

The MEMORY chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

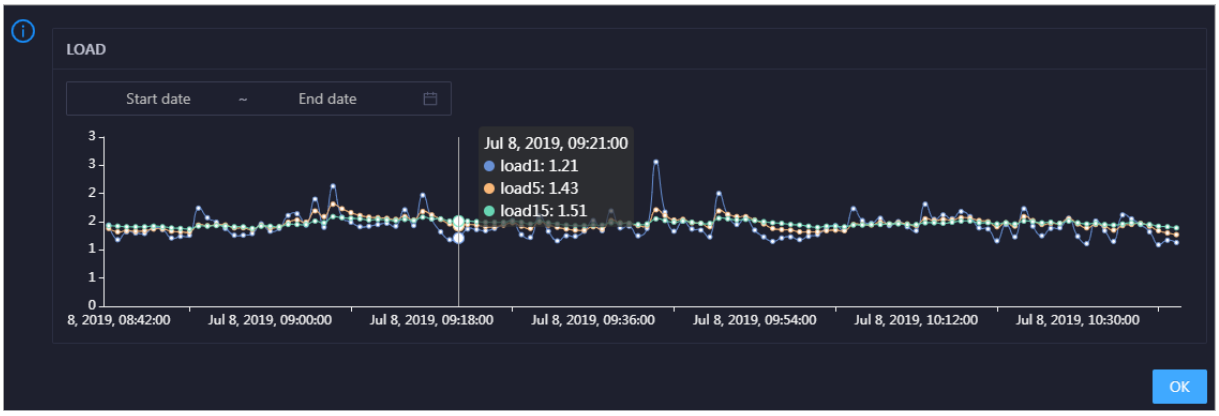


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the host in the specified period.

LOAD

The LOAD chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

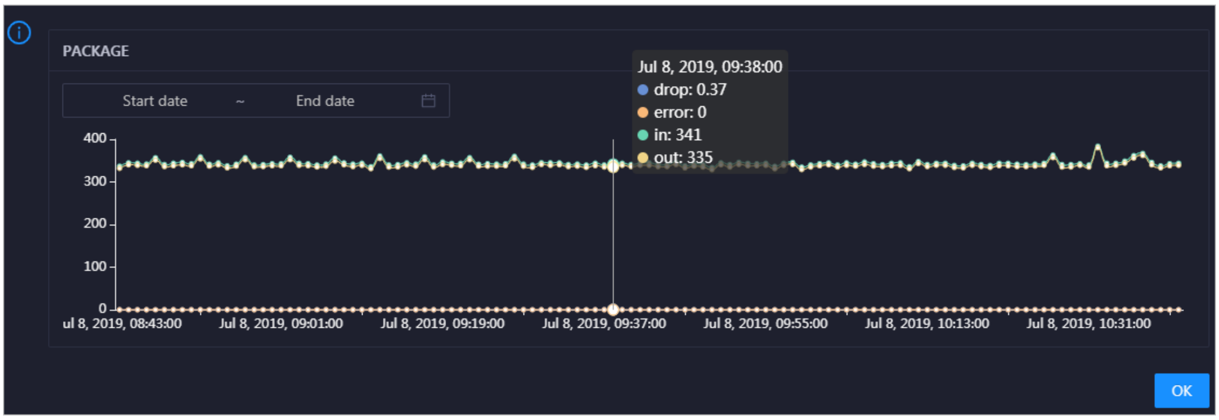


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the host in the specified period.

PACKAGE

The PACKAGE chart shows the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the host over time in different colors. These trend lines reflect the data transmission status of the host.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

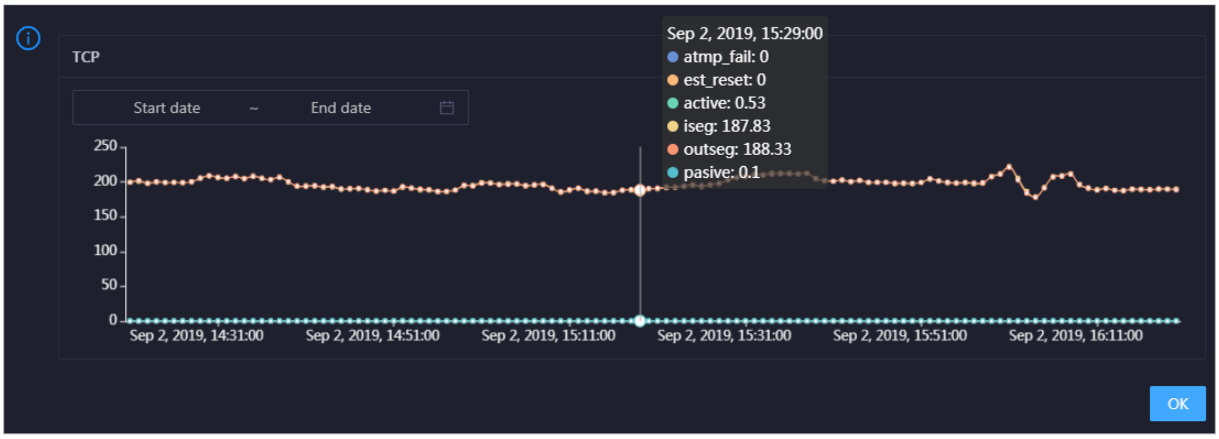


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the host in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the host over time in different colors. These trend lines reflect the TCP connection status of the host.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

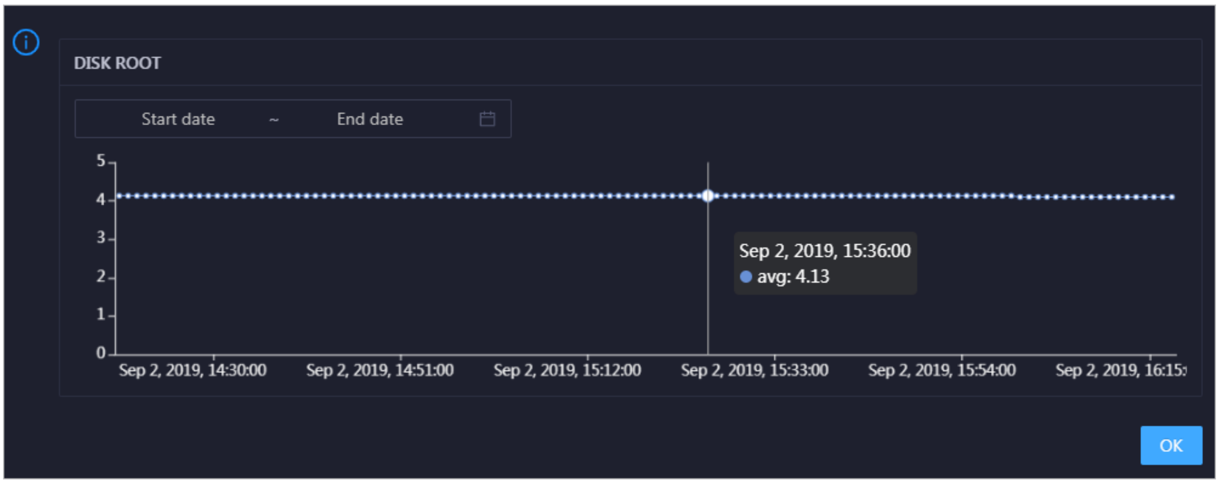


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the host in the specified period.

DISK ROOT

This chart displays the trend line of the average usage of the root disk (/) for the host over time.

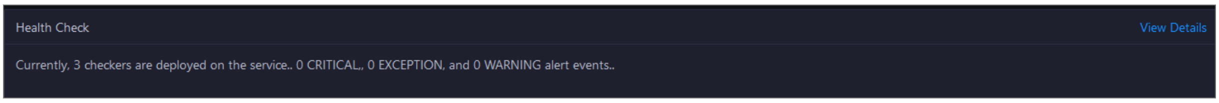
Click ⤢ in the upper-right corner of the chart to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the host in the specified period.

Health Check

This section displays the number of checkers deployed for the host and the respective number of Critical, Warning, and Exception alerts.



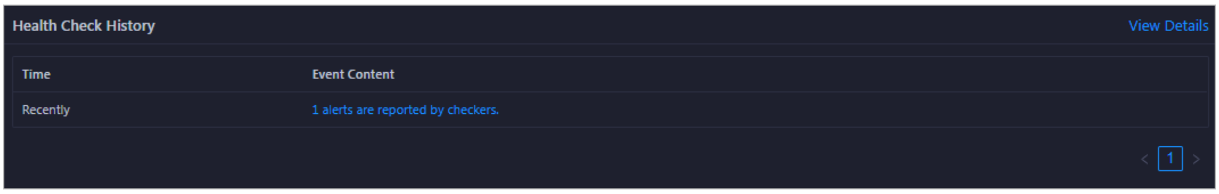
Health Check View Details

Currently, 3 checkers are deployed on the service.. 0 CRITICAL,. 0 EXCEPTION, and 0 WARNING alert events..

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Host health.

Health Check History

This section displays a record of the health checks performed on the host.



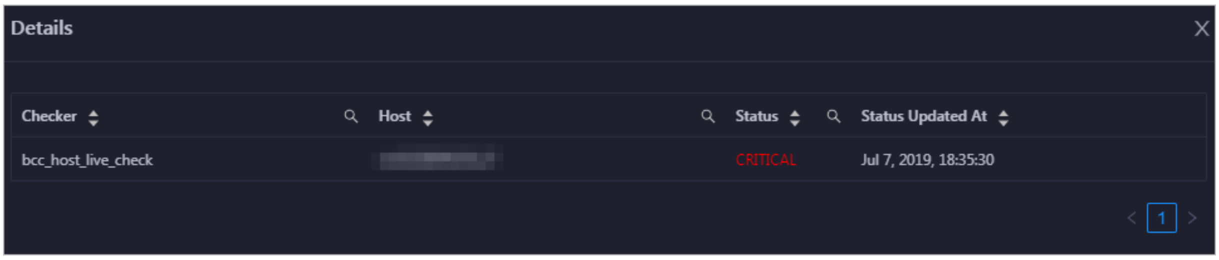
Health Check History

View Details

Time	Event Content
Recently	1 alerts are reported by checkers.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Host health.

You can click the event content of a check to view the exception items.



Details

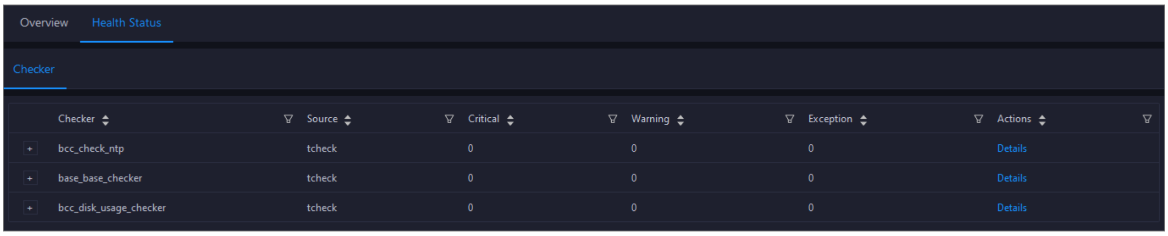
Checker	Host	Status	Status Updated At
bcc_host_live_check	[redacted]	CRITICAL	Jul 7, 2019, 18:35:30

11.3.2.5.2. Host health

On the Health Status page, you can view the checkers of the selected host, including the checker details, check results, and schemes to clear alerts (if any). In addition, you can log on to the host and perform manual checks on the host.

Go to the Health Status page under Hosts

1. Log on to the ABM console.
2. Click in the upper-left corner and select **DataWorks**.
3. On the page that appears, click **O&M** in the upper-right corner.
4. Click the **Hosts** tab at the top of the **O&M** page.
5. On the **Hosts** page, select a host in the left-side navigation pane, and click the **Health Status** tab. The **Health Status** page appears.

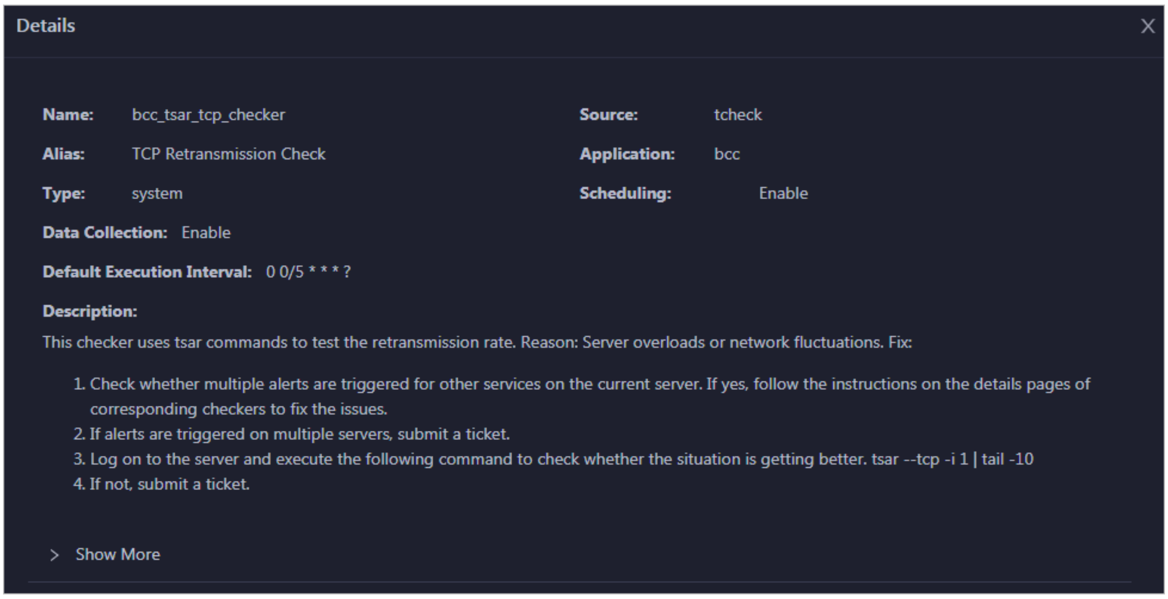


Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	0	0	Details
base_base_checker	tcheck	0	0	0	Details
bcc_disk_usage_checker	tcheck	0	0	0	Details

On the **Health Status** page, you can view all checkers and the check results for the host. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

View checker details

1. On the Health Status page, click **Details** in the Actions column of a checker. In the dialog box that appears, view the checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

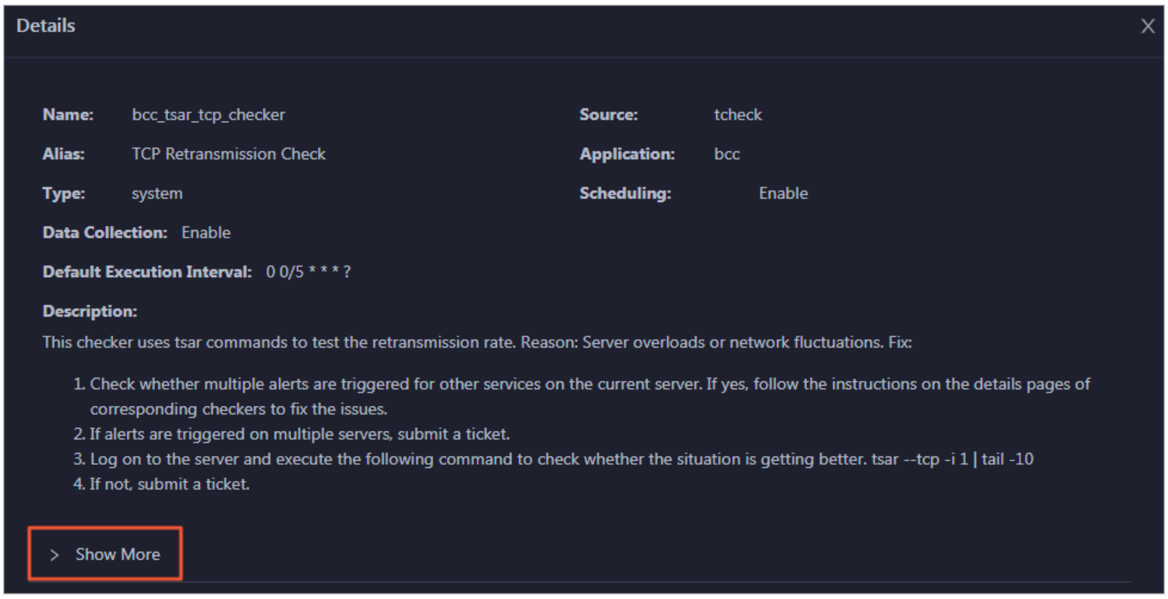
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include the name, source, alias, application, type, default execution interval, and description of the checker, whether scheduling is enabled, and whether data collection is enabled. The schemes to clear alerts are provided in the description.

2. Click **Show More** at the bottom to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

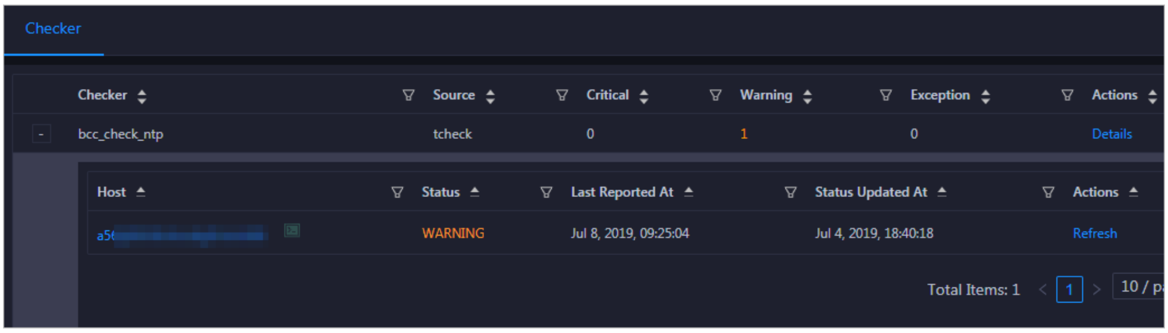
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about the execution script, execution target, default threshold, and mount point for data collection.

View alert causes

You can view the check history and check results of a checker.

1. On the Health Status page, click **+** to expand a checker with alerts.



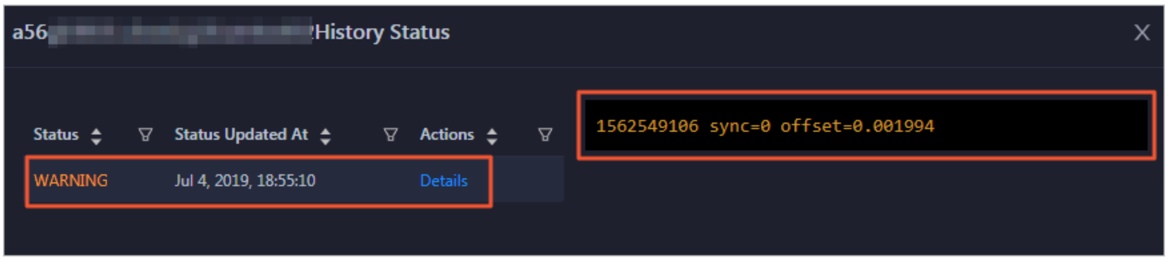
Checker

	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

2. Click the hostname. In the dialog box that appears, click **Details** in the Actions column of a check result to view the alert causes.



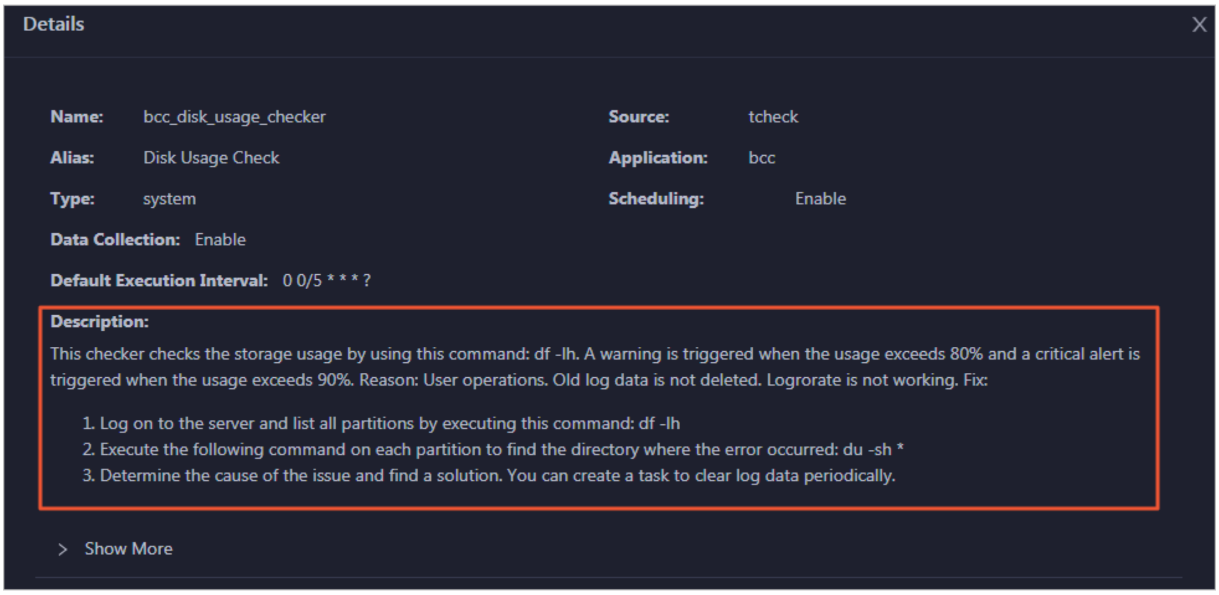
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status page, click **Details** in the Actions column of a checker with alerts. In the dialog box that appears, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker
Source: tcheck
Alias: Disk Usage Check
Application: bcc
Type: system
Scheduling: Enable
Data Collection: Enable
Default Execution Interval: 0 0/5 * * * ?

Description:

This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

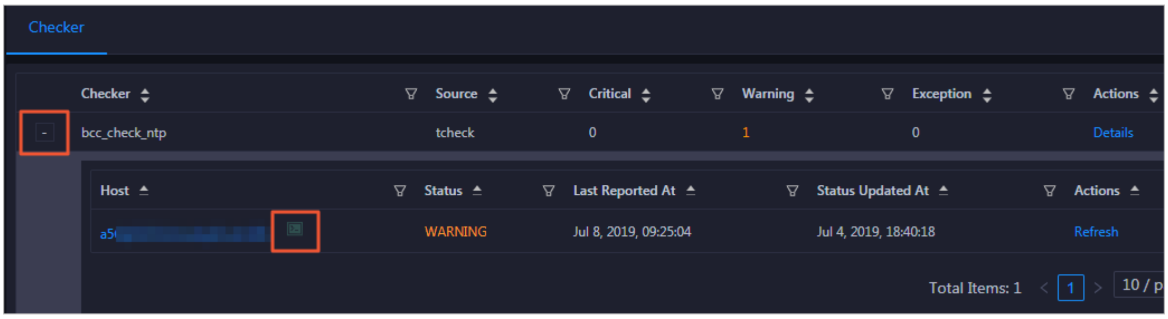
1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

> Show More

Log on to a host

To log on to a host to clear alerts or perform other operations, follow these steps:

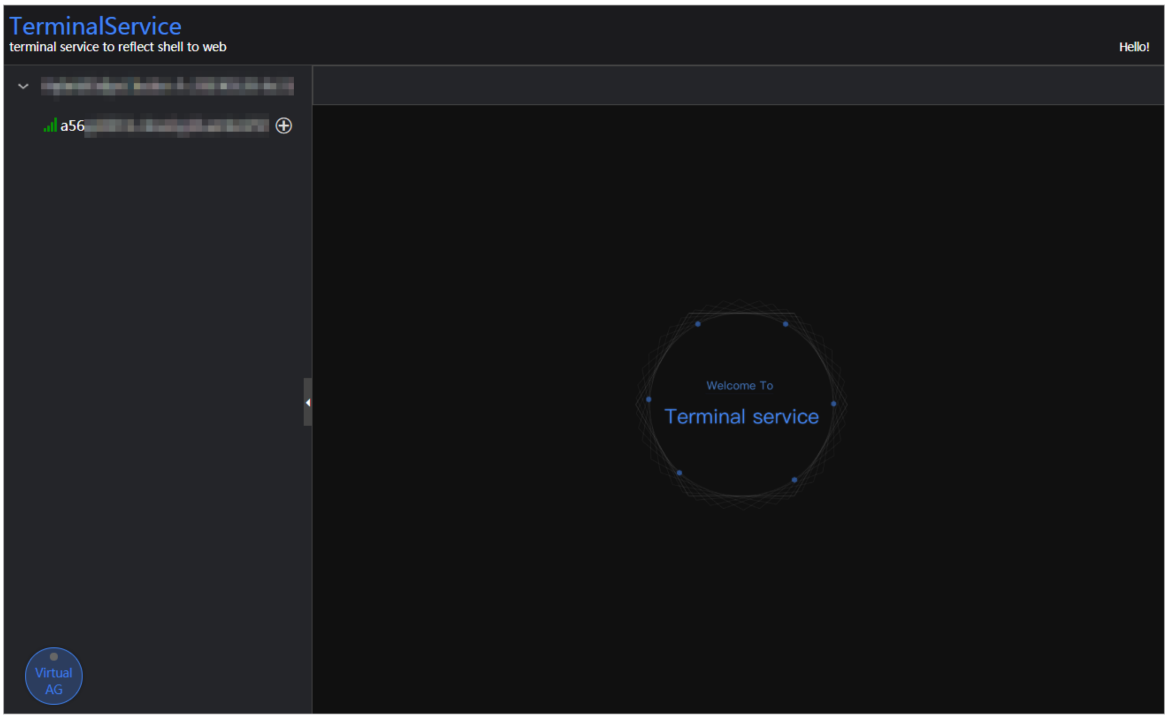
1. On the Health Status page, click **+** to expand a checker with alerts.



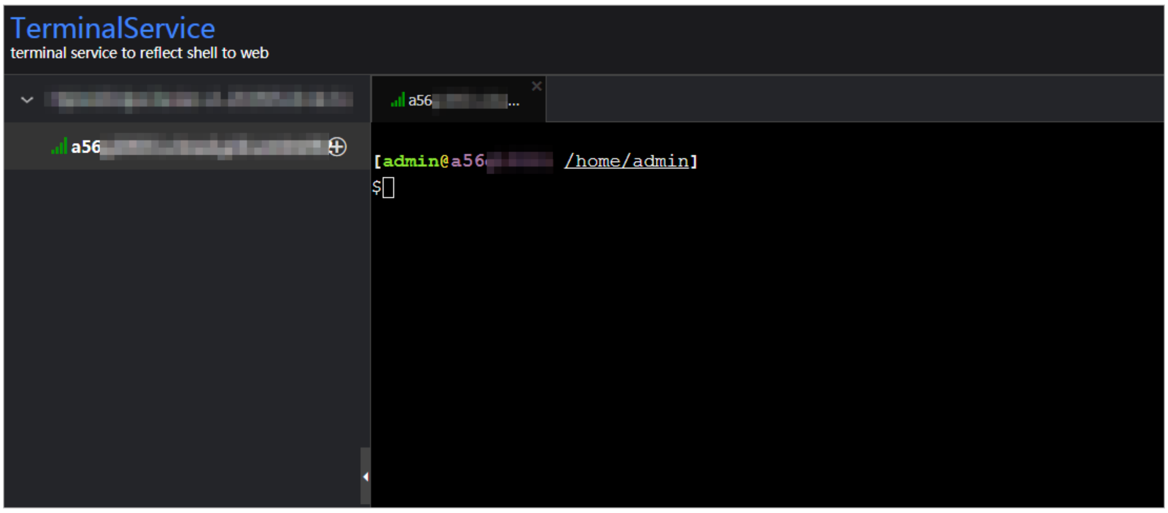
Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

2. Click the **Log On** icon of a host. The **TerminalService** page appears.



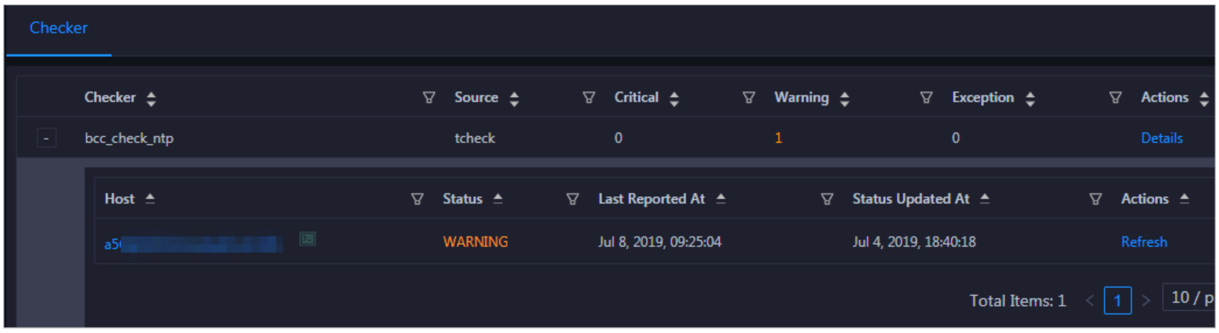
3. On the **TerminalService** page, click the hostname on the left to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. In this way, you can check whether the alert is cleared.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

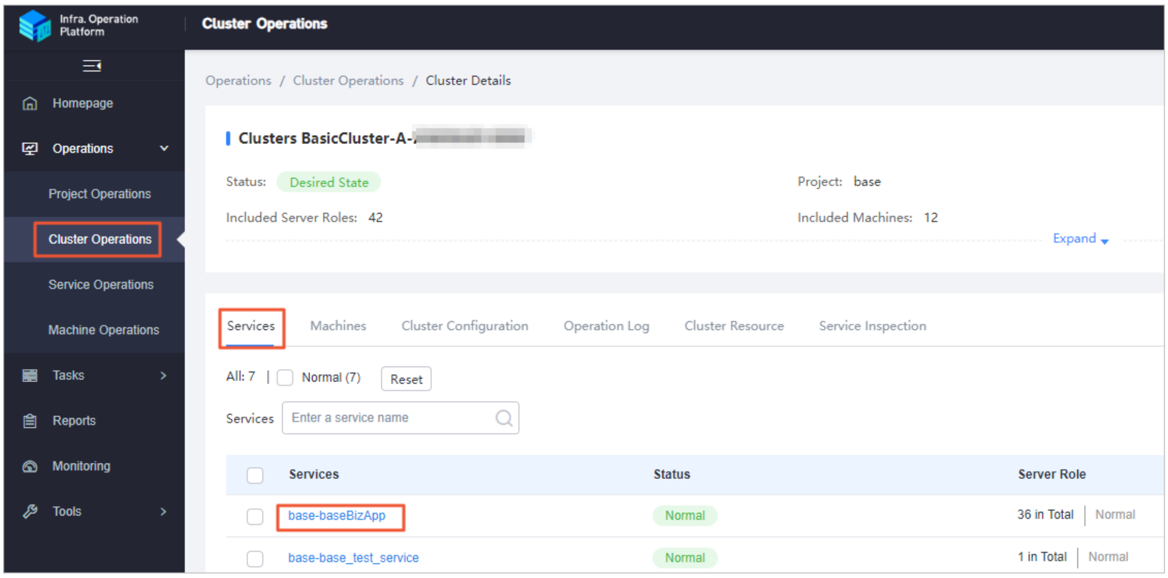
11.3.3. Common administration tools and commands

11.3.3.1. Find the host where a service resides

This topic describes how to find the host where a service resides.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products** > **Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M** > **Basic O&M** > **Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
3. On the page that appears, select **base** from the **Project** drop-down list to filter clusters.
4. Click the name of the target cluster. The **Cluster Details** page appears.



Clusters BasicCluster-A-[redacted]

Status: Desired State

Project: base

Included Server Roles: 42

Included Machines: 12

Services	Status	Server Role
base-baseBizApp	Normal	36 in Total | Normal
base-base_test_service	Normal	1 in Total | Normal

5. Click the **base-baseBizApp** service. On the **Machine Details** page, view information about the host where the service resides.

11.3.3.2. View cluster resources

This topic describes how to view the applications, resources, status, and version of a cluster.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products > Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M > Basic O&M > Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, choose **Operations > Cluster Operations**.
3. On the page that appears, select **base** from the **Project** drop-down list to filter clusters.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. Click the **Cluster Resource** tab. Then, you can filter required cluster information by **Server Role**, **Version**, **Name**, **Type**, or **Status**. Find the target application and click **Details** in the **Application Result** column to view detailed information about the application. For example, if you need to log on to the database of a specific application, you can find detailed logon information about the database in the **Application Result** message.

11.3.3.3. Commands to restart services

Enter the container that runs the service as an admin user, and then run the following commands to restart services.

> **Note** Only admin users can run the following commands to restart the service.

- To restart the base-biz-cdp service, run the `/home/admin/cdp_server/bin/appctl.sh restart` command.
- To restart the base-biz-gateway service, run the `/home/admin/alisatasknode/target/alisatasknode/bin/serverctl restart` command.
- To restart other services, run the `/home/admin/base-biz-[application name]/bin/jbossctl restart` command.

  For example, to restart the base-biz-alisa service, run `/home/admin/base-biz-alisa/bin/jbossctl restart`.

11.3.3.4. View logs of a failed instance

This topic describes how to view logs of a failed instance in Operation Center.

Procedure

1. Log on to the DataWorks console.
2. On the DataStudio page, click ☰ in the upper-left corner and choose **All Products > Operation Center**.
3. On the **Dashboard** page, click **Failed** in the **Instances** section. The **Cycle Instance** page appears. On this page, you can view all the instances that failed to run in the current workspace.
4. Click the target instance, and then right-click the failed node on the DAG that appears on the right

side of the page.

5. Select **View Runtime Log**.

11.3.3.5. Rerun multiple instances at a time

You can use the batch rerun feature of DataWorks to rerun multiple instances at a time.

Procedure

1. Log on to the DataWorks console.
2. On the DataStudio page, click ≡ in the upper-left corner and choose **All Products** > **Operation Center**.
3. On the **Dashboard** page, click **Failed** in the **Instances** section. The **Cycle Instance** page appears. On this page, you can view all the instances that failed to run in the current workspace.
4. Select the instances to be rerun.
5. Choose **More** > **Rerun** in the lower-left corner.
6. In the message that appears, click **Rerun**.

11.3.3.6. Stop multiple instances at a time

You can use the batch stop feature of DataWorks to stop multiple instances at a time.

Procedure

1. Log on to the DataWorks console.
2. On the DataStudio page, click ≡ in the upper-left corner and choose **All Products** > **Operation Center**.
3. On the **Dashboard** page, click **Running** in the **Instances** section. The **Cycle Instance** page appears. On this page, you can view all the running instances in the current workspace.

   > ? **Note** You can stop only instances that are running.

4. Select the instances that you want to stop.
5. Choose **More** > **Stop** in the lower-left corner.
6. In the message that appears, click **Stop**.

11.3.3.7. Commonly used Linux commands

This topic describes the commonly used Linux commands.

Display workloads in the Linux system: top

View the three numbers after load average, which indicate the workload averages for the last 5, 10, and 15 minutes, respectively. If you divide one of these numbers by the quantity of logical CPUs and the result is greater than 5, the Linux system is overloaded.

List the sizes of files: du

You can run the `du -sh` command with a file name added at the end to view the size of the specified file. If you run the `du -sh *` command, you can view the sizes of all the files in the current directory.

List processes in the Linux system: ps

You can run the `ps -ef` command to view the processes that are running in the Linux system.

Search for strings: grep

To search for a string in a specified log file and display all lines that contain the string, run the command in the following format:

```
grep ["String"] [File name]
```

To search for a string in a specified file and display only the first few lines that contain the string, run the command in the following format:

```
grep -C Number of lines ["String"] [File name]
```

> **Note** The -C parameter is an uppercase letter. Set its value to a number.

To search for a string in a specified file and display only the last few lines that contain the string, run the command in the following format:

```
grep -A Number of lines ["String"] [File name]
```

Terminate processes: kill

You can run the `kill -9` command with the PID of a process added at the end to terminate the process.

docker commands

List all containers: `docker ps -a`

List the logs of a container: `docker logs [Container ID]`

Log on to a container: `docker exec -it [Container ID] bash`

11.3.3.8. View the slot usage of resource groups

This topic describes how to view the slot usage of a resource group.

Scenario: When a large number of nodes are waiting for resources in Operation Center, you can run a set of commands to view the slot usage of each resource group.

First, log on to the base-biz-alisa database. In an Apsara Stack V3 environment, select base from the Project drop-down list on the Clusters page in Apsara Infrastructure Management Framework. Locate the base-biz-alisa service whose type is db in the filtered results. Right-click the Result column and choose Show More from the shortcut menu to obtain the connection information of the database. Then, run a MySQL command to log on to the database based on the obtained information.

Run the following command to view the top 10 nodes by execution duration:

```
select task_id,gateway,slot,create_time from alisa_task where status=2 order by create_time limit 10;
```

Run the following command to view the top 10 nodes by slot usage:

```
select task_id,gateway,slot,create_time from alisa_task where status=2 order by slot desc limit 10;
```

Run the following command to view the total number of nodes for each slot. Based on the command output, you can find out nodes that occupy a large number of slot resources.

```
select slot,count(*) from alisa_task where status=2 group by slot;
```

Run the following command to view the slot usage of each resource group:

```
select exec_target,sum(slot) from alisa_task where status=2 group by exec_target;
```

View the status of each gateway server. If the values of live and active_type are 1 for any gateway server, the gateway server fails.

```
select * from alisa_node;
```

11.3.4. Process daily administration operations

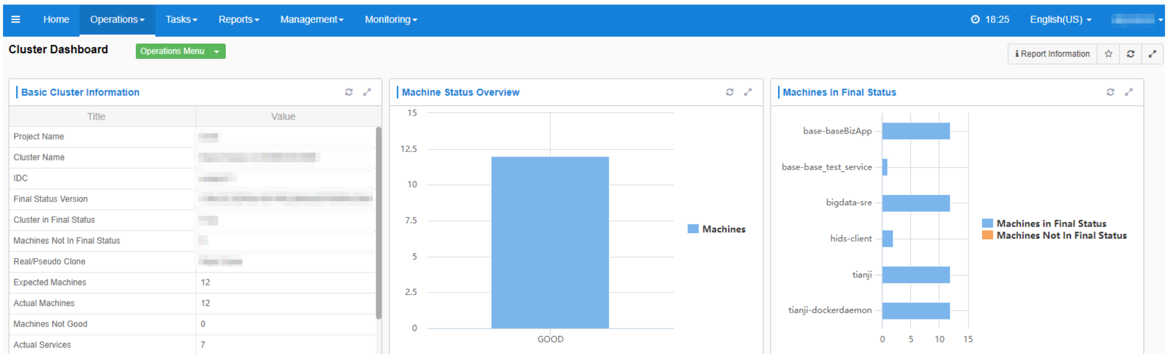
11.3.4.1. Daily check

11.3.4.1.1. Check the service status and basic server information

This topic describes how to view the basic cluster information, server status, and the number of servers in the desired state.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products > Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M > Basic O&M > Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, click **Reports**.
3. On the **C** tab, select **base** from the **Project** drop-down list.
4. Move the pointer over ⋮ next to the target server and select **Dashboard**. On the **Cluster Dashboard** page, view information in the **Basic Cluster Information**, **Machine Status Overview**, and **Machines in Final Status** sections.



Cluster Dashboard

Basic Cluster Information

Title	Value
Project Name	[redacted]
Cluster Name	[redacted]
IDC	[redacted]
Final Status Version	[redacted]
Cluster in Final Status	[redacted]
Machines Not In Final Status	[redacted]
Real/Pseudo Clone	[redacted]
Expected Machines	12
Actual Machines	12
Machines Not Good	0
Actual Services	7

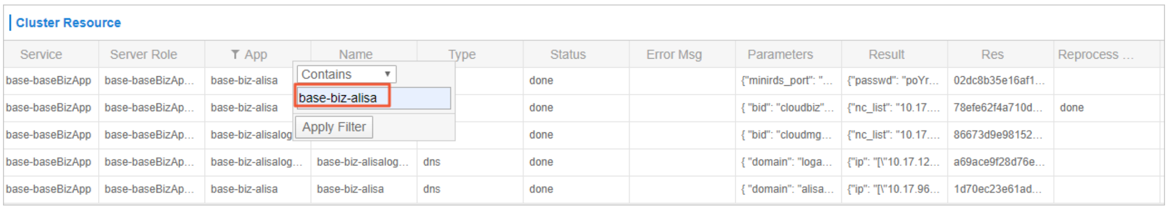
If only blue is shown in the Machine Status Overview section, all servers in the current cluster are running properly. If yellow is shown in the Machine Status Overview section, errors occur on servers.

11.3.4.1.2. Check the status of a gateway server

This topic describes how to check the status of a gateway server.

Procedure

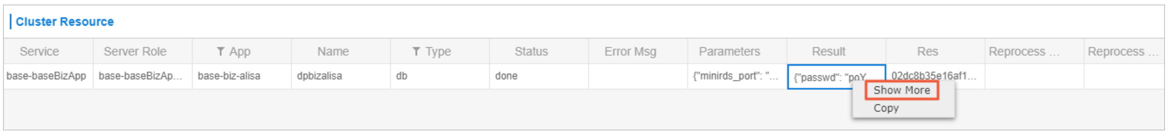
1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products** > **Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M** > **Basic O&M** > **Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, click **Reports**.
3. On the **C** tab, select **base** from the **Project** drop-down list.
4. Move the pointer over ⋮ next to the target server and select **Dashboard**.
5. In the **Cluster Resource** section, move the pointer over the **App** column and click ☰.
6. In the dialog box that appears, enter **base-biz-alisa** in the Filter field and click **Apply Filter**.



Cluster Resource

Service	Server Role	App	Name	Type	Status	Error Msg	Parameters	Result	Res	Reprocess ...
base-baseBizApp	base-baseBizAp...	base-biz-alisa			done		{"minirds_port": "...	{"passwd": "poYr...	02dc8b35e16af1...	
base-baseBizApp	base-baseBizAp...	base-biz-alisa			done		{ "bid": "cloudbiz"...	{"nc_list": "10.17....	78efe62f4a710d...	done
base-baseBizApp	base-baseBizAp...	base-biz-alisalog			done		{ "bid": "cloudmg...	{"nc_list": "10.17....	86673d9e98152...	
base-baseBizApp	base-baseBizAp...	base-biz-alisalog...	base-biz-alisalog...	dns	done		{ "domain": "loga...	{"ip": "[\"10.17.12...	a69ace9f28d76e...	
base-baseBizApp	base-baseBizAp...	base-biz-alisa	base-biz-alisa	dns	done		{ "domain": "alisa...	{"ip": "[\"10.17.96...	1d70ec23e61ad...	

7. Filter services whose type is **db** in the same way.
8. Find the target service, right-click the information in the **Result** column, and then select **Show More** to view the endpoint, username, and password for logging on to the database.



Cluster Resource

Service	Server Role	App	Name	Type	Status	Error Msg	Parameters	Result	Res	Reprocess ...	Reprocess ...
base-baseBizApp	base-baseBizAp...	base-biz-alisa	dpbizalisa	db	done		{"minirds_port": "...	{"passwd": "poY	02dc8b35e16af1...		

9. Connect to the database and run the following MySQL command to query the node information:

```
Select * from alisa_node;
```

If the value of the active_type or live parameter in the command output contains *-1* or *0*, the service is abnormal. Contact Alibaba Cloud technical support engineers.

11.3.4.1.3. Monitor service roles and servers

This topic describes how to view the details of monitored service roles and servers.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
    i. Log on to the ABM console.
    ii. In the left-side navigation pane, choose **Products** > **Product List**.
    iii. On the page that appears, choose **Apsara Stack O&M** > **Basic O&M** > **Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
3. On the page that appears, select **base** from the **Project** drop-down list to filter clusters.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. Click the **Services** tab and then click the **base-baseBizApp** service.
6. On the **Service Details** page, click the target service role to view the servers where the service resides.
7. Find the target server and click **View** in the **Metric** column.
8. In the **Machine Metrics** dialog box, view the information on the **Server Role Metric** and **Machine Metrics** tabs.

11.3.4.2. View logs of the services

Logs of the gateway service are stored in `/home/admin/alisatasknode/logs/alisatasknode.log` .

Logs of the cdp services are stored in `/home/admin/cdp_server/logs/cdp_server.log` .

Logs of other services are stored in `/home/admin/base-biz-[service name]/base-biz-[service name].log` .

For example, the logs of the base-biz-phoenix service are stored in `/home/admin/base-biz-phoenix/base-biz-phoenix.log` .

11.3.4.3. Scale out the cluster that runs the base-biz-gateway service

This topic describes how to scale out the cluster that runs the base-biz-gateway service.

Prerequisites

Before you apply a scaling change, make sure that the system is running in a status that is conducive to your change. For example, make sure that the storage space is large enough, and verify prerequisites such as the permissions on the files, the owners and paths of the files, and the software version.

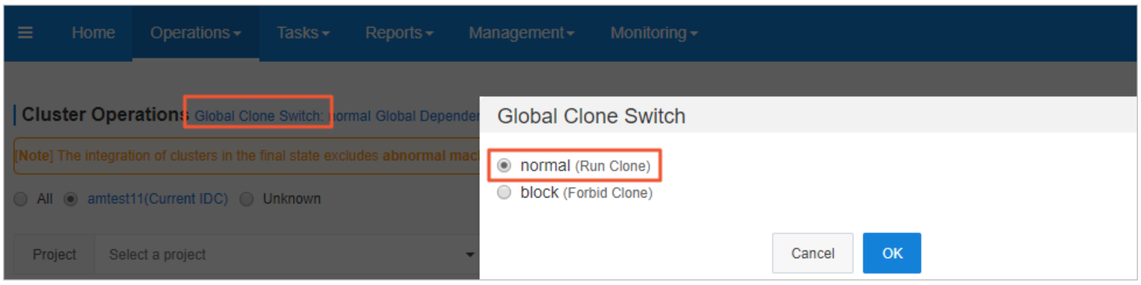
- Before you scale out a BasicCluster cluster, make sure that it reaches the desired state and works as expected.
- A screenshot of the key initial configurations for the cluster is saved.

- IP addresses do not conflict. If you need to use a new buffer cluster for the scale-out, make sure that the IP addresses that Deployment Planner assigns to the servers in the cluster are not used in the current environment. This can avoid exceptions arising from IP address conflicts after the scale-out.
- The clone_mode parameter is set to normal.

  > **Note** Apsara Infrastructure Management Framework of V3.3 and later versions support cloning protection. Before the scale-out, you must set the clone_mode parameter to normal. After the scale-out is complete, set this parameter to block.

  To set the clone_mode parameter to normal, perform the following steps:

  i. Log on to Apsara Infrastructure Management Framework.
  ii. In the left-side navigation pane, click **Reports**.
  iii. In the top navigation bar, choose **Operations > Cluster Operations**.
  iv. Click **Global Clone Switch**. In the **Global Clone Switch** dialog box, select **normal**.



Cluster Operations Global Clone Switch: normal Global Depende

[Note] The integration of clusters in the final state excludes abnormal mac

○ All ● amtest11(Current IDC) ○ Unknown

Global Clone Switch

● normal (Run Clone)
○ block (Forbid Clone)

  v. Click **OK**.

Procedure

1. Create a buffer cluster. Skip this step if an existing buffer cluster has idle servers and the physical machine, memory, CPU, and disk size of the idle servers are the same as those of current servers that run the base-biz-gateway service.

   *In the scale-out procedure, use the actual parameter values and IP addresses instead of the specific parameter values in this guide.

   > **Note** When you plan to scale out the cluster with Deployment Planner, make sure that the name of the new buffer cluster is different from that of any existing buffer cluster.

   i. Copy and paste *_tianji_imports* to the */apsarapangu/disk3/u_disk/* directory of the OPS1 server and run the following command in the *tianji_zhuque_sdk* directory:

   ```
   ./tianji_zhuque_exchanger.py import --skip_packages -o ${Final status in Apsara Infrastructure Management Framework} -c tianji_dest.conf
   ```

   ii. Log on to Apsara Infrastructure Management Framework. Select **buffer** from the **Project** drop-down list.
   iii. Click the buffer cluster to view the status of servers in the cluster.

iv. Run the following commands on the OPS1 server to check scale-out information by calling API operations:

```
cd /cloud/app/tianji-tools/PrivateCloudTool#/tianji_ops_tool/current
ln -s /cloud/data/bootstrap_controller/BootstrapController#/bootstrap_controller/tianji_dest.con
f clt2.conf
./tianji_clt machinestatus -c buffer --config clt2.conf
```

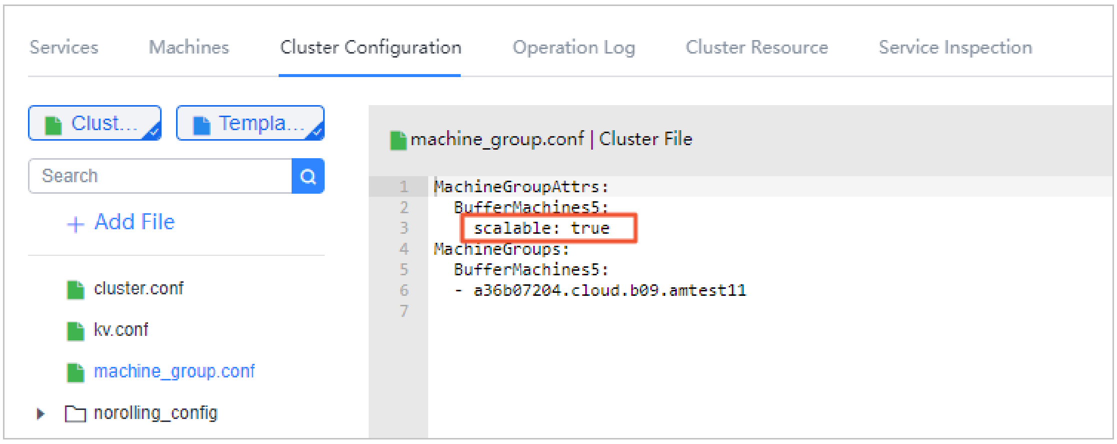
2. Scale in the buffer cluster by moving idle servers to the default cluster.

> **Note** You can use the default cluster to scale out the cluster that runs base-biz-cdp and base-biz-gateway services.

i. On the **Cluster Operations** page, click the target buffer cluster.

ii. On the **Cluster Details** page, click the **Cluster Configuration** tab.

iii. Click the **machine_group.conf** file. Make sure that the value of the scalable tag value is true for the new buffer cluster.



```
MachineGroupAttrs:
  BufferMachines5:
    scalable: true
MachineGroups:
  BufferMachines5:
  - a36b07204.cloud.b09.amtest11
```

iv. Run the following commands on the OPS1 server to scale in the buffer cluster:

```
cd /cloud/app/tianji-tools/PrivateCloudTool#/tianji_ops_tool/current
ln -s /cloud/data/bootstrap_controller/BootstrapController#/bootstrap_controller/tianji_dest.con
f clt2.conf (After you run this command, if a message appears indicating that a soft link already exis
ts, proceed with the next command.)
./tianji_ops_tool.py contract_nc -c [buffer cluster name] -l [Hostname of the server to be removed]
, [Hostname of the server to be removed],.... --config clt2.conf -s [SRG name]
```

Parameter	Description
-c	The name of the buffer cluster that you scale in, which starts with buffer-cluster.
-l	The list of hostnames of servers to be removed. Separate multiple hostnames with commas (,).
-s	The name of the SRG where the servers reside. You can find the SRG name in the *machine_group.conf* file of the buffer cluster.
-config	The tianji_clt file. ⓘ **Note** These commands cannot contain Chinese characters.

v. On the **Cluster Operations** page, verify that the servers have been removed.

vi. Run the following commands on the OPS1 server to check scale-in information by calling API operations:

```
cd /cloud/app/tianji-tools/PrivateCloudTool#/tianji_ops_tool/current
ln -s /cloud/data/bootstrap_controller/BootstrapController#/bootstrap_controller/tianji_dest.con
f clt2.conf (After you run this command, if a message appears indicating that a soft link already exis
ts, proceed with the next command.)
./tianji_clt machinestatus -c default --config clt2.conf
```

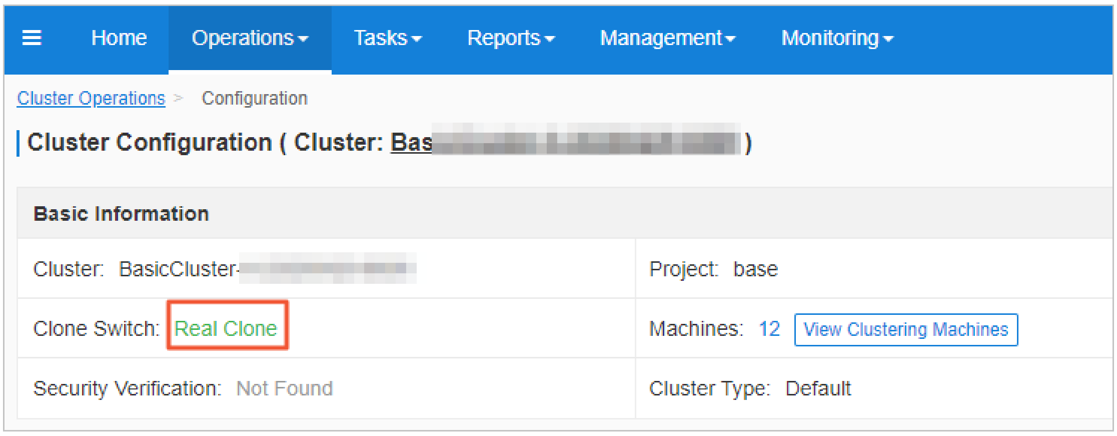
vii. Go to the details page of the new buffer cluster, and check whether the servers have been deleted from the machine_group.conf file. If the servers still exist, delete them from the machine_group.conf file and then submit a rolling task.

3. Add servers to the BasicCluster cluster and specify the name of the SRG where the servers reside.

i. Log on to Apsara Infrastructure Management Framework. In the left-side navigation pane, click **Reports**.

ii. In the top navigation bar, choose **Operations > Cluster Operations**.

iii. Right-click the target BasicCluster cluster and choose Monitoring > **Cluster Configuration**. On the page that appears, verify that **Clone Switch** is set to **Real Clone**.



Cluster Operations > Configuration

Cluster Configuration (Cluster: Bas[redacted])

Basic Information

Cluster: BasicCluster-[redacted]	Project: base
Clone Switch: Real Clone	Machines: 12
Security Verification: Not Found	Cluster Type: Default

iv. Run the following commands to perform scaling. A rolling task is triggered after you run these commands.

```
cd /cloud/app/tianji-tools/PrivateCloudTool#/tianji_ops_tool/current
ln -s /cloud/data/bootstrap_controller/BootstrapController#/bootstrap_controller/tianji_dest.conf clt2.conf (After you run this command, if a message appears indicating that a soft link already exists, proceed with the next command.)
```

To add servers to the cluster that runs the base-biz-gateway service, run the following command:

```
./tianji_ops_tool.py expand_nc -c [BasicCluster cluster name] -s BaseGwGroup -l [machine1,machine2] --config clt2.conf
```

To add servers to the cluster that runs the base-biz-gateway service, run the following command:

```
./tianji_ops_tool.py expand_nc -c [BasicCluster cluster name] -s BaseCdpGwGroup -l [machine1,machine2] --config clt2.conf
```

v. Run the following command to call an API operation to check the scaling result:

```
curl http://127.0.0.1:7070/api/v3/column/m. *?m.id=[machine hostname]
```

vi. Log on to the OpsClone container and run the following command to view the clone status:

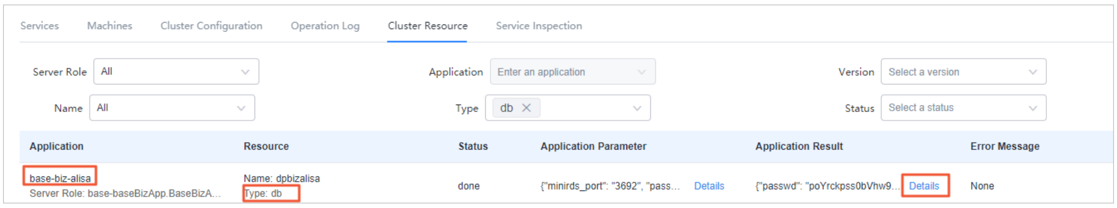
```
/home/tops/bin/python /root/opsbuild/bin/opsbuild.py acli list --status=ALL -n 10000 | vim -
```

4. Export the file that contains the information of desired state. After you complete the scale-out, export the file that contains the information of recent desired state to Deployment Planner. This ensures the success of subsequent scale-in and scale-out operations.
5. Verify the scale-out.

   i. Check the heartbeat logs of the servers. Open the terminal of each added server, log on to the gateway container, and then run the `tail -f /home/admin/alisatasknode/logs/heartbeat.log` command.

   If the logs are refreshed every 5 seconds, the heartbeat service is running as expected.

ii. Query the database information and check whether the server is online. Log on to Apsara Infrastructure Management Framework. Go to the **Cluster Details** page of the target BasicCluster cluster, click the **Cluster Resource** tab, set the Type parameter to **db**, and then find the **base-biz-alisa** service. Click **Details** in the **Application Result** column to check the database connection information.



Server Role: All
Application: Enter an application
Version: Select a version
Name: All
Type: db
Status: Select a status

Application	Resource	Status	Application Parameter	Application Result	Error Message
base-biz-alisa Server Role: base-baseBizApp.BaseBizA...	Name: dpbizalisa Type: db	done	{"minirds_port": "3692", "pass... Details	{"passwd": "poYrckpss0bVhw9... Details	None

Connect to the database by using a MySQL command, and run the `select * from alisa_node;` command. The information of all servers that run the base-biz-gateway service appears.

Check the values of the live and active_type parameters for each added server. If both the two values are 1, the server is online.

11.3.4.4. Scale in the base-biz-gateway cluster

Prerequisite

If a server in the base-biz-gateway cluster fails, you can repair and restart the server to redeploy the server.

If you want to remove a healthy server from the base-biz-gateway cluster, follow the instructions in this topic.

Note Before removing a healthy server, perform an on-site check to guarantee that the following conditions are met:

- No business applications are running on the server.
- The hostname of the server is correct.

Procedure

Perform checks before the scale-in

1. Perform an on-site check.

   Collect the detailed information of the server to be removed and the cluster that contains the server.

2. Make sure that the value of the scalable tag is true for the service resource group (SRG) of the server to be removed. If the value is false, change it to true and submit a rolling task.

   Log on to Apsara Infrastructure Management Framework. In the left-side navigation pane, choose **BasicCluster > Cluster Configuration File > machine_group.conf**. In this file, verify that the value of the scalable tag is true for the SRG of the server to be removed.

Stop the base-biz-gateway service

1. Log on to the server to be removed and run the `ps -ef|grep gateway` command to obtain the container ID of the base-biz-gateway service.
2. Run the `docker exec -it [container ID] bash` command to enter the container.

3. Switch to the admin account and run the `/home/admin/alisatasknode/target/alisatasknode/bin/serverctl stop` command.
4. Run the `ps -ef|grep java` command to check whether any process is running on the server. If any process is running, run the `kill -9 [process ID]` command to terminate the process.
5. Delete the program directories from the server.

   Clean up the disks of the server. Skip this step if you want to clone the server.

   ```
   #rm -rf /home/admin/*
   ```

   ```
   #rm -rf /opt/taobao/tbdpapp/
   ```

Move servers from the base-biz-gateway cluster to the default cluster in Apsara Infrastructure Management Framework

1. Log on to the ops1 server and run the following commands to remove a server from the base-biz-gateway cluster:

   ```
   cd /cloud/app/tianji-tools/PrivateCloudTool#/tianji_ops_tool/current
   ln -s /cloud/data/bootstrap_controller/BootstrapController#/bootstrap_controller/tianji_dest.conf clt
   2.conf (After you run this command, if a message appears indicating that a symbolic link already exists,
   proceed with the next command.)
   ./tianji_ops_tool.py contract_nc -c [clusterName] -l [machineList] --config tianji_clt.conf -s [SRGname]
   ```

   The parameters are described as follows:

   - -c: Required. Set this parameter to the name of the base cluster to be scaled in. To obtain the cluster name, choose Operations > Cluster Operations in the top navigation bar and select base from the Project drop-down list.
   - -l: Required. Set this parameter to the hostname of the server to be removed. Separate multiple hostnames with commas (,).
   - -s: Required. Set this parameter to the SRG name of the server to be removed. Find the machine_group.conf file among the configuration files of the base cluster. In this file, find the SRG of the server to be removed.
   - -config: Required. Set this parameter to tianji_clt.conf.
2. After you run the preceding command, check whether the scale-in operation succeeds in Apsara Infrastructure Management Framework.

   Go to the Cluster Operation and Maintenance Center of the base cluster.
3. On the **Cluster Operation and Maintenance Center** page, check the number of servers that are being removed.
4. Click the number next to Machine: in: to identify the status of the servers that are being removed.

   If the scale-in operation succeeds, the number of servers that are being removed decreases to zero. Otherwise, check the server status on this page.

   You can follow the preceding steps to scale in a node cluster by moving servers to the default cluster in Apsara Infrastructure Management Framework. The following section describes how to remove servers from Apsara Infrastructure Management Framework.

Remove servers from Apsara Infrastructure Management Framework

1. In the top navigation bar, choose **Operations > Machine Operations**.

2. On the Machine Operations page that appears, click **Machine Online/Offline** in the upper-right corner.
3. In the Machine Online/Offline dialog box that appears, click Remove Machine.
4. On the Remove Machine tab, search for the server to be removed by hostname in the left-side Enter Machine List section. You can only remove servers in the default cluster.
5. Confirm the information of the server and click **Clear Machines** to remove it.

Verify the server removal result

1. Check whether the server is moved to the default cluster in Apsara Infrastructure Management Framework.

   In the top navigation bar, choose **Operations** > **Machine Operations**. On the Machine Operations page that appears, search for the target server by hostname and check whether it is in the default cluster.

2. Check whether the server is removed from the default cluster.

   In the top navigation bar, choose **Operations** > **Machine Operations**. On the Machine Operations page that appears, search for the server by hostname. If you cannot find the server in the search results, the server is removed.

3. To check whether the server is removed from the default cluster, run the following command on the ops1 server to call the GetMachineInfo operation:

   ```
   curl http://127.0.0.1:7070/api/v5/GetMachineInfo?hostname=$hostname
   ```

11.3.4.5. Restart the base-biz-tenant service

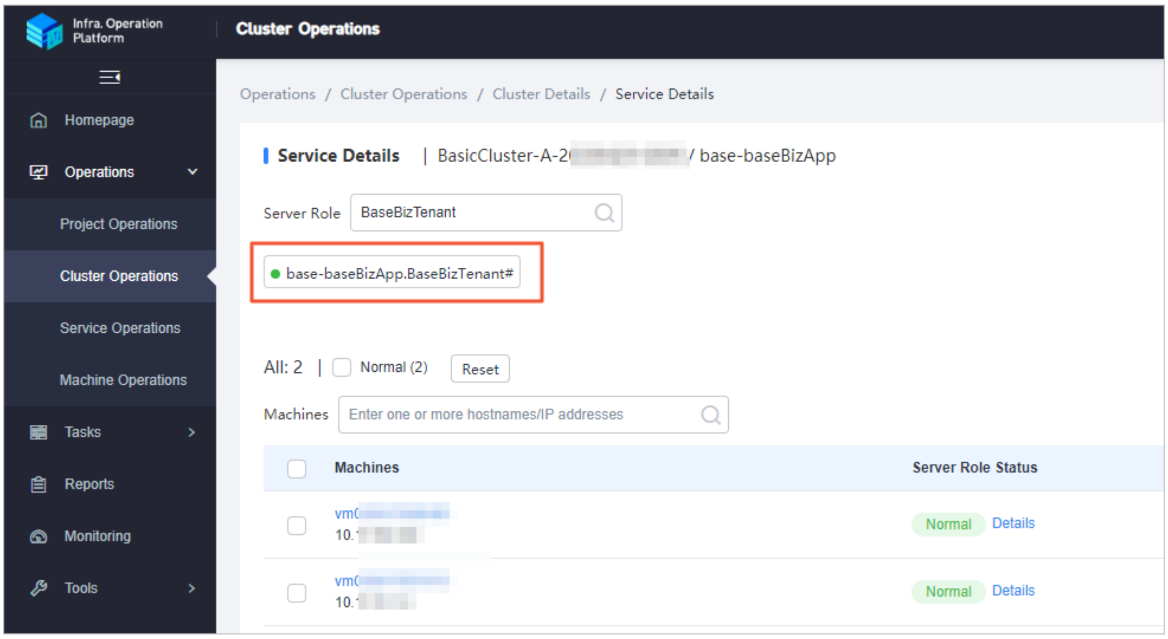
This topic describes how to go to the Service Details page and restart the base-biz-tenant service.

Go to the Service Details page

1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products** > **Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M** > **Basic O&M** > **Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
3. On the page that appears, select **base** from the **Project** drop-down list to filter clusters.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. Click the **base-baseBizApp** service. The **Service Details** page appears.

Restart the base-biz-tenant service

1. On the Service Details page, click the **base-baseBizApp.BaseBizTenant** service. You can also enter BaseBizTenant in the **Server Role** field to search for the target service.



Service Details | BasicCluster-A-2[redacted] / base-baseBizApp

Server Role: BaseBizTenant

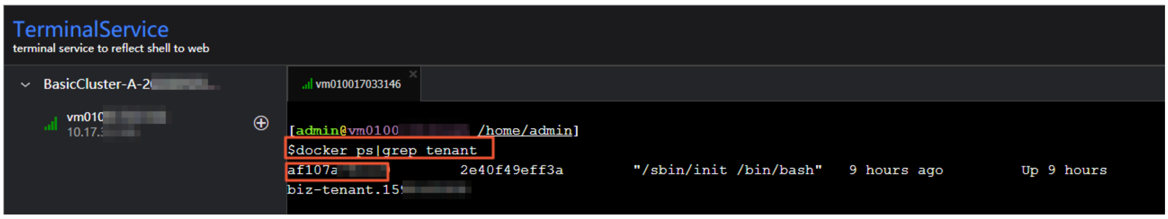
● base-baseBizApp.BaseBizTenant#

All: 2 | □ Normal (2)

Machines: Enter one or more hostnames/IP addresses

□	Machines	Server Role Status
□	vm0[redacted] 10.1[redacted]	Normal Details
□	vm0[redacted] 10.1[redacted]	Normal Details

2. Click the name of the target server. The Machine Details page appears.
3. Click **Terminal** in the upper-right corner of the page.
4. In the left-side navigation pane of the **TerminalService** page, click the server name. The configuration tab appears on the right-side of the page.
5. Enter `docker ps|grep tenant` and press Enter to view the ID of the server.

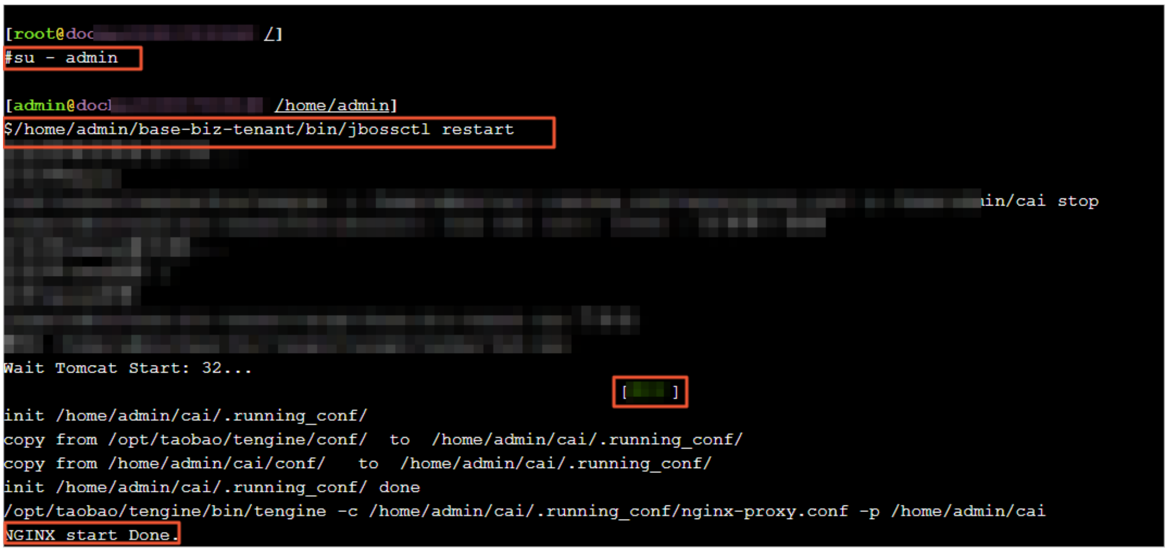

TerminalService
terminal service to reflect shell to web
BasicCluster-A-2[redacted]
vm010[redacted]
10.17.[redacted]
vm010017033146

```
[admin@vm0100[redacted] /home/admin]
$docker ps|grep tenant
af107a[redacted]          2e40f49eff3a        "/sbin/init /bin/bash"    9 hours ago         Up 9 hours
biz-tenant.15[redacted]
```

6. Enter `docker exec -it *yourID* bash` and press Enter to enter the corresponding container.

> **Note** The *yourID* parameter specifies the container ID.

7. Enter `su - admin` and press Enter to switch to the admin user.
8. Enter `/home/admin/base-biz-tenant/bin/jbossctl restart` and press Enter to restart the base-biz-tenant service.



```
[root@doc[redacted] /]
#su - admin

[admin@doc[redacted] /home/admin]
$/home/admin/base-biz-tenant/bin/jbossctl restart
[redacted]
[redacted]in/cai stop
[redacted]
Wait Tomcat Start: 32...
                                                        [ [redacted] ]
init /home/admin/cai/.running_conf/
copy from /opt/taobao/tengine/conf/  to  /home/admin/cai/.running_conf/
copy from /home/admin/cai/conf/   to  /home/admin/cai/.running_conf/
init /home/admin/cai/.running_conf/ done
/opt/taobao/tengine/bin/tengine -c /home/admin/cai/.running_conf/nginx-proxy.conf -p /home/admin/cai
NGINX start Done.
```

When the **OK** and **NGINX start Done** information appears, the base-biz-tenant service is restarted.

11.3.4.6. Restart the Redis services

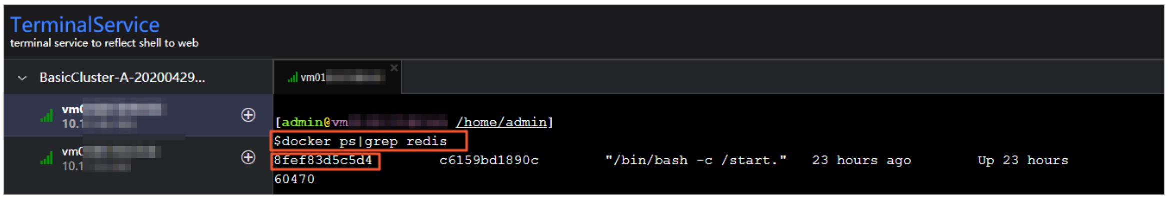
This topic describes how to go to the Service Details page and restart the Redis services.

Go to the Service Details page

1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products** > **Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M** > **Basic O&M** > **Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
3. On the page that appears, select **base** from the **Project** drop-down list to filter clusters.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. Click the **base-baseBizApp** service. The **Service Details** page appears.

Restart the Redis services

1. On the Service Details page, click the **base-baseBizApp.Redis1#** service.Redis services include Redis1 and redis2. This topic uses Redis1 as an example. You can also enter Redis in the **Server Role** field to search for the target service.
2. Click the name of the target server. The Machine Details page appears.
3. Click **Terminal** in the upper-right corner of the page.
4. In the left-side navigation pane of the **TerminalService** page, click the server name. The configuration tab appears on the right-side of the page.
5. Enter `docker ps|grep redis` and press Enter to view the ID of the server.



```
[admin@vm[redacted] /home/admin]
$docker ps|grep redis
8fef83d5c5d4        c6159bd1890c        "/bin/bash -c /start."   23 hours ago        Up 23 hours
60470
```

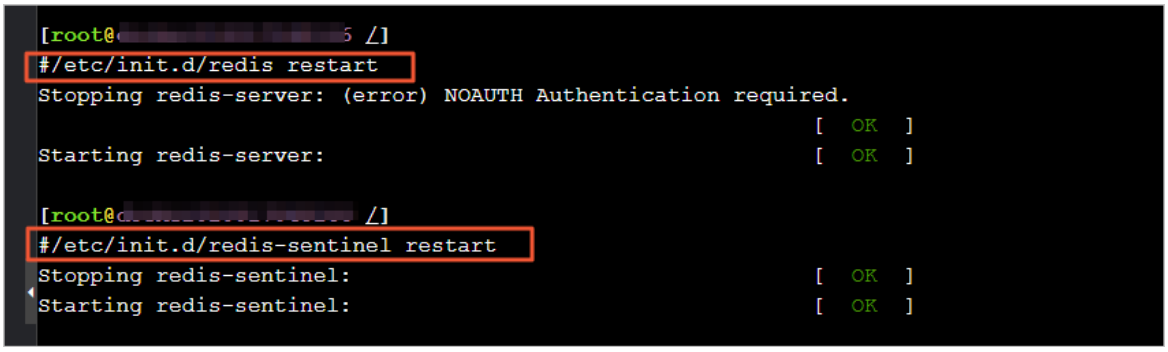
6. Enter `docker exec -it yourID bash` and press Enter to enter the corresponding container.

> Note The *yourID* parameter specifies the container ID.

7. Enter the following statements and press Enter to restart the Redis service:

```
/etc/init.d/redis restart
```

```
/etc/init.d/redis-sentinel restart
```



```
[root@[redacted] /]
#/etc/init.d/redis restart
Stopping redis-server: (error) NOAUTH Authentication required.
                                                           [  OK  ]
Starting redis-server:                                     [  OK  ]

[root@[redacted] /]
#/etc/init.d/redis-sentinel restart
Stopping redis-sentinel:                                   [  OK  ]
Starting redis-sentinel:                                   [  OK  ]
```

11.3.4.7. Restart the base-biz-dmc service

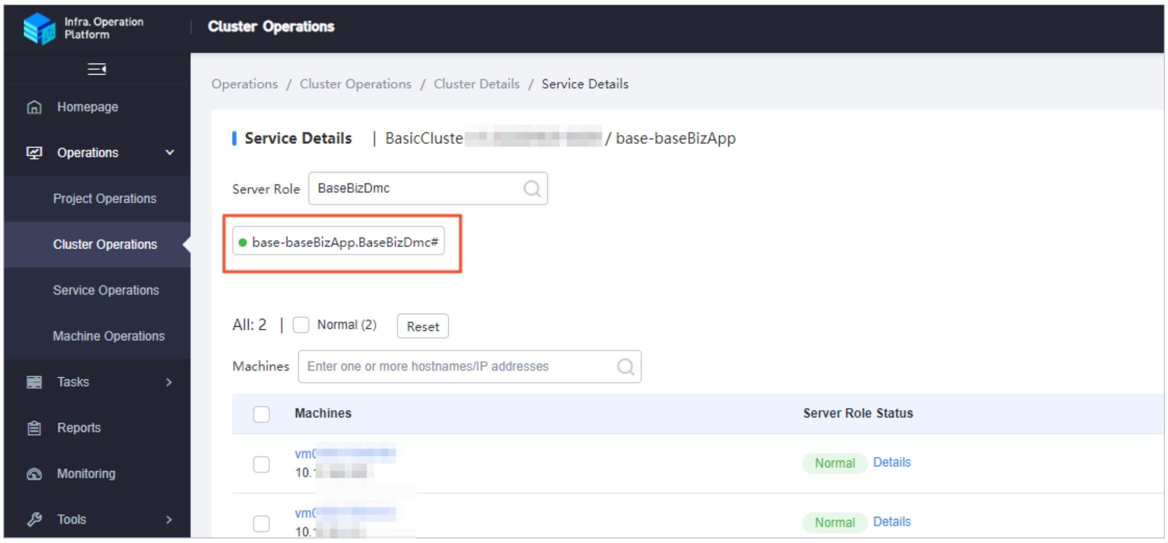
This topic describes how to go to the Service Details page and restart the base-biz-dmc service.

Go to the Service Details page

1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products > Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M > Basic O&M > Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, choose **Operations > Cluster Operations**.
3. On the page that appears, select **base** from the **Project** drop-down list to filter clusters.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. Click the **base-baseBizApp** service. The **Service Details** page appears.

Restart the base-biz-dmc service

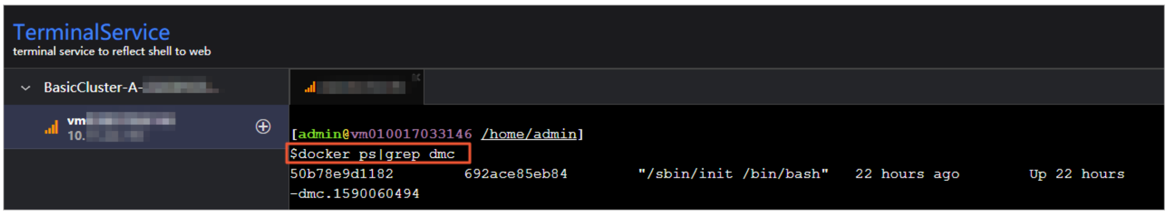
1. On the Service Details page, click the **base-baseBizApp.BaseBizDmc** service.You can also enter BaseBizDmc in the **Server Role** field to search for the target service.


Infra. Operation Platform
Cluster Operations
Homepage
Operations
Project Operations
Cluster Operations
Service Operations
Machine Operations
Tasks
Reports
Monitoring
Tools
Operations / Cluster Operations / Cluster Details / Service Details
Service Details | BasicCluste[redacted] / base-baseBizApp
Server Role
base-baseBizApp.BaseBizDmc#
All: 2 | □ Normal (2) Reset
Machines
Enter one or more hostnames/IP addresses
□ Machines
Server Role Status
Details
Details

Server Role: BaseBizDmc

□	Machines	Server Role Status
□	vm[redacted] 10.[redacted]	Normal Details
□	vm[redacted] 10.[redacted]	Normal Details

2. Click the name of the target server. The Machine Details page appears.
3. In the left-side navigation pane of the **TerminalService** page, click the server name. The configuration tab appears on the right-side of the page.
4. Enter `docker ps|grep dmc` and press Enter to view the ID of the server.

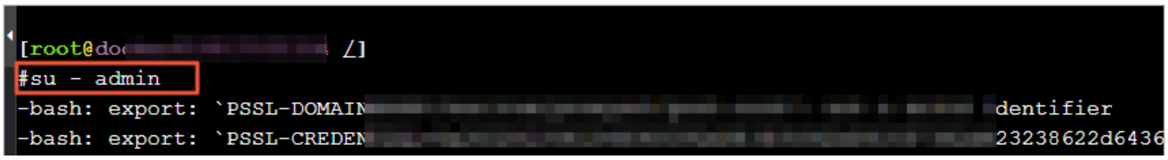

TerminalService
terminal service to reflect shell to web
BasicCluster-A-[redacted]
vm[redacted]
10.[redacted]

```
[admin@vm010017033146 /home/admin]
$docker ps|grep dmc
50b78e9d1182        692ace85eb84        "/sbin/init /bin/bash"   22 hours ago        Up 22 hours
-dmc.1590060494
```

5. Enter `docker exec -it *yourID* bash` and press Enter to enter the corresponding container.

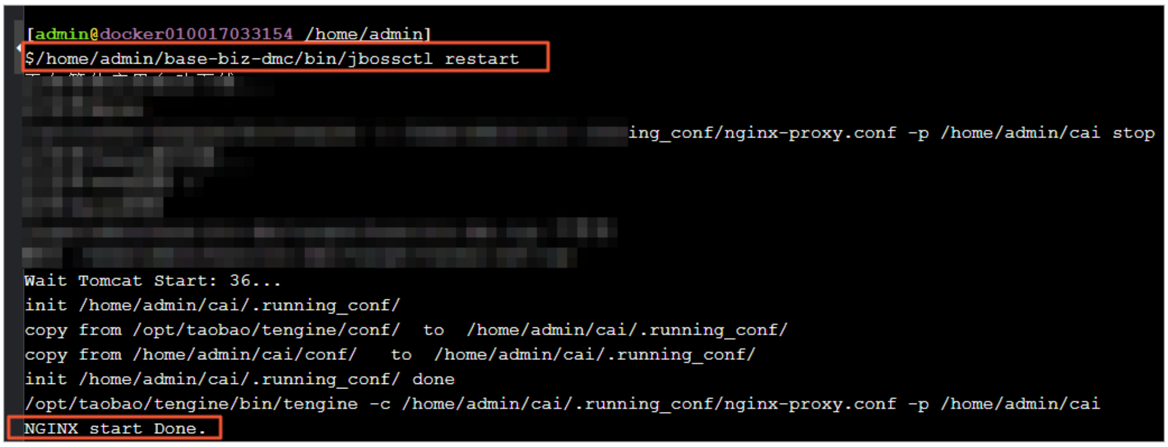
> **Note** The *yourID* parameter specifies the container ID.

6. Enter `su - admin` and press Enter to switch to the admin user.



```
[root@do[redacted] /]
#su - admin
-bash: export: `PSSL-DOMAIN[redacted]dentifier
-bash: export: `PSSL-CREDEN[redacted]23238622d6436
```

7. Enter `/home/admin/base-biz-dmc/bin/jbossctl restart` and press Enter to restart the base-biz-dmc service.



```
[admin@docker010017033154 /home/admin]
$/home/admin/base-biz-dmc/bin/jbossctl restart
[redacted]ing_conf/nginx-proxy.conf -p /home/admin/cai stop
Wait Tomcat Start: 36...
init /home/admin/cai/.running_conf/
copy from /opt/taobao/tengine/conf/  to  /home/admin/cai/.running_conf/
copy from /home/admin/cai/conf/   to  /home/admin/cai/.running_conf/
init /home/admin/cai/.running_conf/ done
/opt/taobao/tengine/bin/tengine -c /home/admin/cai/.running_conf/nginx-proxy.conf -p /home/admin/cai
NGINX start Done.
```

When the **OK** and **NGINX start Done** information appears, the base-biz-dmc service is restarted.

11.3.4.8. Restart the base-biz-alisa service

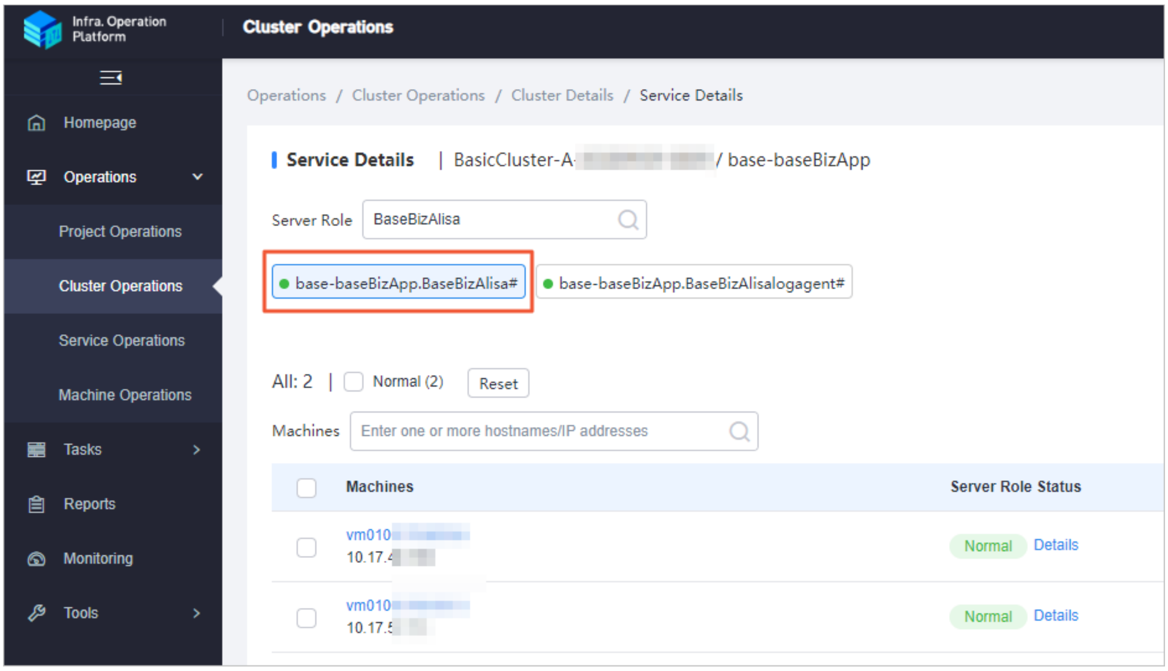
This topic describes how to go to the Service Details page and restart the base-biz-alisa service.

Go to the Service Details page

1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products** > **Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M** > **Basic O&M** > **Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, choose **Operations** > **Cluster Operations**.
3. On the page that appears, select **base** from the **Project** drop-down list to filter clusters.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. Click the **base-baseBizApp** service. The **Service Details** page appears.

Restart the base-biz-alisa service

1. On the Service Details page, click the **base-baseBizApp.BaseBizAlisa** service. You can also enter BaseBizAlisa in the **Server Role** field to search for the target service.



Service Details | BasicCluster-A[redacted] / base-baseBizApp

Server Role: BaseBizAlisa

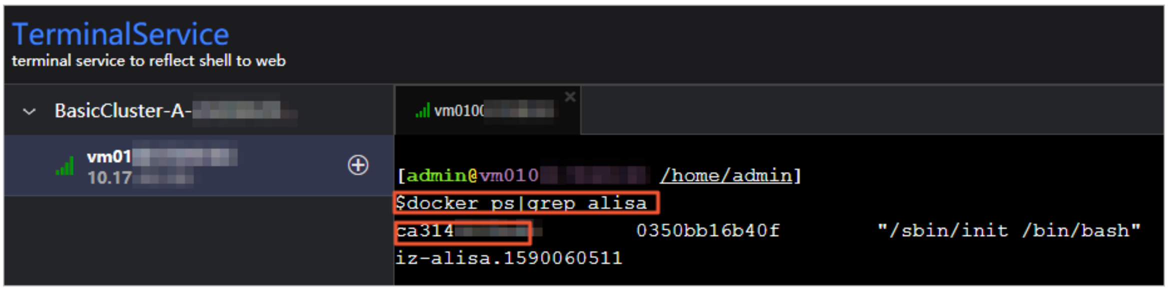
● base-baseBizApp.BaseBizAlisa# ● base-baseBizApp.BaseBizAlisalogagent#

All: 2 | □ Normal (2) Reset

Machines: Enter one or more hostnames/IP addresses

□	Machines	Server Role Status	
□	vm010[redacted] 10.17.[redacted]	Normal	Details
□	vm010[redacted] 10.17.[redacted]	Normal	Details

2. Click the name of the target server. The Machine Details page appears.
3. Click **Terminal** in the upper-right corner of the page.
4. In the left-side navigation pane of the **TerminalService** page, click the server name. The configuration tab appears on the right-side of the page.
5. Enter `docker ps|grep alisa` and press Enter to view the ID of the server.

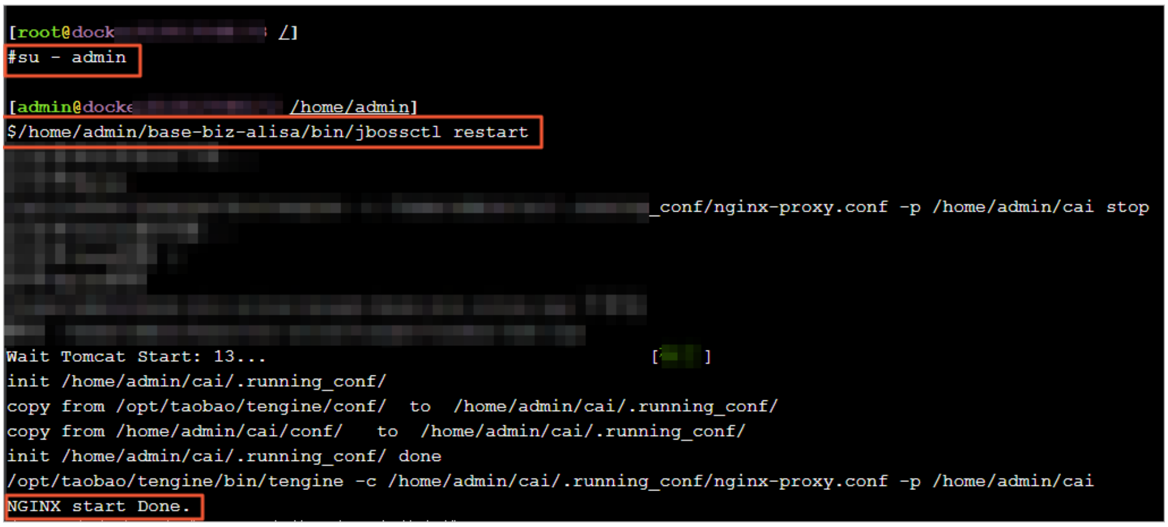

TerminalService
terminal service to reflect shell to web
BasicCluster-A-[redacted]
vm01[redacted]
10.17[redacted]
vm010[redacted]

```
[admin@vm010[redacted] /home/admin]
$docker ps|grep alisa
ca314[redacted]          0350bb16b40f        "/sbin/init /bin/bash"
iz-alisa.1590060511
```

6. Enter `docker exec -it yourID bash` and press Enter to enter the corresponding container.

> **Note** The *yourID* parameter specifies the container ID.

7. Enter `su - admin` and press Enter to switch to the admin user.
8. Enter `/home/admin/base-biz-alisa/bin/jbossctl restart` and press Enter to restart the base-biz-alisa service. When the **OK** and **NGINX start Done** information appears, the base-biz-alisa service is started.



```
[root@dock[redacted] /]
#su - admin

[admin@docke[redacted] /home/admin]
$/home/admin/base-biz-alisa/bin/jbossctl restart
[redacted]
[redacted]_conf/nginx-proxy.conf -p /home/admin/cai stop
[redacted]
Wait Tomcat Start: 13...                                   [[redacted]]
init /home/admin/cai/.running_conf/
copy from /opt/taobao/tengine/conf/  to  /home/admin/cai/.running_conf/
copy from /home/admin/cai/conf/   to  /home/admin/cai/.running_conf/
init /home/admin/cai/.running_conf/ done
/opt/taobao/tengine/bin/tengine -c /home/admin/cai/.running_conf/nginx-proxy.conf -p /home/admin/cai
NGINX start Done.
```

11.3.4.9. Restart the base-biz-phoenix service

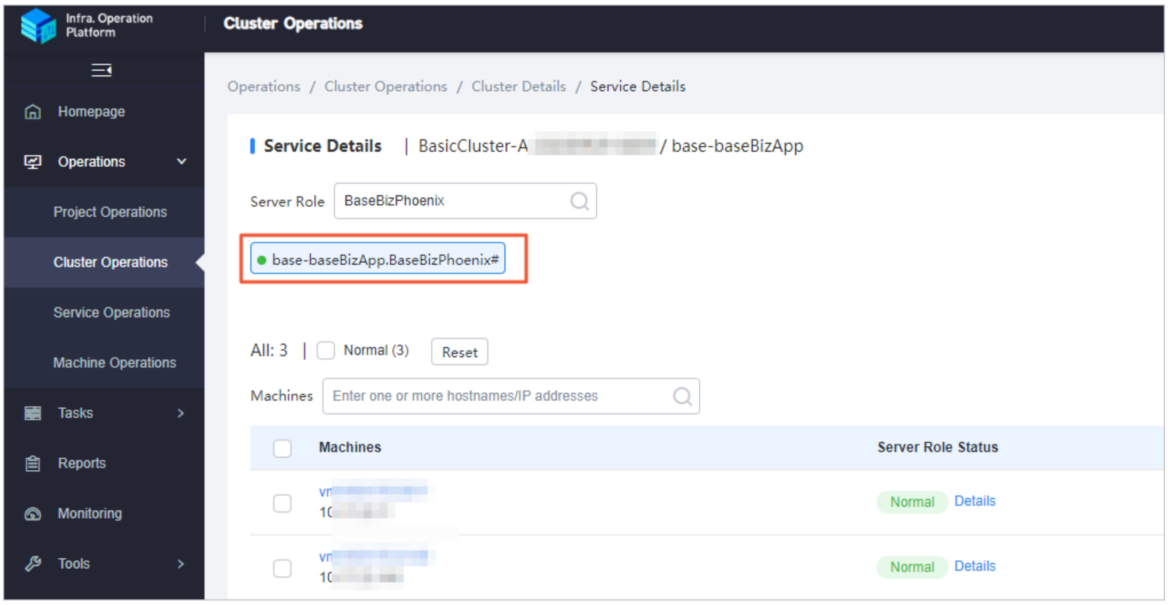
This topic describes how to go to the Service Details page and restart the base-biz-phoenix service.

Go to the Service Details page

1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products > Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M > Basic O&M > Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, choose **Operations > Cluster Operations**.
3. On the page that appears, select **base** from the **Project** drop-down list to filter clusters.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. Click the **base-baseBizApp** service. The **Service Details** page appears.

Restart the base-biz-phoenix service

1. On the Service Details page, click the **base-baseBizApp.BaseBizPhoenix** service. You can also enter BaseBizPhoenix in the **Server Role** field to search for the target service.



Service Details | BasicCluster-A[redacted] / base-baseBizApp

Server Role: BaseBizPhoenix

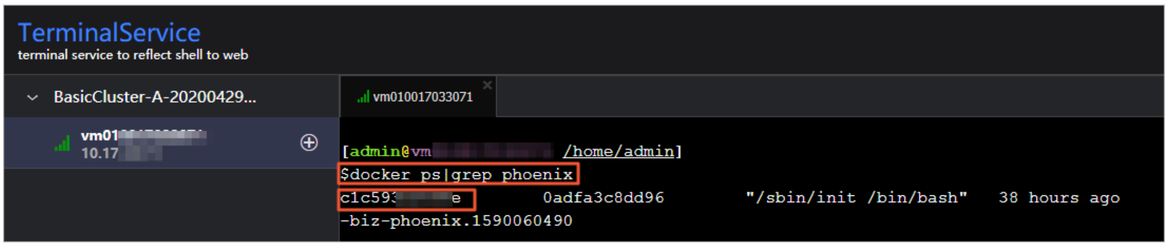
● base-baseBizApp.BaseBizPhoenix#

All: 3 | □ Normal (3)

Machines: Enter one or more hostnames/IP addresses

□	Machines	Server Role Status
□	vm[redacted] 10[redacted]	Normal Details
□	vm[redacted] 10[redacted]	Normal Details

2. Click the name of the target server. The Machine Details page appears.
3. Click **Terminal** in the upper-right corner of the page.
4. In the left-side navigation pane of the **TerminalService** page, click the server name. The configuration tab appears on the right-side of the page.
5. Enter `docker ps|grep phoenix` and press Enter to view the ID of the server.

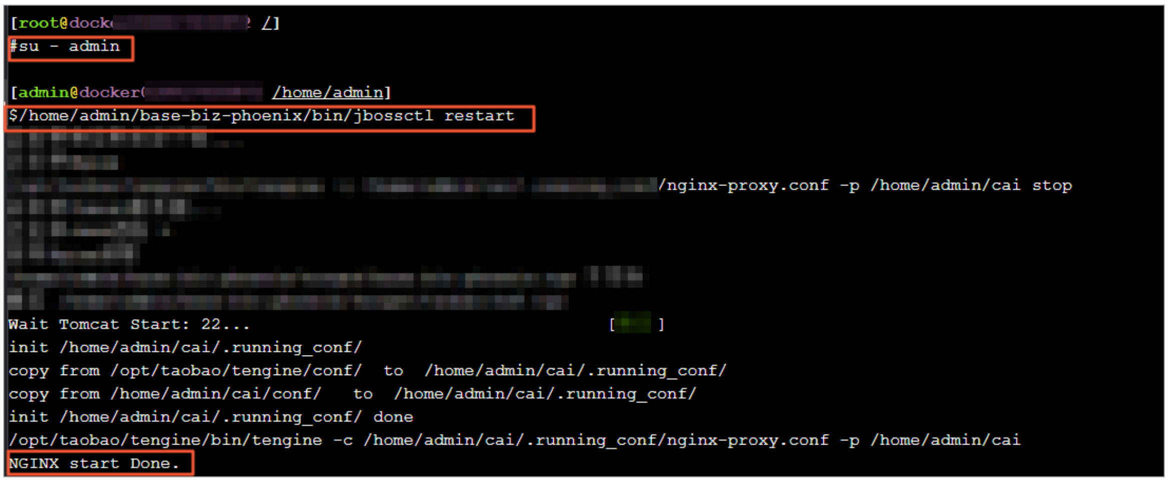

TerminalService
terminal service to reflect shell to web
BasicCluster-A-20200429...
vm01[redacted]
10.17[redacted]
vm010017033071

```
[admin@vm[redacted] /home/admin]
$docker ps|grep phoenix
c1c59[redacted]e         0adfa3c8dd96         "/sbin/init /bin/bash"    38 hours ago
-biz-phoenix.1590060490
```

6. Enter `docker exec -it yourID bash` and press Enter to enter the corresponding container.

> **Note** The *yourID* parameter specifies the container ID.

7. Enter `su - admin` and press Enter to switch to the admin user.
8. Enter `/home/admin/base-biz-phoenix/bin/jbossctl restart` and press Enter to restart the base-biz-phoenix service.



```
[root@dock[redacted] /]
#su - admin

[admin@docker([redacted] /home/admin]
$/home/admin/base-biz-phoenix/bin/jbossctl restart
[redacted]
[redacted] /nginx-proxy.conf -p /home/admin/cai stop
[redacted]

[redacted]
Wait Tomcat Start: 22...                              [ [redacted] ]
init /home/admin/cai/.running_conf/
copy from /opt/taobao/tengine/conf/  to  /home/admin/cai/.running_conf/
copy from /home/admin/cai/conf/   to  /home/admin/cai/.running_conf/
init /home/admin/cai/.running_conf/ done
/opt/taobao/tengine/bin/tengine -c /home/admin/cai/.running_conf/nginx-proxy.conf -p /home/admin/cai
NGINX start Done.
```

When the **OK** and **NGINX start Done** information appears, the base-biz-phoenix service is started.

11.3.4.10. Restart the base-biz-gateway service

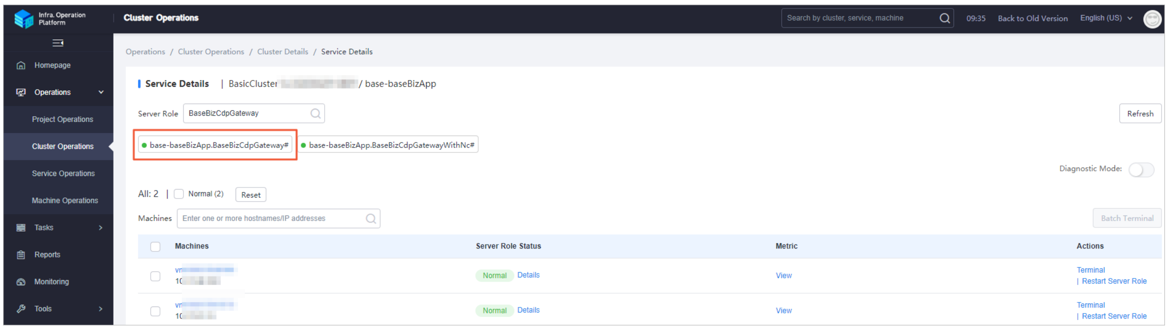
This topic describes how to go to the Service Details page and restart the base-biz-gateway service.

Go to the Service Details page

1. Log on to Apsara Infrastructure Management Framework.
   i. Log on to the ABM console.
   ii. In the left-side navigation pane, choose **Products > Product List**.
   iii. On the page that appears, choose **Apsara Stack O&M > Basic O&M > Apsara Infrastructure Management Framework**.
2. In the left-side navigation pane, choose **Operations > Cluster Operations**.
3. On the page that appears, select **base** from the **Project** drop-down list to filter clusters.
4. Click the name of the target cluster. The **Cluster Details** page appears.
5. Click the **base-baseBizApp** service. The **Service Details** page appears.

Restart the base-biz-gateway service

1. On the Service Details page, click the **base-baseBizApp.BaseBizCdpGateway** service. You can also enter BaseBizCdpGateway in the **Server Role** field to search for the target service.



Operations / Cluster Operations / Cluster Details / Service Details

Service Details | BasicCluster[redacted] / base-baseBizApp

Server Role BaseBizCdpGateway

● base-baseBizApp.BaseBizCdpGateway# ● base-baseBizApp.BaseBizCdpGatewayWithNc#

All: 2 | □ Normal (2)

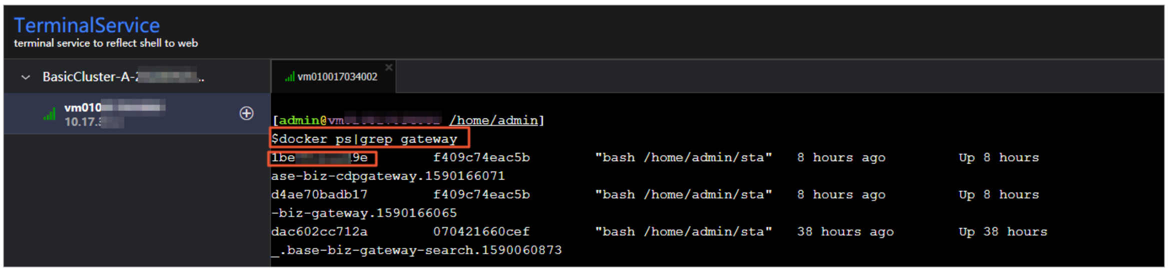
Machines Enter one or more hostnames/IP addresses

□	Machines	Server Role Status	Metric	Actions
□	vr[redacted] 1([redacted]	Normal Details	View	Terminal | Restart Server Role
□	vr[redacted] 1([redacted]	Normal Details	View	Terminal | Restart Server Role

2. Click the name of the target server. The Machine Details page appears.
3. Click **Terminal** in the upper-right corner of the page.
4. In the left-side navigation pane of the **TerminalService** page, click the server name. The

configuration tab appears on the right-side of the page.

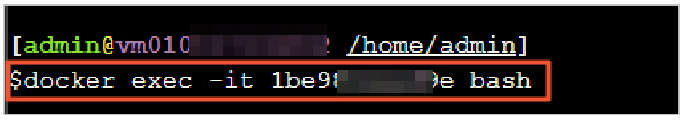
5. Enter `docker ps|grep gateway` and press Enter to view the ID of the server.


TerminalService
terminal service to reflect shell to web
BasicCluster-A-[redacted]..
vm010[redacted]
10.17.[redacted]
vm010017034002

```
[admin@vm[redacted] /home/admin]
$docker ps|grep gateway
1be[redacted]9e         f409c74eac5b        "bash /home/admin/sta"   8 hours ago         Up 8 hours
ase-biz-cdpgateway.1590166071
d4ae70badb17         f409c74eac5b        "bash /home/admin/sta"   8 hours ago         Up 8 hours
-biz-gateway.1590166065
dac602cc712a         070421660cef        "bash /home/admin/sta"   38 hours ago        Up 38 hours
_.base-biz-gateway-search.1590060873
```

6. Enter `docker exec -it *yourID* bash` and press Enter to enter the corresponding container.

> **Note** The *yourID* parameter specifies the container ID.



```
[admin@vm010[redacted] /home/admin]
$docker exec -it 1be9[redacted]9e bash
```

7. Enter `su - admin` and press Enter to switch to the admin user.
8. Enter `/home/admin/alisatasknode/target/alisatasknode/bin/serverctl restart` and press Enter to restart the base-biz-gateway service.

11.3.4.11. Restart DataWorks Data Service

Procedure

1. In the Apsara Infrastructure Management Framework console, search for dataworks-dataservice on the S tab.
2. Hover over the vertical dots next to BasicCluster, and then click Operations to open the Operations page to view the details of dataworks-dataservice.
3. Click the service instance name to open Service Instance Dashboard, and then find Service Role List.
4. If you want to restart the server, select BaseBizDataServiceServer#. If you want to restart the Web application, select BaseBizDataServiceWeb#. Hover over the vertical dots next to the service name, and then click **Details** to open the Service Role Dashboard page, and then find the virtual machine in the Server Information area.
5. Open the terminal window of the VM host, and run the `docker ps|grep dataservice` command to find the container ID.
6. Run the `docker exec -it [container ID] bash` command to enter the container.
7. Switch to the admin account, and run the `/home/admin/data-service-web/bin/jbossctl restart` command to restart the service.

   If you are restarting the server, run the `/home/admin/data-service-server/bin/jbossctl restart` command.
8. After you run the command, if the status is **OK** and the command output displays [OK] -- SUCCESS at the end, the dataservice service is restarted successfully.

11.3.4.12. Restart base-biz-gateway

Procedure

1. In the Apsara Infrastructure Management Framework console, select base from the project drop-down list and then select BasicCluster from the search result.
2. On the Service tab in the lower part of the left-side navigation pane, double-click base-baseBizApp, double-click BaseBizCdpGateway, and then the host that runs the service appears.
3. Open the terminal window of the host, and run the `docker ps|grep gateway` command to find the container ID.
4. Run the `docker exec -it [container ID] bash` command to enter the container.
5. Switch to the admin account, and run the `/home/admin/alisatasknode/target/alisatasknode/bin/serverctl restart` command to restart the service.
6. After the service is restarted, run the `ps -ef|grep java` command to check whether the process is started.

   > ⓘ **Note** This method can only be used where the gateway service is deployed in a Docker container.

For the service deployed on a physical server

If the service is deployed on a physical server, use the following method to restart the service.

1. In the Apsara Infrastructure Management Framework console, open the Dashboard page of BasicCluster. In the cluster resource list, find and right-click the base-biz-alisa service that has a type of db, and then click Show More. The database logon address, username, and password are displayed.
2. Run the `select * from alisa_node;` command in the database to view the information of all gateway servers, and use the node IP address to find and maintain the gateway server.
3. In the terminal window of the server, switch to the admin account, and then run the `/home/admin/alisatasknode/target/alisatasknode/bin/serverctl restart` command.

11.3.4.13. Configure a resource group in a multi-region environment

In a multi-region environment, nodes in all regions are run on the resource group named sys_default in the central region by default. This is the cause of resource preemption and node backlog. To resolve the issues, you must isolate resources and enable level-1 scheduling nodes in your region to run on your own resource groups.

Prerequisites

- Idle Elastic Compute Service (ECS) instance resources are available in a region rather than the central region. You can view the idle resources in the Apsara Infrastructure Management Framework console.
- Resource groups are created in DataWorks and resources are isolated.
- A custom resource group is specified as the default resource group in your workspace.
- Historical nodes that are run on the original default resource group are migrated to the new resource group. This is a high-risk operation.

Create a resource group

1. Go to the Schedule Resources page in DataWorks.
   i. Log on to the DataWorks console.
   ii. Click the ≡ icon in the upper-left corner and choose **All Products** > **Project Management**.
   iii. In the left-side navigation pane, click **Schedule Resources**.
2. On the **Schedule Resources** page, click **Add scheduling resources** in the upper-right corner.
3. In the **Add scheduling resources** dialog box, set the **Resource Name** and **Belonging workspace** parameters.In this example, the resource name is region_test. The resource group belongs to a tenant that is a level-1 department. All workspaces that are created by the tenant can use this resource group, whereas other tenants need to create their own resource groups.

   After a resource group is created, a cluster that corresponds to the resource group is also created. In the background database, you can view the resource group in the alisa_group table and view the cluster in the alisa_cluster table.
4. Click **Confirm**.After you create the resource group, you can log on to the dpbizalisa background database to view detailed information about the resource group and cluster.

```
select group_name,group_display_name,cluster_name,max_slot where group_display_name='xxxx';
select cluster_name,username,password from alisa_cluster where cluster_name ='xxxx';
// max_slot: the number of slots that are assigned to the current resource group. The number is determined based on actual resources and requirements. You must set the number of slots to a proper value.
// group_display_name: the name of the custom resource group.
// cluster_name: the name of the cluster that corresponds to the custom resource group.
```

Migrate ECS instances to a new cluster

1. To migrate an ECS instance, run the following command:

```
update alisa_node set cluster_name='xxxxxx' where node_name='${hostname}';
```

2. To set the number of slots in the resource group to a proper value, run the following command:

```
update alisa_group set max_slot = xxxx where group_display_name='region_test';
```

3. Restart the base-biz-alisa service. For more information, see Restart the base-biz-alisa service.

   Note Both base-biz-alisa services need to be restarted. After one base-biz-alisa service is restarted, you can restart the other.

Specify the custom resource group as the default resource group in your workspace

1. Log on to the dwphoenix background database to view data.

```
select resource_group_id,name,identifier,is_default,project_env from phoenix_resgroup where name = 'region_test';
// resource_group_id: the ID of the resource group in the phoenix database.
// name: the name of the resource group.
// identifier: the name of the resource group in the alisa database.
// project_env: the production environment or the development environment.
select * from phoenix_app_resgroup where app_id=xxxx;
// app_id: the ID of the project. The app_id parameter is equivalent to the project_id parameter that is described in other topics.
```

2. Specify a new resource group as the default resource group in your workspace.

```
create table phoenix_app_resgroup_20200108_bak as select * from phoenix_app_resgroup; // Back up the table.
update phoenix_app_resgroup set is_default=1 where is_default=0 and app_id=xxxx;
update phoenix_app_resgroup set is_default=0 where app_id=xxxx and resource_group_id=1;
select * from phoenix_app_resgroup where app_id=xxxx; // View data again after the change.
```

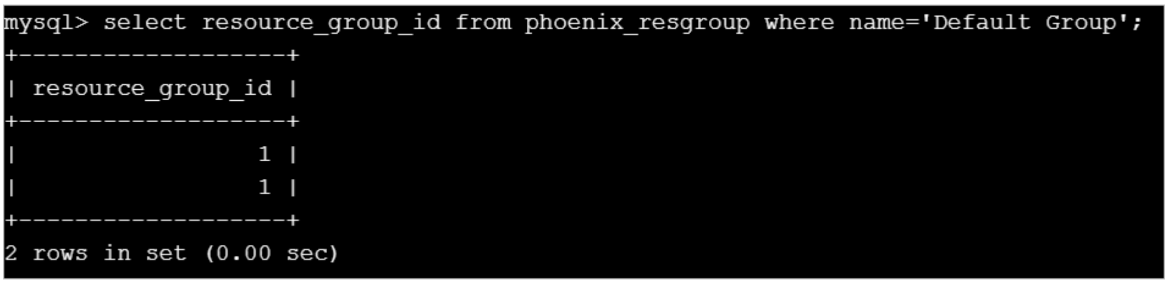
> **Note** After the change, one workspace has only two data entries whose is_default value is 1. If the preceding result is not displayed, the change is invalid. You must check the operations you have performed.
>
> The resource group belongs to a tenant so that you must change the default resource group for all workspaces that are created by the tenant.

Change the resource group for multiple nodes at a time

You can change the resource group for multiple nodes at a time on the Operation Center page. If a large number of nodes exist, you must perform the change operation multiple times on the page until the resource group is changed for all the nodes. If you do not want to change the resource group in that way, you can change the resource group for all the nodes at a time in the scheduled database. However, this is a high-risk operation. To change the resource group in the database, you must perform the operations based on your business requirements. You must write the code based on the data in the current environment by following the template. In this example, the resource group for nodes in the datam4 workspace is changed to the resource group named region_test in the following way:

1. Log on to the dwphoenix database that corresponds to the base-biz-phoenix service.
2. Query the ID of the resource group named sys_default. The obtained value is used as the default ID.

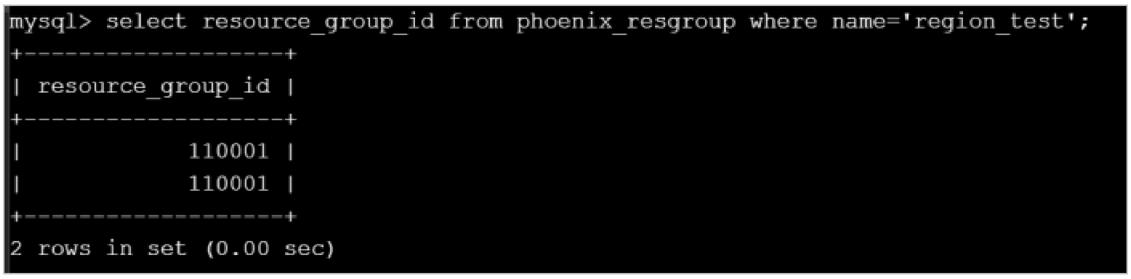
```
select resource_group_id from phoenix_resgroup where name='Default Group';
```



```
mysql> select resource_group_id from phoenix_resgroup where name='Default Group';
+-------------------+
| resource_group_id |
+-------------------+
|                 1 |
|                 1 |
+-------------------+
2 rows in set (0.00 sec)
```

3. Query the ID of the resource group named region_test. The obtained value is used as the region_test_id value.

```
select resource_group_id from phoenix_resgroup where name='region_test';
```



```
mysql> select resource_group_id from phoenix_resgroup where name='region_test';
+-------------------+
| resource_group_id |
+-------------------+
|            110001 |
|            110001 |
+-------------------+
2 rows in set (0.00 sec)
```

4. Query the ID of the required workspace. The obtained value is used as the app_id value.

```
select app_id from phoenix_app_config where name="datam4";
```

5. Change the resource group for historical nodes in the workspace that you want to change to the new resource group named region_test.

```
create table phoenix_node_def_20200108_bak as select * from phoenix_node_def; // Back up the table.
update phoenix_node_def set resgroup_id={region_test_id} where resource_group_id={Default ID} and app_id={app_id};
```

   This way, the resource group for historical nodes in the datam4 workspace is changed to the resource group named region_test. After the resource group is changed, test whether all the historical nodes can be run as expected.

11.3.4.14. Configure a resource group for Data Integration in a multi-region environment

This topic describes how to configure a resource group for Data Integration in a multi-region environment.

Procedure

1. On the Data Integration page in DataWorks, create a custom resource group.This custom resource group must be real and can be used. In this example, you can specify the Elastic Compute Service (ECS) instance on which the region_group custom resource group is hosted as the default ECS instance to run nodes.
   i. Log on to the DataWorks console.
   ii. Click the ≡ icon in the upper-left corner and choose **All Products > Data Aggregation > Data Integration**.
   iii. In the left-side navigation pane, click **Custom Resource Group**.
   iv. Click **Add Resource Group** in the upper-right corner.
2. In the **Add Resource Group** wizard, perform the following steps:
   i. In the **Create Resource Group** step, set the **Resource Group Name** parameter.

      > ? **Note** The name can contain letters, digits, and underscores (_), and must start with a letter.

ii. Click **Next**.

iii. In the **Add Server** step, set the parameters as required.

iv. Click **Next**.

v. Perform the steps that are described in the **Install Agent** step.

> Note If an error occurs when you run the `install.sh` command or you need to run it again, run the `rm -rf install.sh` command in the same directory as the `install.sh` command to delete the generated file. Then, run the `install.sh` command again.
>
> The commands to run during the installation and initialization process differ for each user. Run relevant commands based on the instructions on the initialization interface.

vi. Click **Next**.

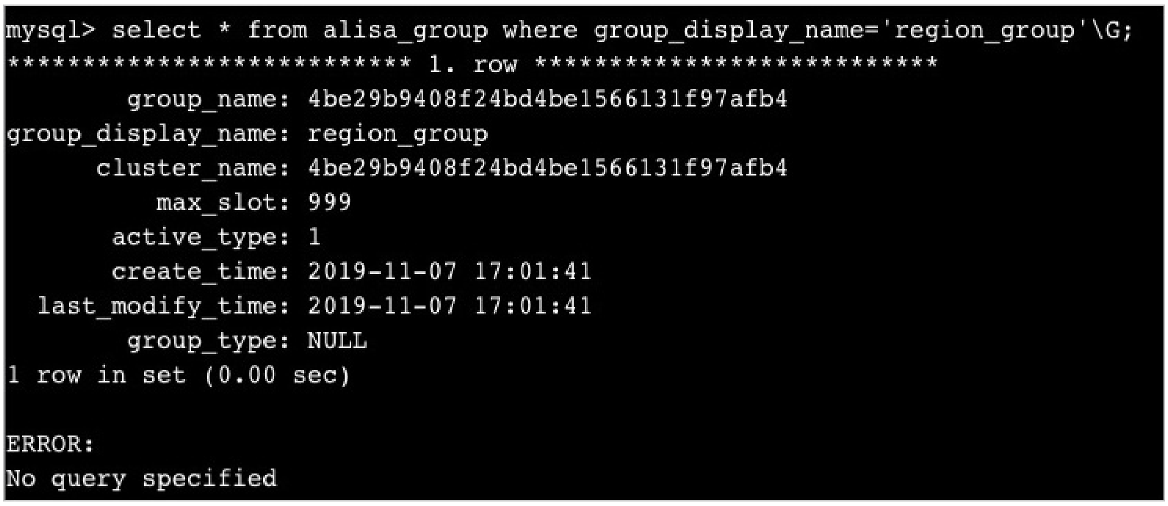
vii. In the **Test Connection** step, click **Refresh** and check the status of the ECS instance.

viii. Click **Complete**.

Resource groups that you have created on the Data Integration page can be used only in workspaces to which they belong. If you create a resource group in Workspace A, this resource group cannot be used in Workspace B. If you need to use a resource group in Workspace B, perform the preceding steps to create one in Workspace B.

3. View the newly created resource group in the alisa database.

```
select * from alisa_group where group_display_name='region_group'\G;
```



```
mysql> select * from alisa_group where group_display_name='region_group'\G;
*************************** 1. row ***************************
        group_name: 4be29b9408f24bd4be1566131f97afb4
group_display_name: region_group
      cluster_name: 4be29b9408f24bd4be1566131f97afb4
          max_slot: 999
       active_type: 1
       create_time: 2019-11-07 17:01:41
  last_modify_time: 2019-11-07 17:01:41
        group_type: NULL
1 row in set (0.00 sec)

ERROR:
No query specified
```

4. Create an alisa cluster.To deploy services in a new region, you must first create an alisa cluster. You can find the dpbizalisa database and execute the following SQL statements in this database:

```
insert ignore into alisa_cluster(
 cluster_name,
 cluster_display_name,
 username,
 password,
 create_time,
 last_modify_time
 )
 values(
 'sys_region_cdp_${regionId}',
 'sys_region_cdp_${regionId}',
 'private_cluster',
 'tyn3n71c2oyhah447m6fnfuq',
 now(),
 now()
 );
```

Replace ${regionId} in the code with an actual value. You can log on to the Apsara Infrastructure Management Framework console and go to the **Cluster Configuration** tab to view the cluster file.

5. Migrate the ECS instance that you have bound to the custom resource group to this cluster.

```
update alisa_node set cluster_name='sys_region_cdp_${regionId}' where node_name='ECS instance name';
```

> **Note** You must check the name of the ECS instance in the current region.

6. Mount the cluster that is created in this region to the resource group.

```
update alisa_group set cluster_name='sys_region_cdp_${regionId}' where group_name='4be29b9408f24bd4be1566131f97afb4';
```

In the code, group_name indicates the resource group name that is specified in Step 2.

7. Log on to the Apsara Infrastructure Management Framework console and restart the BaseBizAlisa service.

8. On the configuration tab of a sync node, select the name of the required custom resource group, and save and commit the node.The preceding steps describe how to create a resource group in a region for the first time. If you need to create resource groups for multiple workspaces, repeat steps 1, 2, 3, 6, and 7 to create resource groups as required.

To perform the rollback operation, run the following command:

```
update alisa_group set cluster_name='4be2***' where group_name='4be2***';
```

> **Note** group_name and cluster_name indicate the name and cluster name of the custom resource group.

11.3.5. Common issues and solutions

11.3.5.1. Nodes remain in the Pending (Resources) state

Symptom

After you log on to the DataWorks console and click **Operation Center** in the upper-right corner of the console, the following issue occurs on the **Dashboard** page that appears: The instances of many recurring nodes remain in the Pending (Resources) state for a long period of time.

Causes

The issue may occur due to any one of the following four reasons:

- A gateway server is overloaded or offline and its status value is -1 in the database.
- The slots that handle concurrent jobs are fully occupied.
- The disk on a gateway server is full.
- The system time of servers in the base cluster is out of sync with the time of the Network Time Protocol (NTP) server.

Solutions

To resolve this issue, follow these steps:

- Check the status of a gateway server in the database.

  i. Log on to the database that hosts the base-biz-alisa service. In Apsara Stack V3, you can find the database endpoint from the resource list of the base cluster in Apsara Infrastructure Management Framework.

  ii. Run the `select * from alisa_node;` command to check the values of the active_type and live fields.

     If the value of the live field is -1, the server is offline. If the value of the active_type field is -1, the server is overloaded.

     > **Note** In either case, use SSH to connect to the gateway server and then check the server load and heartbeat.
     >
     > ■ Run the `tail -f/home/admin/alisatasknode/logs/heartbeat.log` command to check the heartbeat of the gateway server.
     >
     > If the heartbeat log is updated every five seconds, the heartbeat is normal. Otherwise, check the configuration files for an error.
     >
     > ■ Run the top command to display the load of the gateway server.
     >
     > The status of the server becomes -1 in the database as a result of the high load. In this case, check whether the CPU and memory are overloaded. You can find out the high-load processes in the output of the top command.
     >
     > You can run the `ps -ef|greppid` command to view processes of the specified node and identifv which process causes the high load. To terminate a process, run the `kill -9 [process ID]` command. After the load drops, check whether the status of the server resumes to 1.

- Check whether the slots that handle concurrent jobs are fully occupied.

Log on to the database that hosts the base-biz-alisa service and run the following statements:

```
select group_name,max_slot from alisa_group where group_name like '%default%';
select exec_target,sum(slot) from alisa_task where status=2 group by exec_target;
```

Compare the query results of the two statements.

- The first statement returns the maximum number of slots that can be assigned in each resource group.
- The second statement returns the number of slots that are occupied in each resource group.

If the query results of the two statements are the same or almost the same, all resource groups run out of slots. In this case, if a large number of nodes are running, the subsequent nodes do not run until the preceding nodes are completed.

Run the following statement to list the top 10 nodes that require the longest runtime:

```
select task_id,gateway,slot,create_time from alisa_task where status=2 and create_time>current_time order by create_time desc limit 10;
```

Log on to the gateway server and run the `ps -ef|grep task_id` command.

> **Note** Replace task_id in this command with one of the node IDs that are returned by the preceding SELECT statement. You can obtain the node name from the command output.

Then, you can troubleshoot the node. If required, run the `kill -9` command to terminate the node and release resources immediately. Otherwise, new nodes can start only after the existing nodes are completed.

- Check whether the disk on a gateway server is full.

  Log on to the gateway server and run the `df -h` command to check whether the disk attached to /home/admin is full. If the disk is full, run the `du-sh` command to identify the files in the /home/admin directory that consume a large amount of space. You can manually remove some large log files from the /home/admin/alisatasknode/taskinfo/ directory.

- Check the system time of servers in the base cluster against the time of the NTP server.

  i. Log on to the database that hosts the base-biz-alisa service and run the `select now();` command to view the current time of the database.

  ii. Check the system time of servers in the base cluster against the time of the database.

  iii. Run the date command on the servers to check whether the system time of each server is synchronized with the time of the database. If the time difference is greater than 30 seconds, the base-biz-alisa service may fail. In this case, synchronize the system time of servers in the base cluster with the time of the NTP server.

  > **Note** In Apsara Stack V3, you can find the servers of the base cluster in the service list in the Apsara Infrastructure Management Framework console and follow the proceeding steps to resolve the issue.

- Rename the phoenix folder to change it to a .bak file and restart the base-biz-alisa service.

  If the issue persists after you perform the preceding steps, run the following command on the gateway server:

```
cd /home/admin/alisatasknode/taskinfo/prevDay/phoenix/
```

> ⓘ **Note** Replace prevDay in this command with the date of the previous day in the format YYYYMMDD, for example, 20180306.

In this directory, run the `mkdir test` command. If the error message "Cannot create directory too many links" appears, the issue occurs because the number of subdirectories in the directory has reached the maximum and you cannot create more subdirectories. To resolve this issue, follow these steps:

i. Rename the /home/admin/alisatasknode/taskinfo/20180306/phoenix directory as /home/admin/alisatasknode/taskinfo/20180306/phoenix.bak.

ii. Run the following command to restart the base-biz-alisa service:

```
sudo su admin -c "/home/admin/alisatasknode/target/alisatasknode/bin/serverctlrestart"
```

> ⓘ **Note** This is a rare problem which tends to occur when a gateway server uses the third extended (ext3) file system.

11.3.5.2. An out-of-memory (OOM) error occurs when synchronizing data from an Oracle database

Description

During the data synchronization from an Oracle database to MaxCompute or other platforms, an `java.lang.OutOfMemoryError: Java heap space` error is displayed in the task log.

Cause

This issue is often caused by a large volume of data in the data synchronization task, which causes a JVM OOM error.

Solution

Set a low fetchsize value.

Use MySQL statements to connect to the cdp database, and modify the template configuration of the Oracle reader plug-in by changing the fetchsize value from 1024 to 128. Run the following statement:

```
update t_plugin_template set template=replace(template,'1024','128') where name='oracle' and type='read
er';
```

Rerun the task after the fetchsize value is changed. To reset the fetchsize value, run the following statement:

```
update t_plugin_template set template=replace(template,'128','1024') where name='oracle' and type='read
er';
```

11.3.5.3. A task does not run at the specified time

Description

A periodic task does not run, and no data is displayed in the overview.

Solution

1. Check whether periodic scheduling is enabled in this workspace.

   On the Workspace Configuration page in Workspace Management, ensure that the periodic scheduling is enabled.

2. If it is enabled, check whether the phoenix service runs properly.

   Connect to the phoenix database and run the following statement.

   ```
   select to_char(to_timestamp(next_fire_time/1000),'YYYY-MM-DDHH24:MI:SS') from qrtz_triggers;
   ```

   If the output contains 00:00:00 of the next day, the service is running properly. If not, you need to check whether the time of the two base-biz-phoenix containers are different.

   If the two containers have the same system time, you need to switch to the admin account and run the `/home/admin/base-biz-phoenix/bin/jbossctl restart` command to restart the phoenix service, and then check the time again.

3. After the time is corrected, you can run tasks that failed to run on the previous day.

   Run the following command in either of the phoenix containers. Note that you can run this command only once.

   ```
   curl -v -H "Accept:application/json"-H "Content-type: application/json"-X POST -d'{"opCode":11,"opSEQ":12345,"opUser":"067605","name":"SYSTEM","bizdate":"2017-04-2300:00:00","gmtdate":"2017-04-2400:00:00"}' http://localhost:7001/engine/2.0/flow/create_unified_daily
   ```

   Note bizdate refers to the previous day, and gmtdate refers to the current day. Modify the command if needed before running it.

11.3.5.4. The test service of base is not in the desired status

1. On the S tab, select base-baseBizApp.
2. Select the cluster in the lower part of the left-side navigation pane, and then open the dashboard.
3. View the report of service monitoring.

   Analyze the causes of the failed test based on the log.

11.3.5.5. The Data Management page does not display the number of tables and the usage of tables

Description

.

The Data Management page is blank.

Solution

1. Log on to the Apsara Infrastructure Management Framework console, select odps from the project drop-down list, and then open the HybridOdpsCluster dashboard page.
2. Find the accesskey type base_admin service in the Cluster Resource area.
3. Right-click the result field, and click Show More to view the username and the password.
4. Log on to DataWorks.

   > **Note** To log on to DataWorks, enter the domain name of base in the browser. By default, the domain name is ide.[your Apsara Stack second-level domain].

5. Select the base_meta workspace, and go to Administration.

   Rerun all failed tasks, and then check whether the Data Management page is displayed properly. If the task fails again, contact Alibaba Cloud Customer Support.

11.3.5.6. Logs are not automatically cleaned up

Description

Logs are not cleaned up automatically because of an error.

Solution

Follow the following steps to clean up the logs manually.

1. Establish a terminal session to the VM.
2. Run the following command to clean up real-time analysis logs.

   ```
   find /home/admin/cai/logs/cronolog/ -mtime +7 -type f -exec rm –rf {} \;
   find /home/admin/dw-realtime-analysis/logs/ -mtime +7 -type f -exec rm -rf {} \;
   ```

3. Run the following command to clean up base-biz-diide application logs.

   ```
   find /home/admin/cai/logs/cronolog/ -mtime +7 -type f -exec rm –rf {} \;
   find /home/admin/base-biz-diide/logs/ -mtime +7 -type f -exec rm -rf {} \;
   ```

4. Run the following command to clean up base-biz-cdp application logs.

   ```
   find /home/admin/cai/logs/cronolog/ -mtime +7 -type f -exec rm –rf {} \;
   find /home/admin/base-biz-cdp/logs/ -mtime +7 -type f -exec rm -rf {} \;
   ```

11.3.5.7. The real-time analysis service is not in the desired status

Description

The real-time analysis service is not in the desired status.

Solution

1. On the S tab, select dataworks-realtime.
2. Open the dashboard page of the cluster in the lower part of the left-side navigation pane.
3. View the report of service monitoring.

   View the log to find out what caused the failed test.

11.4. Realtime Compute

11.4.1. Job status

11.4.1.1. Overview

RealtimeCompute allows you to view the real-time running information and instantaneous values of a job. You can also determine whether a job is running properly and whether the job performance meets expectations based on the job status.

11.4.1.2. Task status

A task can be in one of the following seven statuses: created, running, failed, completed, scheduling, canceling, and canceled. You can determine whether a job is running properly based on the task status.

11.4.1.3. Health score

To help you quickly locate job performance issues, Realtime Compute offers a health check feature.

If the health score of a job is lower than 60, lots of data has been piled up on the current task node and data processing performance needs to be optimized. To optimize the performance, you can enable automatic resource configuration or manually reconfigure the resources. You can optimize the performance based on your business requirements.

11.4.1.4. Job instantaneous values

Job parameters

Name	Description
Consumed compute time	Indicates the computing performance of a job.
Input TPS	Indicates the number of data blocks that are read from the source per second. For Log Service, multiple data records can be included in a log group and the log group functions as the basic unit of measurement for data. In this scenario, the number of blocks indicates the number of log groups that are read from the source per second.
Input RPS	Indicates the number of data records that are read from the source table per second.

Name	Description
Output RPS	Indicates the number of data records that are written into result tables per second.
Input BPS	Indicates the data transmission rate per second, which is measured in bytes per second.
CPU usage	Indicates the CPU usage of the job.
Start time	Indicates the start time of the job.
Running duration	Indicates the duration during which the job has been running.

11.4.1.5. Running topology

A running topology shows the execution of the computing logic of Realtime Compute. Each component corresponds to a task. Each data stream starts from one or more sources and ends in one or more result tables. The data flow resembles an arbitrary directed acyclic graph (DAG). To enable efficient distributed execution, Realtime Compute chains operator subtasks together into tasks if possible. Each task is executed by one thread.

You can chain operators together into tasks for the following benefits:

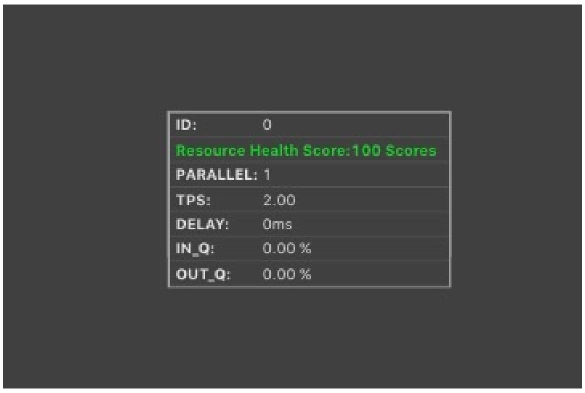
- Reduces thread-to-thread handovers.
- Reduces message serialization and deserialization.
- Reduces data handovers in the buffer zone.
- Increases the overall throughput while decreasing the delay.

An operator describes the computing logic, and a task is a collection of operators.

View mode

The computing logic is visualized in the view mode for an intuitive display, as shown in the View mode figure.

View mode



ID: 0
Resource Health Score:100 Scores
PARALLEL: 1
TPS: 2.00
DELAY: 0ms
IN_Q: 0.00 %
OUT_Q: 0.00 %

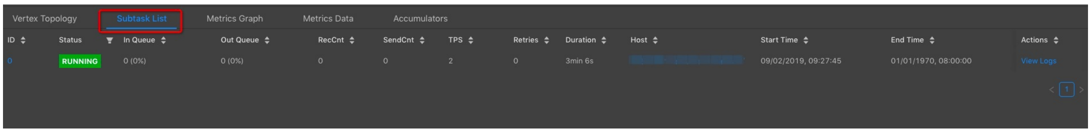
You can view the detailed information about a task by moving the pointer over the task. The Task parameters table describes the task parameters.

Task parameters

Parameter	Description
ID	The ID of the task in the running topology.
PARALLEL	The number of requests that are concurrently processed.
CPU	The CPU usage of a parallel instance for the task.
MEM	The memory usage of a parallel instance for the task.
TPS	The amount of data that is read from the upstream. Unit: blocks per second.
LATENCY	The compute time consumed at the task node.
DELAY	The processing delay that occurs at the task node.
IN_Q	The percentage of input queues for the task node.
OUT_Q	The percentage of output queues for the task node.

You can also click a task node to access its details page. On this page, you can view its subtasks, as shown in the Task details figure.

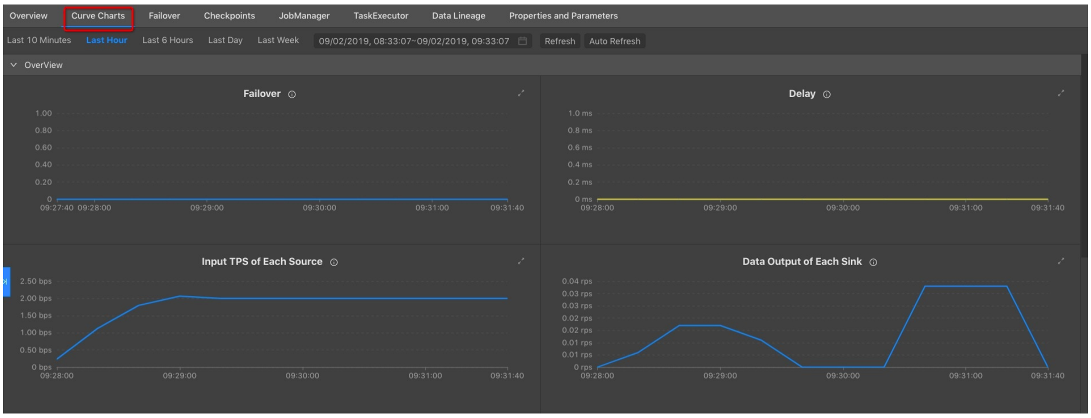
Task details



ID	Status	In Queue	Out Queue	RecCnt	SendCnt	TPS	Retries	Duration	Host	Start Time	End Time	Actions
0	RUNNING	0 (0%)	0 (0%)	0	0	2	0	3min 6s	[redacted]	09/02/2019, 09:27:45	01/01/1970, 08:00:00	View Logs

The **Curve Charts** tab provides curve charts that show the metrics of each task, as shown in the Curve charts for task metrics figure.

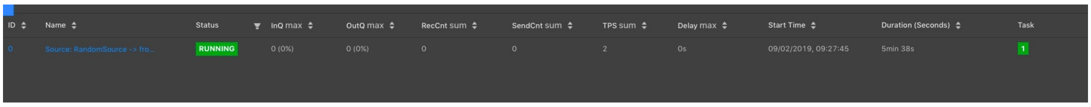
Curve charts for task metrics



List mode

In addition to the view mode, Realtime Compute allows you to view each task in the list mode, as shown in the List mode figure.

List mode



ID	Name	Status	InQ max	OutQ max	RecCnt sum	SendCnt sum	TPS sum	Delay max	Start Time	Duration (Seconds)	Task
0	Source: RandomSource -> fro...	RUNNING	0 (0%)	0 (0%)	0	0	2	0s	09/02/2019, 09:27:45	5min 38s	1

The Task parameters table describes the task parameters.

Task parameters

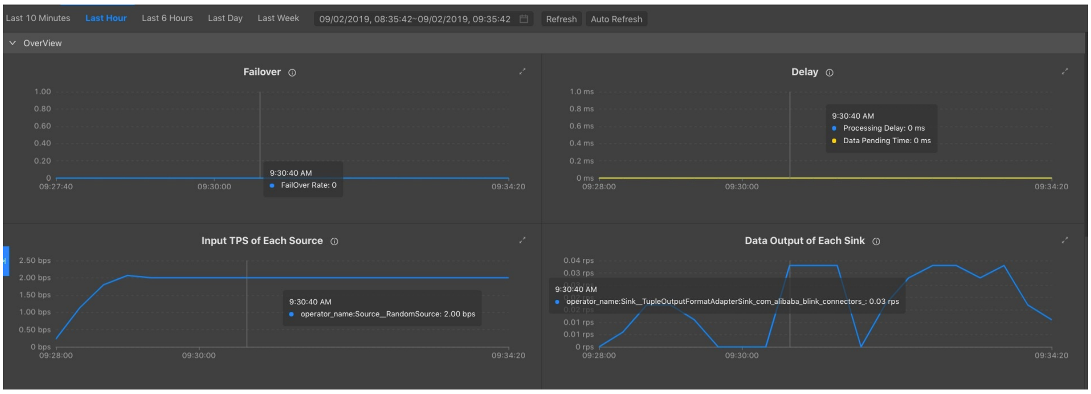
Parameter	Description
ID	The ID of the task in the running topology.
Name	The name of the task. The name shows the task details.
Status	The status of the task.
InQ max	The percentage of input queues for the task node.
OutQ max	The percentage of output queues for the task node.
RecCnt sum	The total amount of data that is received by the task node.
SendCnt sum	The total amount of data that is sent from the task node.
TPS sum	The total amount of data that is read from the upstream per second.
Delay max	The processing delay that occurs at the task node.
Task	The status of parallel instances for the task node.
Start Time	The start time of the task node.
Duration (Seconds)	The running duration of the task node.

11.4.2. Curve charts

11.4.2.1. Overview

On the Curve Charts tab of the Realtime Compute development platform, you can view the key metrics of a job. This allows you to easily analyze the performance of a job. Currently, we are working on intelligent and automatic diagnosis by developing in-depth intelligent analysis algorithms based on the job running information.

Curve Charts tab



Note

- The metrics shown in this figure are displayed only when the job is in the running status.
- The metrics are asynchronously collected in the background, which results in delays. The metrics can be collected and displayed only after a job has been running for more than 1 minute.

11.4.2.2. Overview

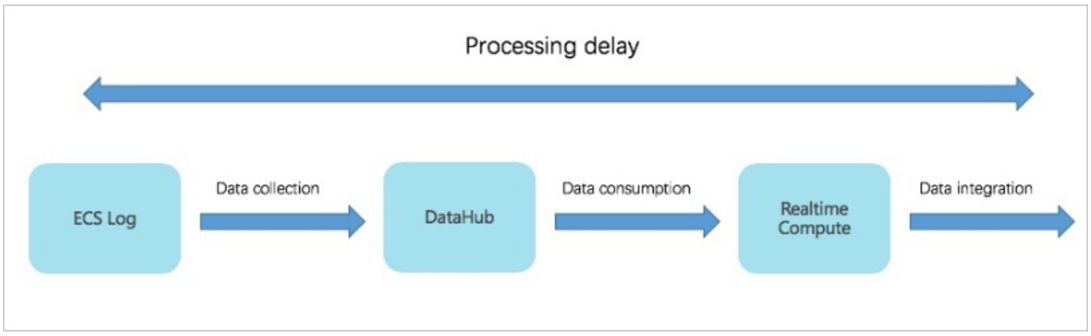
Failover

The failover rate indicates the percentage of the number of times that errors or exceptions occur on the current job. The failover rate curve allows you to easily analyze the issues of the current job.

Processing delay

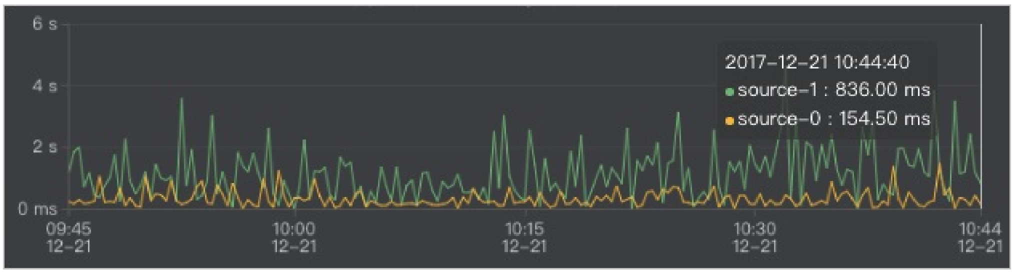
The processing delay refers to the time interval between the timestamp carried by the streaming data in the source table and the time when Realtime Compute processes the streaming data. If no field in the source table indicates the streaming data timestamp, the delay is calculated based on the system timestamp assigned by source data stores to the data. Examples of the source data stores include DataHub and LogHub. The processing delay shows the timeliness of end-to-end data processing. For example, if the current processing time is 05:00 and the timestamp of the stored data is 01:00, the processing delay is four hours. In this example, the data to be processed was stored at 01:00, which is four hours earlier than the current processing time. The data processing progress is based on the processing delay. For example, if data fails to flow into the DataHub source data store because of faults, the processing delay increases, which causes the processing progress to be delayed. Processing delay shows the processing delay.

Processing delay

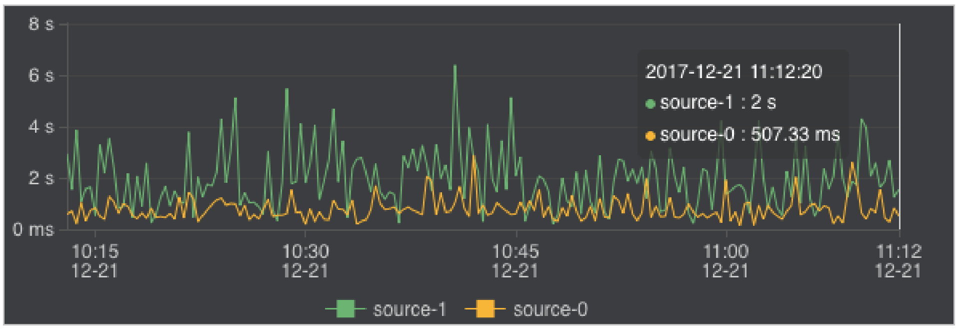


The processing delay can be categorized into the following three types:

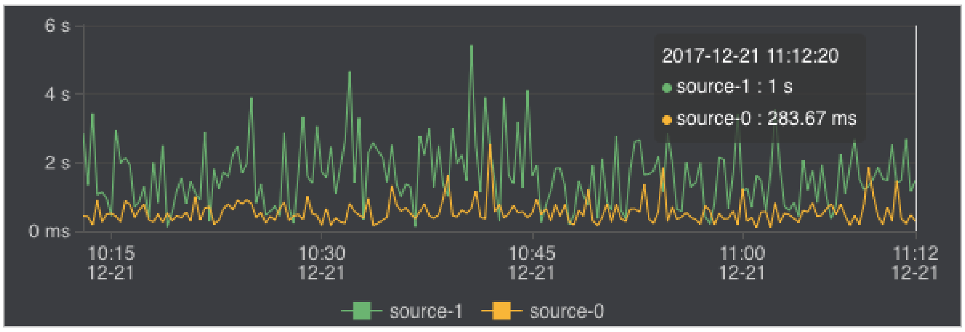
- Shortest delay: indicates the shortest processing delay that a shard in each data source experiences.



- Longest delay: indicates the longest processing delay that a shard in each data source experiences.



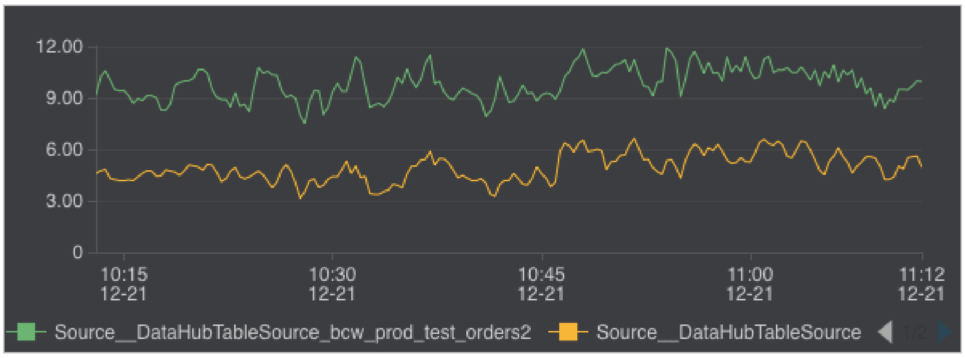
- Average delay: indicates the average processing delay of shards in each data source.



Input TPS of each source

Realtime Compute collects statistics about streaming data inputs of each job to visualize input transactions per second (TPS). The input TPS describes the amount of data read from the source table, which is measured in blocks per second. Unlike TPS, records per second (RPS) indicates the number of data records parsed based on the data blocks that are read from the source table.

For example, in Log Service, X log groups are read per second and Y log records are parsed based on the X log groups. In this example, the input TPS is X, and the output RPS is Y.



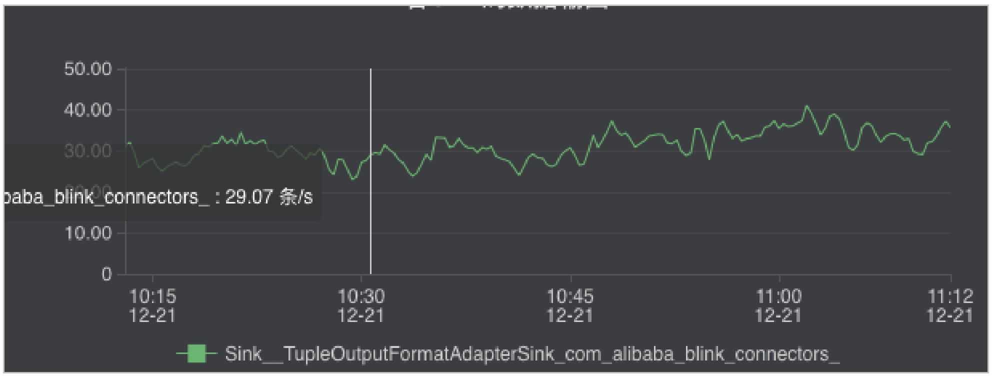
Data outputs of each sink

Realtime Compute collects statistics about data outputs of each job to visualize the output RPS.

Note You can view the data outputs for all the target data stores, including data stores for streaming and non-streaming data.

If you find that no data outputs are detected during job administration, you must check whether data inputs exist in the upstream. You must also check whether data outputs exist in the downstream.

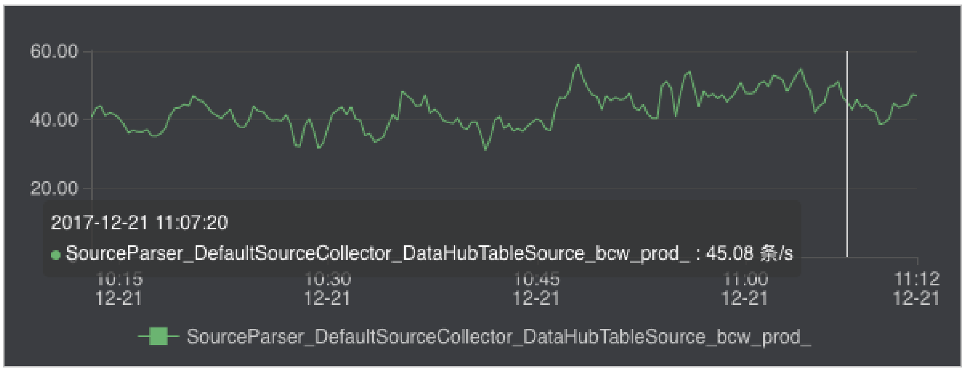
Data outputs of each sink



Input RPS of each source

Realtime Compute collects statistics about streaming data inputs of each job to visualize the input data records per second. If you find that no data outputs are detected during job administration, you must check whether data inputs from the source exist.

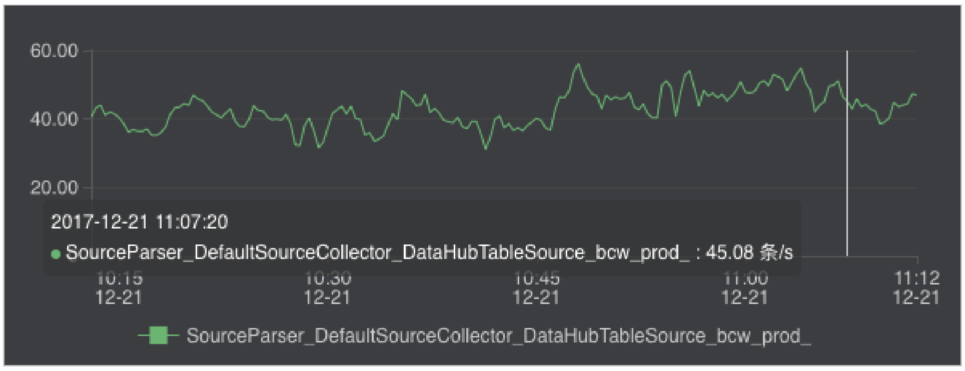
Input RPS of each source



Input BPS of each source

Realtime Compute collects statistics about streaming data inputs of each job to visualize the input data bytes per second (BPS). The input BPS indicates the amount of data that is read from the source table per second.

Input BPS of each source



CPU usage

The CPU usage describes the CPU resources that are consumed by a Realtime Compute job. Realtime Compute provides the following two metrics to reflect the CPU usage:

- The number of CPUs that you have requested.
- The CPU usage of the current job at a specified time. You can view the CPU usage from the curve chart.

Memory usage

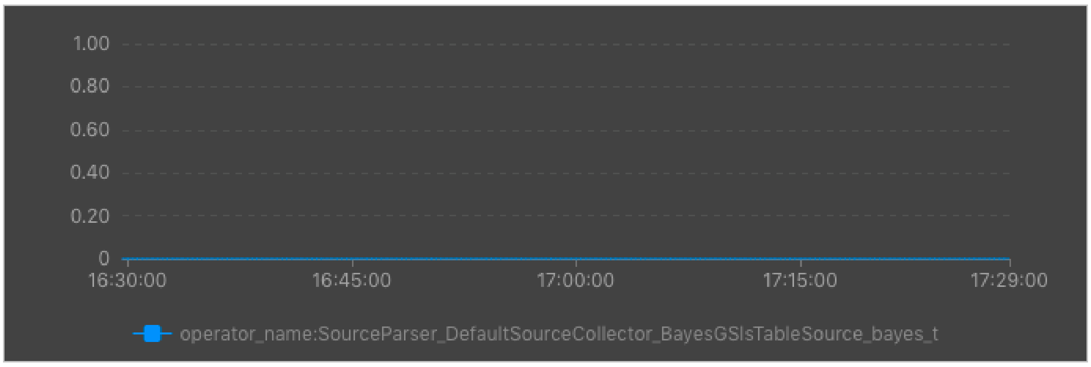
The memory usage describes the memory resources that are consumed by a Realtime Compute job. Realtime Compute provides the following two metrics to reflect the memory usage:

- The memory size that you have requested.
- The memory usage of the current job at a specified time. You can view the memory usage from the curve chart.

Dirty data from each source

Realtime Compute allows you to view the statistics of dirty data from each source in a curve chart.

Dirty data from each source



11.4.2.3. Advanced view

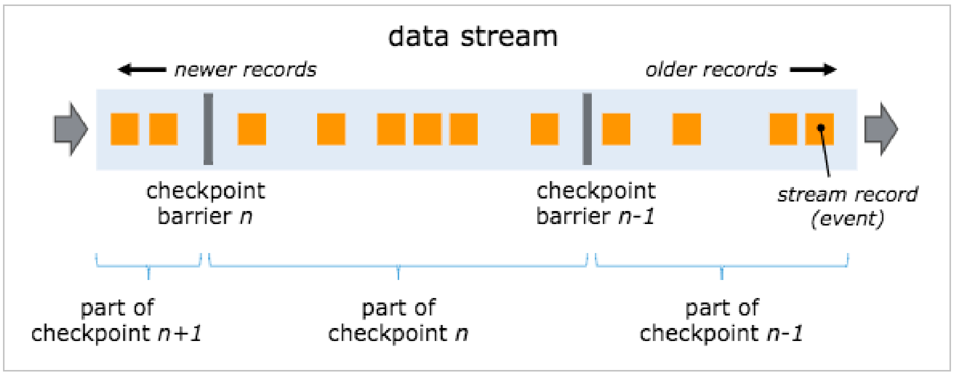
Realtime Compute offers a fault tolerance mechanism to consistently recover the state of data streaming applications. The central part of the fault tolerance mechanism is creating consistent snapshots of distributed data streams and the state. These snapshots act as consistent checkpoints to which the system can fall back when a failure occurs.

One of the core concepts of distributed snapshots is the barrier. Barriers are inserted into data streams and flow together with the data streams to the downstream. Barriers do not overtake the source streaming data records, and the records flow strictly in line. A barrier separates the records in a data stream into two sets of records.

- One set of records goes into the current snapshot.
- The other set of records goes into the next snapshot.

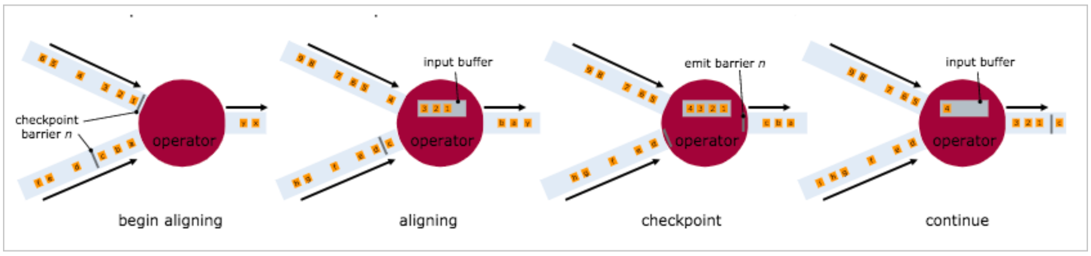
Each barrier carries the ID of a snapshot that contains the records pushed before the barrier. Barriers do not interrupt the flow of the stream, and therefore are very lightweight. Multiple barriers from different snapshots can be found in the stream at the same time, which means that multiple snapshots may be concurrently created.

Barriers



Barriers are inserted into data streams at data sources. The point where the barriers for snapshot n are inserted is the position in the source stream, up to which the snapshot covers the data. This point is indicated by Sn. The barriers then flow to the downstream. When an intermediate operator has received a barrier for snapshot n from all of its input streams, the operator emits a barrier for snapshot n into all of its outgoing streams. When a sink operator has received barrier n from all of its input streams, the sink operator acknowledges that snapshot n to the checkpoint coordinator. A sink operator is the end of a streaming directed acyclic graph (DAG). After all sink operators have acknowledged a snapshot, the snapshot is considered completed.

Barrier



Checkpoint parameters

- **Checkpoint Duration**

  This parameter indicates the time spent on saving the state for each checkpoint. The duration is measured in milliseconds.

- **Checkpoint Size**

  This parameter indicates the state size of a checkpoint, which is measured in MiB.

- **Checkpoint Alignment Time**

This parameter indicates the time that is spent on receiving and acknowledging barrier n from all input streams. When a sink operator has received barrier n from all of its input streams, it acknowledges the snapshot n to the checkpoint coordinator. After all sink operators have acknowledged the snapshot n to the checkpoint coordinator, this snapshot is considered completed. The time consumed by the acknowledgement is included in the checkpoint alignment time.

- Checkpoint Count
- Get

  This parameter indicates the longest time that a subtask spends on performing a GET operation on the RocksDB database within a specified period.

- Put

  This parameter indicates the longest time that a subtask spends on performing a PUT operation on the RocksDB database within a specified period.

- Seek

  This parameter indicates the longest time that a subtask spends on performing a SEEK operation on the RocksDB database within a specified period.

- State Size

  This parameter indicates the state size of a job. If the size increases excessively fast, we recommend that you check and resolve potential issues.

- CMS GC Time

  This parameter indicates the garbage collection (GC) time consumed by the underlying container that runs the job.

- CMS GC Rate

  This parameter indicates how often the garbage collection is performed in the underlying container that runs the job.

11.4.2.4. Processing delay

Top 15 source subtasks with the longest processing delay

This metric describes the processing delays of each parallelism of a source.

11.4.2.5. Throughput

Task Input TPS

This indicates the data inputs of all tasks for the job.

Task Output TPS

This indicates the data outputs of all tasks for the job.

11.4.2.6. Queue

Input Queue Usage

This indicates the input data queues of all tasks for the job.

Output Queue Usage

This indicates the output data queues of all tasks for the job.

11.4.2.7. Tracing

The available parameters for advanced users are as follows:

- **Time Used In Processing Per Second**

  This parameter indicates the time that a task spends on processing the data of each second.

- **Time Used In Waiting Output Per Second**

  This parameter indicates the time that a task spends on waiting for outputs of each second.

- **TaskLatency**

  This parameter indicates the computing delay of each task for a job. This delay is indicated by the interval between the time when data enters a task node and the time when data processing is completed on the task node. You can view the delay from the corresponding curve chart.

- **WaitOutput**

  This parameter indicates the time that a task spends on waiting for outputs. You can view the waiting time from the corresponding curve chart.

- **WaitInput**

  This parameter indicates the time that a task spends on waiting for inputs. You can view the waiting time from the corresponding curve chart.

- **Source Latency**

  This parameter indicates the delay of each parallelism for a data source. You can view the delay from the corresponding curve chart.

11.4.2.8. Process

Process MEM Rss

You can view the memory usage of each process from the curve chart.

Memory NonHeap Used

You can view the non-heap memory usage of each process from the curve chart.

CPU Usage

You can view the CPU usage of each process from the curve chart.

11.4.2.9. JVM

Memory Heap Used

This indicates the Java Virtual Machine (JVM) heap memory usage of the job.

Memory NonHeap Used

This indicates the JVM non-heap memory usage of the job.

Threads Count

This indicates the number of threads for the job.

GC (CMS)

This indicates how often garbage collection (GC) is performed for the job.

11.4.3. FailOver

On the FailOver tab of the Realtime Compute development platform, you can check whether the job is running properly.

Latest FailOver

On the Latest FailOver tab, you can view the running errors of the job.

FailOver History

On the FailOver History tab, you can view the previous running errors of the job.

11.4.4. CheckPoints

Realtime Compute offers a fault tolerance mechanism to consistently recover the state of data streaming applications. The central part of the fault tolerance mechanism is drawing consistent snapshots of the distributed data stream and the state. These snapshots act as consistent checkpoints to which the system can fall back when a failure occurs.

Completed Checkpoints

On this tab, you can view the checkpoints that have been created. Parameter description describes the parameters for the created checkpoints.

Parameter description

Parameter	Description
ID	The ID of the checkpoint.
StartTime	The start time when the checkpoint is created.
Durations(ms)	The time that is spent on creating the checkpoint.

Task Latest Completed Checkpoint

On this tab, you can view the detailed information about the latest checkpoint. Parameter description describes the parameters for the latest checkpoint.

Parameter description

Parameter	Description
SubTask ID	The ID of the subtask.
State Size	The state size of the checkpoint.

Parameter	Description
Durations(ms)	The time that is spent on creating the checkpoint.

11.4.5. JobManager

After a Realtime Compute cluster is started, one JobManager and one or more TaskManagers are started. A client submits jobs to the JobManager, and the JobManager assigns the tasks of jobs to TaskManagers. During task execution, TaskManagers report the heartbeats and statistics to the JobManager. The TaskManagers exchange the data streams.

Similar to Storm Nimbus, a JobManager schedules jobs and functions as a coordinator to create checkpoints for tasks. A JobManager receives resources, such as jobs and JAR files, from a client. Then, the JobManager generates an optimized execution plan based on these resources and assigns tasks to TaskManagers.

11.4.6. TaskExecutor

After a Realtime Compute cluster is started, one JobManager and one or more TaskManagers are started. A client submits jobs to the JobManager, and the JobManager assigns the tasks of jobs to TaskManagers. During task execution, TaskManagers report the heartbeats and statistics to the JobManager. The TaskManagers exchange the data streams.

The number of slots is specified before a TaskManager is started. A TaskManager executes each task in each slot, and each task can be considered as a thread. A TaskManager receives tasks from the JobManager, and then establishes a Netty connection with its upstream to receive and process data.

TaskExecutor shows the detailed information about each TaskManager.

11.4.7. Data lineage

On the Data Lineage tab of the Realtime Compute development platform, you can view the dependencies of a job, including its relationship with its source table and result table. The topology on this tab allows you to easily and clearly view the complex dependencies of a job.

Data sampling

Realtime Compute provides the data sampling feature for source tables and result tables of jobs. The data to be sampled is the same as the data on the Development page. The data sampling feature allows you to check data at any time on the Administration page to facilitate fault locating. In the topology, click the button on the right side of the table name to enable the data sampling feature.

11.4.8. Properties and Parameters

The Properties and Parameters page provides detailed information about the current job, including the current running information and running history.

Job Code

On this tab page, you can preview the SQL job. You can also click **Edit Job** to go to the **Development** page.

Resource Configuration

On this tab page, you can view the resources that have been configured for the current job, including the CPU, memory, and parallelism.

Properties

On this tab page, you can view the basic running information of the current job. Job properties describes the basic job properties that are displayed on this tab page.

Job properties

No.	Field and Description
1	Job Name: indicates the name of the job.
2	Job ID: indicates the ID of the job.
3	Referenced Resources: indicates the resources that are referenced by the job.
4	Execution Engine: indicates the engine of the job.
5	Last Operated By: indicates the user who last operates the job.
6	Action: indicates the action that is last performed.
7	Created By: indicates the user who creates the job.
8	Created At: indicates the time when the job is created.
9	Last Modified By: indicates the user who last modifies the job.
10	Last Modified At: indicates the time when the job is last modified.

Running Parameters

On this tab page, you can view the underlying checkpoints, start time, and running parameters of the job.

History

On this tab page, you can view the detailed information about all versions of the job, including the start time, end time, and the user who operates the job.

Parameters

On this tab page, you can view additional job parameters, such as the separator used in the debugging file.

11.4.9. Performance optimization by using automatic configuration

To improve user experience, Realtime Compute allows you to use automatic configuration to optimize job performance.

> **Note** Automatic configuration applies to Blink 1.0 and Blink 2.0.

Background and scope

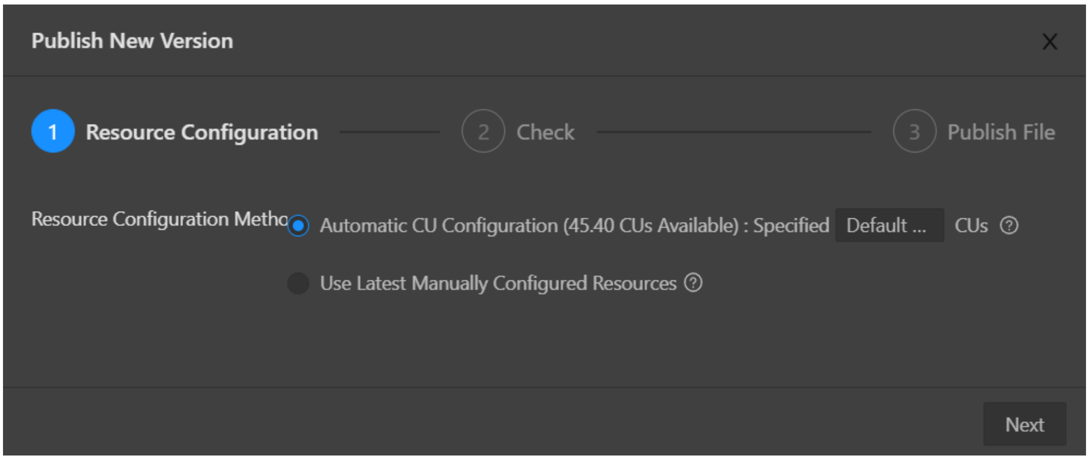
If all the operators and both the upstream and downstream storage systems of your Realtime Compute job meet the performance requirements and remain stable, automatic configuration can help you properly adjust job configurations, such as operator resources and parallelism. It also helps optimize your job throughout the entire process to resolve performance issues such as low throughput or upstream and downstream backpressure.

In the following scenarios, you can use this feature to optimize job performance but cannot eliminate job performance bottlenecks. To eliminate the performance bottlenecks, manually configure the resources or contact the Realtime Compute support team.

- Performance issues exist in the upstream or downstream storage systems of a Realtime Compute job.
  - Performance issues in the data source, such as insufficient DataHub partitions or Message Queue (MQ) throughput. In this case, you must increase the partitions of the relevant source table.
  - Performance issues in a data sink, such as a deadlock in ApsaraDB RDS.
- Performance issues of user-defined extensions (UDXs) such as user-defined functions (UDFs), user-defined aggregate functions (UDAFs), and user-defined table-valued functions (UDTFs) in your Realtime Compute job.

Description

- New jobs
  i. Publish a job.
    a. After you complete SQL development and syntax check on the **Development** page, click **Publish**. The **Publish New Version** dialog box appears.



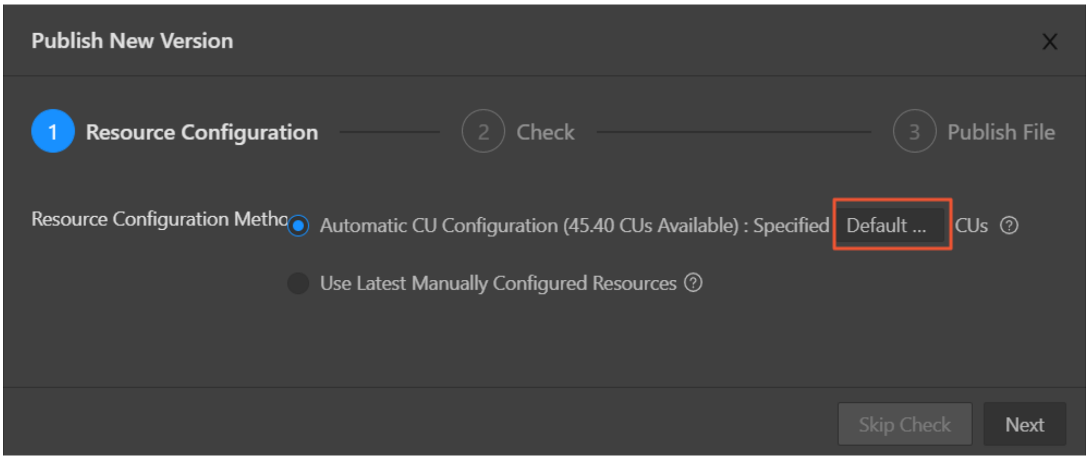
Resource Configuration Metho ● Automatic CU Configuration (45.40 CUs Available) : Specified Default ... CUs ⓘ
○ Use Latest Manually Configured Resources ⓘ

b. Specify **Resource Configuration Method**.

- **Automatic CU Configuration**: If you select this option, you can specify the number of compute units (CUs). The automatic configuration algorithm generates an optimized resource configuration and assigns a value for the number of CUs based on the default configuration. If you use automatic CU configuration for the first time, the default number of CUs is used. This algorithm generates an initial configuration based on empirical data when you use automatic CU configuration for the first time. We recommend that you select Automatic CU Configuration if your job has been running for 5 to 10 minutes and its metrics, such as source RPS, remain stable for 2 to 3 minutes. You can obtain the optimal configuration after you repeat the optimization process for three to five times.
- **Use Latest Manually Configured Resources**: The latest saved resource configuration is used. If the latest resource configuration is generated based on automatic CU configuration, the latest resource configuration is used. If the latest resource configuration is obtained based on the manual configuration, the manual configuration is used.

ii. Use the default configuration to start the job.

a. Use the default configuration to start the job, as shown in the following figure.



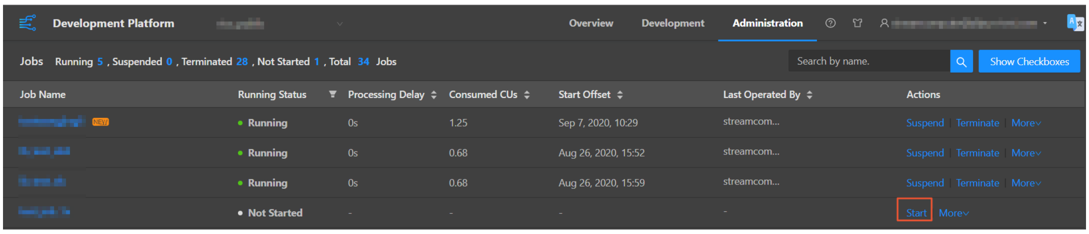
Publish New Version

1 Resource Configuration — 2 Check — 3 Publish File

Resource Configuration Metho ● Automatic CU Configuration (45.40 CUs Available) : Specified Default ... CUs

○ Use Latest Manually Configured Resources

b. On the Administration page, find the job and click **Start** in the Actions column to start the job.



Jobs Running 5 , Suspended 0 , Terminated 28 , Not Started 1 , Total 34 Jobs

Job Name	Running Status	Processing Delay	Consumed CUs	Start Offset	Last Operated By	Actions
[redacted] NEW	● Running	0s	1.25	Sep 7, 2020, 10:29	streamcom...	Suspend | Terminate | More
[redacted]	● Running	0s	0.68	Aug 26, 2020, 15:52	streamcom...	Suspend | Terminate | More
[redacted]	● Running	0s	0.68	Aug 26, 2020, 15:59	streamcom...	Suspend | Terminate | More
[redacted]	● Not Started	-	-	-	-	Start More

Assume that the default number of CUs generated the first time is 71.

> **Note** Make sure that your job runs longer than 10 minutes and its metrics such as source RPS remain stable for 2 to 3 minutes before you select Automatic CU Configuration for Resource Configuration Method.

iii. Use the automatic CU configuration to start a job.

a. Resource performance optimization

   If you select Automatic CU Configuration for Resource Configuration Method and specify 40 CUs to start your job, you can change the number of CUs based on your job to optimize resource performance.

   - Determine the minimum number of CUs.

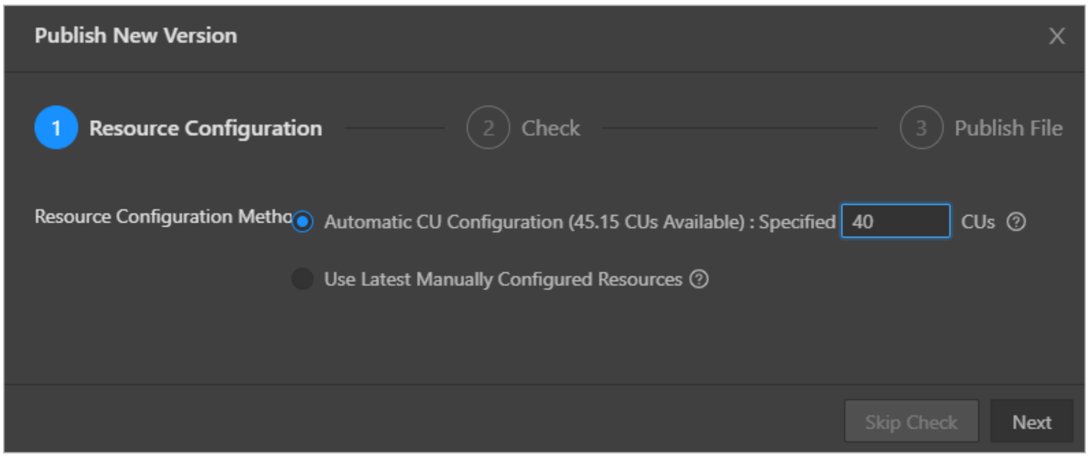
     We recommend that you set the number of CUs to a value that is greater than or equal to 50% of the default value. The number of CUs cannot be less than 1. Assume that the default number of CUs for automatic CU configuration is 71. The recommended minimum number of CUs is 36, which is calculated by using the following formula: 71 CUs × 50% = 35.5 CUs.

   - Increase the number of CUs.

     If the throughput of your Realtime Compute job does not meet your requirements, increase the number of CUs. We recommend that you increase the number of CUs by more than 30% of the current value. For example, if the number of CUs that you specified last time is 10 CUs, you can increase the number to 13.

   - Repeat the optimization process.

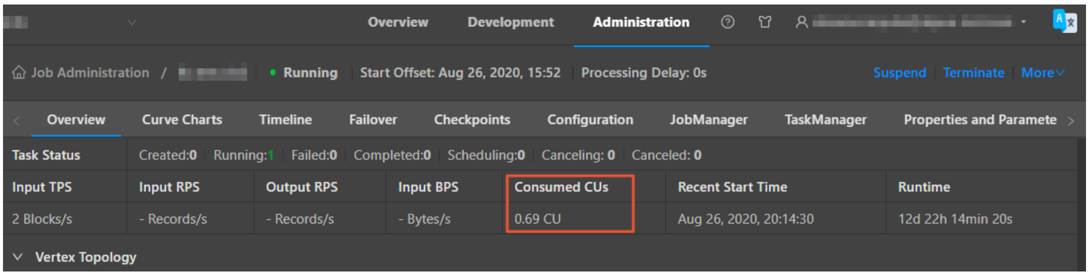
     If the first optimization attempt does not meet your requirements, repeat the process until you obtain the desired results. You can change the number of CUs based on your job status after each optimization attempt.



Resource Configuration Metho ● Automatic CU Configuration (45.15 CUs Available) : Specified 40 CUs

○ Use Latest Manually Configured Resources

b. View the result of optimization. The following figure shows an example.



Job Administration / [redacted] ● Running | Start Offset: Aug 26, 2020, 15:52 | Processing Delay: 0s

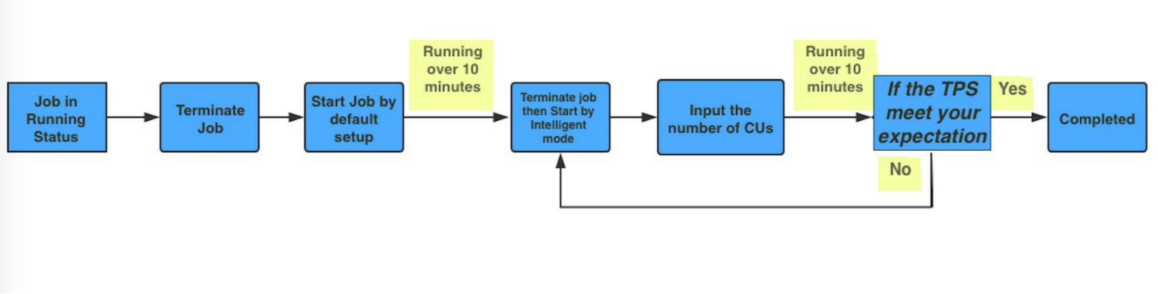
Task Status | Created:0 | Running:1 | Failed:0 | Completed:0 | Scheduling:0 | Canceling: 0 | Canceled: 0

Input TPS	Input RPS	Output RPS	Input BPS	Consumed CUs	Recent Start Time	Runtime
2 Blocks/s	- Records/s	- Records/s	- Bytes/s	0.69 CU	Aug 26, 2020, 20:14:30	12d 22h 14min 20s

> **Note** Do not select **Use Latest Manually Configured Resources** for a new job. Otherwise, an error is returned.

- Existing jobs

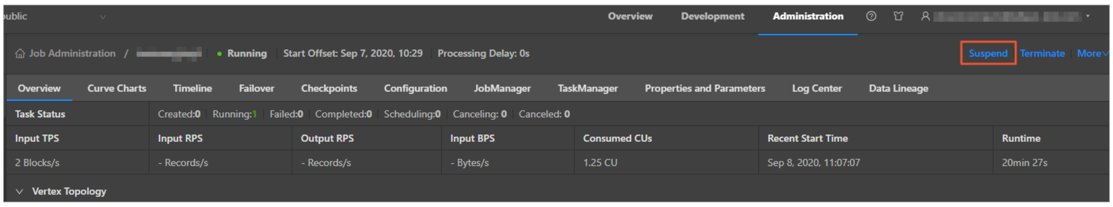
- The following figure shows the optimization process of automatic configuration.



> **Note**
>
> - Before you use automatic configuration for a job that is in the running state, check whether stateful operations are involved. This is because the saved state data of a job may be cleared during the optimization process of automatic configuration.
> - If you make changes to a job, for example, modifying SQL statements or changing the Realtime Compute version, automatic configuration may fail. These changes may lead to topology changes, which results in some issues. For example, curve charts may not be able to display the latest data, or the state data may not able to be used for fault tolerance. In this case, resource configurations cannot be optimized based on the job running history and therefore an error is returned when you perform automatic configuration. To rectify the fault, you must treat the changed job as a new job and repeat the previous operations.

- Procedure

  a. Suspend the job.

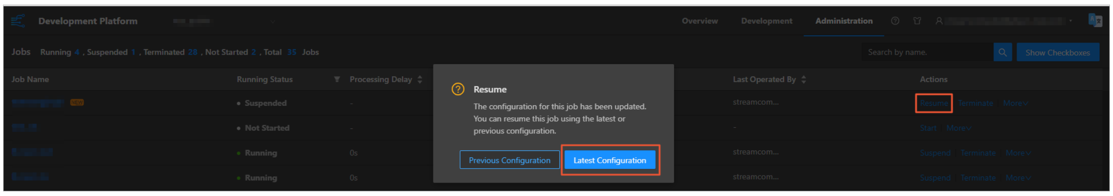


Job Administration / [redacted] ● Running | Start Offset: Sep 7, 2020, 10:29 | Processing Delay: 0s

Task Status: Created:0 | Running:1 | Failed:0 | Completed:0 | Scheduling:0 | Canceling: 0 | Canceled: 0

Input TPS	Input RPS	Output RPS	Input BPS	Consumed CUs	Recent Start Time	Runtime
2 Blocks/s	- Records/s	- Records/s	- Bytes/s	1.25 CU	Sep 8, 2020, 11:07:07	20min 27s

  b. Repeat the steps performed for new jobs and resume the job with the latest configuration.



Jobs Running 4 , Suspended 1 , Terminated 28 , Not Started 2 , Total 35 Jobs

Job Name	Running Status	Processing Delay	Last Operated By	Actions
[redacted] NEW	● Suspended	-	streamcom...	Resume | Terminate | More
[redacted]	● Not Started	-	-	Start | More
[redacted]	● Running	0s	streamcom...	Suspend | Terminate | More
[redacted]	● Running	0s	streamcom...	Suspend | Terminate | More

Resume

The configuration for this job has been updated. You can resume this job using the latest or previous configuration.

FAQ

The optimization result of automatic configuration may not be accurate in the following scenarios:

- If the job runs only for a short period of time, the data collected during data sampling is insufficient. We recommend that you increase the running duration of the job and make sure that the curves of job metrics such as source RPS remain stable for at least 2 to 3 minutes.
- A job fails. We recommend that you check and fix the failure.
- Only a small amount of data is available for a job. We recommend that you retrieve more historical data.

- The effect of automatic configuration is affected by multiple factors. Therefore, the latest configuration obtained by using automatic configuration may not be optimal. If the effect of automatic configuration does not meet your requirements, you can manually configure the resources. For more information, see Optimize performance by manual configuration.

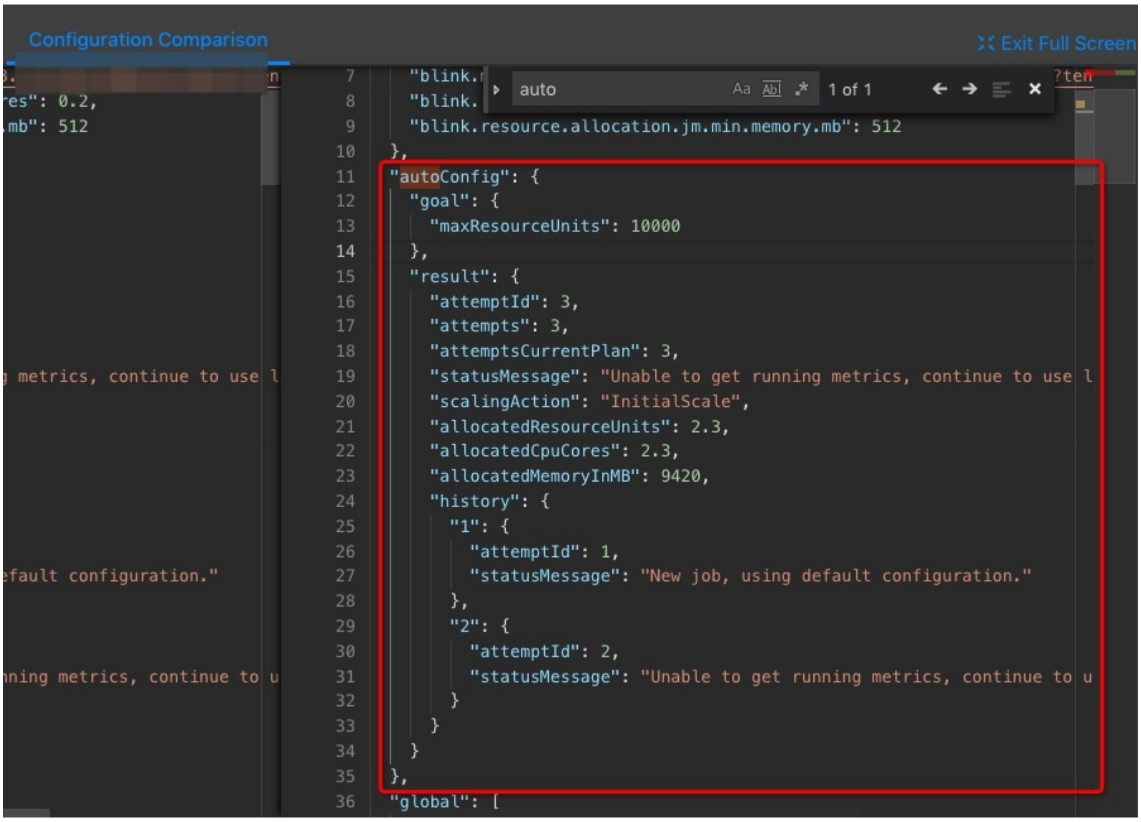
Recommendations

- To help automatic configuration accurately collect the runtime metric information of a job, make sure that the job runs stably for more than 10 minutes before you apply automatic configuration to the job.
- Job performance can be improved after you use automatic configuration for three to five times.
- When you use automatic configuration, you can specify the start offset to retrieve historical data or even accumulate large amounts of data for a job to create backpressure to accelerate the optimization effect.

Method used to determine the effectiveness of automatic configuration

Automatic configuration of Realtime Compute is enabled based on a JSON configuration file. After you use automatic configuration to optimize a job, you can view the JSON configuration file to check whether the feature is running as expected.

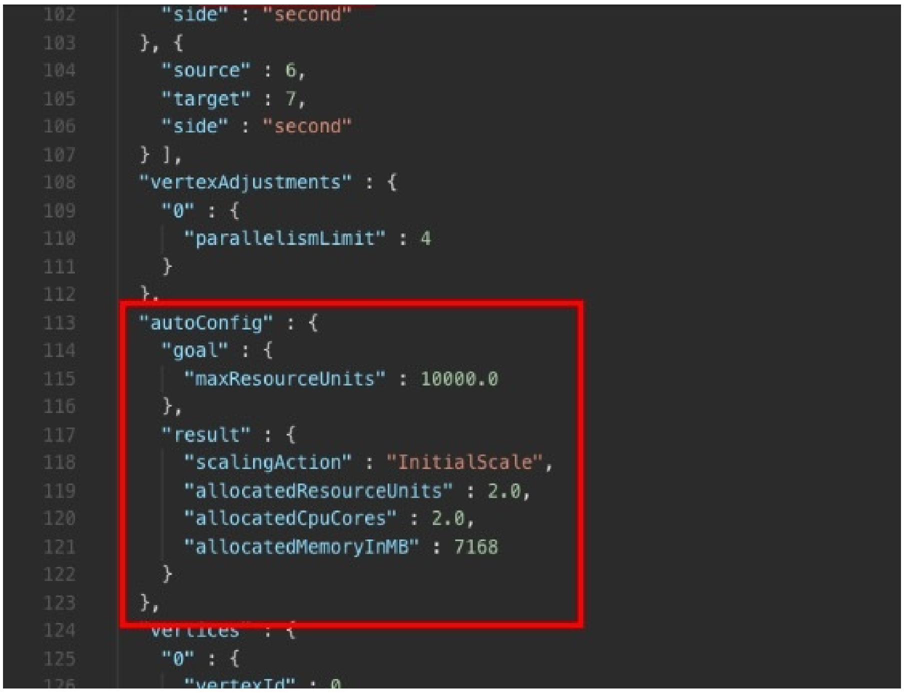
- You can view the JSON configuration file by using one of the following methods:
    i. View the file on the job edit page, as shown in the following figure.



```
3.[redacted]n
res": 0.2,
.mb": 512

g metrics, continue to use l

efault configuration."

nning metrics, continue to u
```

```
  "blink.r
  "blink.
  "blink.resource.allocation.jm.min.memory.mb": 512
},
"autoConfig": {
  "goal": {
    "maxResourceUnits": 10000
  },
  "result": {
    "attemptId": 3,
    "attempts": 3,
    "attemptsCurrentPlan": 3,
    "statusMessage": "Unable to get running metrics, continue to use l
    "scalingAction": "InitialScale",
    "allocatedResourceUnits": 2.3,
    "allocatedCpuCores": 2.3,
    "allocatedMemoryInMB": 9420,
    "history": {
      "1": {
        "attemptId": 1,
        "statusMessage": "New job, using default configuration."
      },
      "2": {
        "attemptId": 2,
        "statusMessage": "Unable to get running metrics, continue to u
      }
    }
  }
},
"global": [
```

    ii. View the file on the Job Administration page, as shown in the following figure.



```
    "side" : "second"
  }, {
    "source" : 6,
    "target" : 7,
    "side" : "second"
  } ],
  "vertexAdjustments" : {
    "0" : {
      "parallelismLimit" : 4
    }
  },
  "autoConfig" : {
    "goal" : {
      "maxResourceUnits" : 10000.0
    },
    "result" : {
      "scalingAction" : "InitialScale",
      "allocatedResourceUnits" : 2.0,
      "allocatedCpuCores" : 2.0,
      "allocatedMemoryInMB" : 7168
    }
  },
  "vertices" : {
    "0" : {
      "vertexId" : 0
```

- JSON configuration description

```
"autoconfig" : {
  "goal": {  // The goal of automatic configuration.
    "maxResourceUnits": 10000.0,  // The maximum number of CUs for a Blink job. This value cannot be changed. Therefore, you can ignore this item when you check whether the feature is running as expected.
    "targetResoureUnits": 20.0  // The number of CUs that you specified. The specified number of CUs is 20.
  },
  "result" : {  // The result of automatic configuration. We recommend that you pay attention to this item.
   "scalingAction" : "ScaleToTargetResource",  // The action of automatic configuration. *
   "allocatedResourceUnits" : 18.5, // The total resources allocated by automatic configuration.
   "allocatedCpuCores" : 18.5,      // The total CPU cores allocated by automatic configuration.
   "allocatedMemoryInMB" : 40960    // The total memory size allocated by automatic configuration.
   "messages" : "xxxx"  // We recommend that you pay attention to these messages. *
  }
}
```

  - scalingAction: If the value of this parameter is `InitialScale`, this is the first time that you use automatic configuration. If the value of this parameter is `ScaleToTargetResource`, this is not the first time that you use automatic configuration.

- If no message appears, automatic configuration runs properly. If some messages appear, you must analyze these messages. Messages are categorized into the following two types:
    - Warning: This type of message indicates that automatic configuration runs properly but you must pay attention to potential issues, such as insufficient partitions in a source table.
    - Error or exception: This type of message indicates that automatic configuration failed. The following error message is usually displayed: `Previous job statistics and configuration will be used`. The automatic configuration for a job fails in the following two scenarios:
        - The job or Blink version is modified before you use automatic configuration. In this case, the previous running information cannot be used for automatic configuration.
        - An error message that contains "exception" is reported when you use automatic configuration. In this case, you must analyze the error based on the job running information and logs. If you do not have enough information, submit a ticket.

Error messages

IllegalStateException

If the following error messages are displayed, the state data cannot be used for fault tolerance. To resolve this issue, terminate the job, clear its state, and then specify the start offset to re-read the data.

If you cannot migrate the job to a backup node, perform the following steps to mitigate the negative impact of service interruption: Roll back the job to an earlier version and specify the start offset to re-read the data during off-peak hours. To roll back the job, click **Versions** on the right side of the **Development** page. On the page that appears, move the pointer over More in the Actions column, click Compare, and then click Roll Back to Version.

```
java.lang.IllegalStateException: Could not initialize keyed state backend.
   at org.apache.flink.streaming.api.operators.AbstractStreamOperator.initKeyedState(AbstractStreamOpe
rator.java:687)
   at org.apache.flink.streaming.api.operators.AbstractStreamOperator.initializeState(AbstractStreamOper
ator.java:275)
   at org.apache.flink.streaming.runtime.tasks.StreamTask.initializeOperators(StreamTask.java:870)
   at org.apache.flink.streaming.runtime.tasks.StreamTask.initializeState(StreamTask.java:856)
   at org.apache.flink.streaming.runtime.tasks.StreamTask.invoke(StreamTask.java:292)
   at org.apache.flink.runtime.taskmanager.Task.run(Task.java:762)
   at java.lang.Thread.run(Thread.java:834)
Caused by: org.apache.flink.api.common.typeutils.SerializationException: Cannot serialize/deserialize the o
bject.
   at com.alibaba.blink.contrib.streaming.state.AbstractRocksDBRawSecondaryState.deserializeStateEntry(
AbstractRocksDBRawSecondaryState.java:167)
   at com.alibaba.blink.contrib.streaming.state.RocksDBIncrementalRestoreOperation.restoreRawStateDat
a(RocksDBIncrementalRestoreOperation.java:425)
   at com.alibaba.blink.contrib.streaming.state.RocksDBIncrementalRestoreOperation.restore(RocksDBIncr
ementalRestoreOperation.java:119)
   at com.alibaba.blink.contrib.streaming.state.RocksDBKeyedStateBackend.restore(RocksDBKeyedStateBa
ckend.java:216)
   at org.apache.flink.streaming.api.operators.AbstractStreamOperator.createKeyedStateBackend(Abstract
StreamOperator.java:986)
   at org.apache.flink.streaming.api.operators.AbstractStreamOperator.initKeyedState(AbstractStreamOpe
rator.java:675)
   ... 6 more
Caused by: java.io.EOFException
   at java.io.DataInputStream.readUnsignedByte(DataInputStream.java:290)
   at org.apache.flink.types.StringValue.readString(StringValue.java:770)
   at org.apache.flink.api.common.typeutils.base.StringSerializer.deserialize(StringSerializer.java:69)
   at org.apache.flink.api.common.typeutils.base.StringSerializer.deserialize(StringSerializer.java:28)
   at org.apache.flink.api.java.typeutils.runtime.RowSerializer.deserialize(RowSerializer.java:169)
   at org.apache.flink.api.java.typeutils.runtime.RowSerializer.deserialize(RowSerializer.java:38)
   at com.alibaba.blink.contrib.streaming.state.AbstractRocksDBRawSecondaryState.deserializeStateEntry(
AbstractRocksDBRawSecondaryState.java:162)
   ... 11 more
```

11.4.10. Improve performance by manual configuration

11.4.10.1. Overview

You can manually configure resources to improve job performance using one of the following methods:

- Optimize resource configuration. You can modify the resources to improve the performance by reconfiguring parameters, such as parallelism, core, and heap_memory.
- Improve performance based on job parameter settings. You can specify the job parameters such as miniBatch to improve the performance.
- Improve upstream and downstream data storage based on parameter settings. You can specify related parameters to optimize the upstream and downstream storage for a job.

More details about these three methods are described in the following sections. After parameters are reconfigured to improve the performance of a job, the corresponding job must be re-published and started or resumed to apply the new configuration. The detailed process is provided in the following section.

11.4.10.2. Optimize resource configuration

Problem analysis

1. The percentage of input queues at task node 2 has reached 100%. Large amounts of data have piled up at task node 2, which results in the piling up of output queues at task node 1 in the upstream.
2. You can click task node 2 and find the subtask where the percentage of input queues has reached 100%. Then, click View TaskExecutor Logs to view the detailed information.
3. On the TaskExecutor page, you can view the CPU and memory usage. You can increase the number of CPU cores and expand the memory based on the current usage to handle the large amounts of data that have piled up.

Performance improvement

1. On the Development page of the RealtimeCompute development platform, click Properties.
2. Click Configure Resources to enter the page for editing resources.
3. Find the group (if any) or operator that corresponds to task node 2. You can modify the parameters of one operator or multiple operators in one group at a time.
   - Modify the parameters of multiple operators in a group.
   - Modify the parameters of an operator.
4. After modifying the parameters, click **Apply and Close the Page** in the upper-right corner of the page.

> **Note**
>
> If the resources of a group have increased but the performance is not improved, you need to separately analyze each operator in the group and find the abnormal operators. Then, you can modify the resources for the abnormal operators for performance tuning. To separately analyze each operator in a group, click the target operator and change the value of its chainingStrategy parameter to HEAD. If the value is already set to HEAD, click the next operator and change the value of its chainingStrategy parameter to HEAD. The values of the chainingStrategy parameter are as follows:
>
> - ALWAYS: indicates that operators are chained into a group.
> - NEVER: indicates that operators are not chained.
> - HEAD: indicates that operators are separated from a group.

Principles and recommendations

You can modify the following parameters:

- parallelism

  - Source

    Set the parallelism parameter based on the number of source table partitions. For example, if the number of sources is 16, set the parallelism parameter to 16, 8, or 4. Note that the maximum value is 16.

  - Operators

    Set the parallelism parameter based on the estimated queries per second (QPS). For tasks with low QPS, set the parallelism parameter for the operators to the same value as that for the sources. For tasks with high QPS, set the parallelism parameter to a larger value, such as 64, 128, or 256.

  - Sinks

    Set the parallelism parameter for the sinks to a value that is two or three times the number of downstream sink partitions. However, if the specified parallelism limit is exceeded, a write timeout or failure occurs. For example, if the number of downstream sinks is 16, the maximum value of the parallelism parameter for sinks is 48.

- core

  This parameter indicates the number of CPU cores. The default value is 0.1. Set this parameter based on CPU usage. We recommend that you set this parameter to a value whose reciprocal is an integer. The recommended value is 0.25.

- heap_memory

  This parameter indicates the heap memory size, whose default value is 256 MB. The value is determined based on the actual memory usage. You can click GROUP on the resource editing page to modify the preceding parameters.

- For the task nodes that use the GROUP BY operator, you can configure the state_size parameter.

  This parameter specifies the state size. The default value is 0. If the operator state is used, set the state_size parameter to 1. In this case, the corresponding job requests extra memory for this operator. The extra memory is used to store the state. If the state_size parameter is not set to 1, the corresponding job may be killed by YARN.

  > Note
  >
  > - The state_size parameter must be set to 1 for the following operators: GROUP BY, JOIN, OVER, and WINDOW.
  > - General users only need to focus on the core, parallelism, and heap_memory parameters.
  > - For each job, we recommend that you assign 4 GB memory for each core.

11.4.10.3. Improve performance based on job parameter settings

The miniBatch parameter can be used to optimize only GROUP BY operators. During the streaming data processing of Flink SQL, the state is read each time a data record arrives for processing, which consumes large amounts of high I/O resources. After the miniBatch parameter is set, the state is read only once for data records with the same key, and the output contains only the latest data record. This reduces the frequency of reading state and minimizes the data output updates. The settings of the miniBatch parameter are described as follows:

1. The allowed delay for a job.

```
blink.miniBatch.allowLatencyMs=5000
```

2. The size of a batch.

```
blink.miniBatch.size=1000
```

11.4.10.4. Optimize upstream and downstream data storage based on parameter settings

In Realtime Compute, each data record can trigger read and write operations on source and result tables. This brings considerable challenges for upstream and downstream data storage performance. To address these challenges, you can configure batch size parameters to specify the number of data records that are read from a source table or written to a result table at a time. The following table describes the available batch size parameters.

Parameter description

Object	Parameter	Description	Value
DataHub source table	batchReadSize	The number of data records that are read at a time.	Optional. Default value: 10.
DataHub result table	batchSize	The number of data records that are written at a time.	Optional. Default value: 300.
Log Service source table	batchGetSize	The number of log groups that are read at a time.	Optional. Default value: 10.
AnalyticDB for MySQL result table	batchSize	The number of data records that are written at a time.	Optional. Default value: 1000.
ApsaraDB RDS result table	batchSize	The number of data records that are written at a time.	Optional. Default value: 50.

Note To complete batch data read and write settings, add the parameters in the table to the WITH parameter list in DDL statements for the related data storage. For example, add `batchReadSize=’ 500'` to the WITH parameter list in DDL statements for the DataHub source table.

11.4.10.5. Apply new configuration

After resources are reconfigured for a job, you must restart or resume the job to apply the new configuration. Perform the following operations:

1. Publish the job of the new version. In the Publish New Version dialog box, select **Use Latest Configuration**.
2. Suspend the job.

3. Resume the job. In the Resume Job dialog box, select **Resume with Latest Configuration**. Otherwise, the resource configuration cannot take effect.
4. After resuming the job, choose **Administration** > **Overview** > **Vertex Topology** to check whether the new configuration has taken effect.

> **Note**
>
> We do not recommend that you terminate and restart a job to apply the new configuration. After a job is terminated, its status is cleared. In this case, the computing result may be inconsistent with the result that is obtained if you suspend and resume the job.

11.4.10.6. Concepts

- Global

  isChainingEnabled: indicates whether the chaining is enabled. Use the default value (true).

- Nodes
  - id: specifies the unique ID of a node. The ID is automatically generated and does not need to be changed.
  - uid: specifies the UID of a node, which is used to calculate the operator ID. If this parameter is not specified, the value of id is used.
  - pact: specifies the type of a node, such as the data source, operator, and data sink. Use the default value.
  - name: specifies the name of a node, which can be customized.
  - slotSharingGroup: Use the default value.
  - chainingStrategy: specifies the chaining strategy. The options include HEAD, ALWAYS, and NEVER. Use the default value.
  - parallelism: specifies the number of parallel subtasks. The default value is 1. You can increase the value based on the data volume.
  - core: specifies the number of CPU cores. The default value is 0.1. The value is configured based on the CPU usage. We recommend that you set this parameter to a value whose reciprocal is an integer. The recommended value is 0.25.
  - heap_memory: specifies the heap memory size. The default value is 256 MB. Set this parameter based on the memory usage.
  - direct_memory: specifies the JVM non-heap memory size. We recommend that you use the default value (0).
  - native_memory: specifies the JVM non-heap memory size for the Java Native Interface (JNI). The default value is 0. The recommended value is 10 MB.

- Chain

A Flink SQL task is a directed acyclic graph (DAG) that contains many nodes, which are also known as operators. Some upstream and downstream operators can be combined to form a chain when they are running. The CPU capacity of a chain is set to the maximum CPU capacity among operators in the chain. The memory size of a chain is set to the total memory size of operators in the chain. For example, after node 1 (256 MB, 0.2 cores), node 2 (128 MB, 0.5 cores), and node 3 (128 MB, 0.25 cores) are combined to form a chain, the CPU capacity of the chain is 0.5 cores and the memory is 512 MB. The prerequisite for chaining operators is that the operators to be chained must have the same parallelism settings. However, some operators cannot be chained, such as GROUP BY operators. We recommend that you chain operators to improve the efficiency of network transmission.

11.4.11. O&M of Apsara Big Data Manager

11.4.11.1. What is Apsara Big Data Manager?

Apsara Big Data Manager (ABM) provides O&M on big data products from the perspective of business, services, clusters, and hosts. You can also upgrade big data products, customize alert configurations, and view the O&M history in the ABM console.

Onsite Apsara Stack engineers can use ABM to easily manage big data products. They can view resource usage, check and handle alerts, and modify configurations.

For more information about the logon methods and O&M operations of Realtime Compute in the ABM console, see the following topics.

11.4.11.2. Log on to the ABM console

This topic describes how to log on to the Apsara Big Data Manager (ABM) console.

Prerequisites

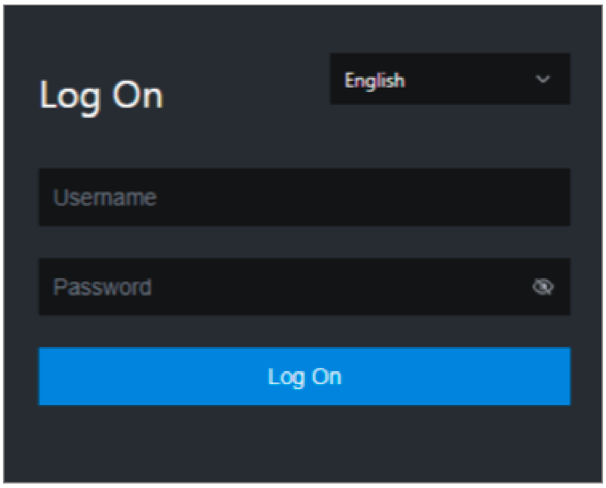
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.



> Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   > Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

   When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   For security reasons, your password must meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password must be 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Product Management** > **Products**.
7. In the **Big Data Services** section, choose **General-Purpose O&M** > **Apsara Big Data Manager**.

11.4.11.3. O&M overview of Realtime Compute for Apache Flink

This topic describes the O&M features of Realtime Compute for Apache Flink supported by Apsara Bigdata Manager (ABM). It also shows how to access the O&M page of Realtime Compute for Apache Flink.

Modules

O&M of Realtime Compute for Apache Flink includes business O&M, service O&M, cluster O&M, and host O&M. The following table describes these modules.

Module	Feature	Description
Business	Item	Displays information about all projects in Realtime Compute for Apache Flink.
	Job	Displays information about all jobs in Realtime Compute for Apache Flink and supports job diagnosis and analysis.
	Queues	Displays information about all queues in Realtime Compute for Apache Flink.
Services	Blink	Displays the overview of the Blink service in Realtime Compute for Apache Flink.
	Yarn	Displays the overview and health status of the YARN service in Realtime Compute for Apache Flink.
	HDFS	Displays the overview and health status of the HDFS service in Realtime Compute for Apache Flink.
Clusters	Overview	Displays the overall running and health check information about a cluster. On this page, you can view the health check result and health check history of the cluster. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, and packet transmission for the cluster.
	Health Status	Displays all check items of a cluster, including the check item details, check results for the hosts in the cluster, and methods to handle alerts. In addition, you can log on to a host and perform manual checks on the host.
	Hosts	Displays the information about hosts in a cluster, including the hostname, IP address, role, type, CPU utilization, memory usage, root disk usage, packet loss rate, and packet error rate.
Hosts	Overview	Displays the overall running and health check information about a host. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.
	Health Status	Displays the check items of the selected host, including the check item details, check results for the host, and methods to handle alerts. In addition, you can log on to the host and perform manual checks on the host.

Entry

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner of the ABM console, and then click **RealtimeCompute**.
3. On the RealtimeCompute page, click **O&M** in the upper-right corner. The **Business** page appears by

default.

The **O&M** page includes four modules, **Business**, **Services**, **Clusters**, and **Hosts**.

11.4.11.4. Business O&M

11.4.11.4.1. Projects

This topic describes how to view information about the projects in Realtime Compute and how to go to the Queue Analysis page from the Projects page.

Projects

On the **Business** page, click **Projects** in the left-side navigation pane. The **Projects** page for Realtime Compute appears.

The **Projects** page displays information about the projects in Realtime Compute, including the name, BRS, queue, used compute units (CUs), total CUs, CU usage percentage, and number of jobs.

Go to the Queue Analysis page

The Queue Analysis page displays the status and resource usage of a queue, and information about jobs running in the queue, so that you can quickly know the running status of the queue.

On the **Projects** page, click a queue in the Queue column. The **Queue Analysis** page of the queue appears. For more information about the Queue Analysis page and operations that you can perform on this page, see Queues.

11.4.11.4.2. Jobs

This topic describes how to view information about the jobs in Realtime Compute and how to go to the Job Analysis page, Queue Analysis page, and Realtime Compute console from the Jobs page.

Jobs

On the **Business** page, click **Jobs** in the left-side navigation pane. The **Jobs** page for Realtime Compute appears.

The **Jobs** page displays information about the jobs in Realtime Compute, including the job names, users who created the jobs, projects to which the jobs belong, queues where the jobs are running, transactions per second (TPS) in the inbound direction, job latency, requested compute units (CUs), job statuses, and start time.

Go to the Realtime Compute console

On the **Jobs** page, click the content in the Failover column of a job to go to the Realtime Compute console.

Go to the Job Analysis page

The job analysis feature allows you to diagnose jobs to quickly troubleshoot job failures.

On the **Jobs** page, click a job in the Name column. The **Job Analysis** page of the job appears. For more information about the Job Analysis page and operations that you can perform on this page, see Job analysis.

Go to the Queue Analysis page

The Queue Analysis page displays the status and resource usage of a queue, and information about jobs running in the queue, so that you can quickly know the running status of the queue.

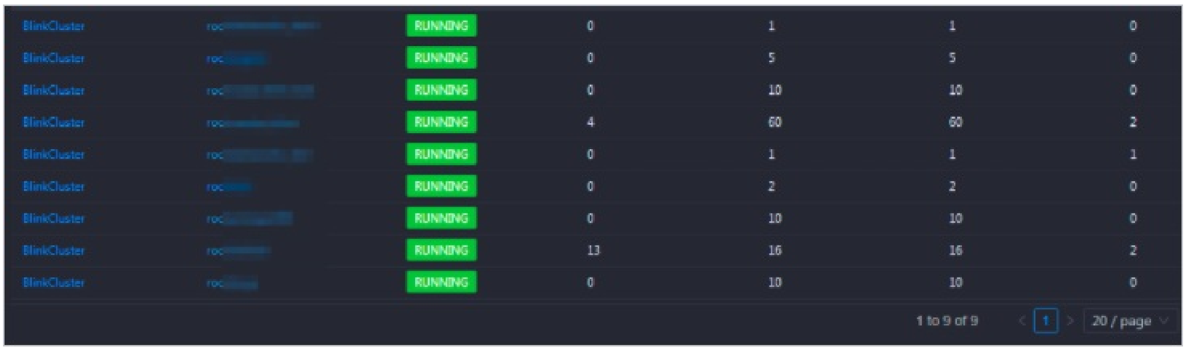
On the **Jobs** page, click a queue in the Queue column. The **Queue Analysis** page of the queue appears. For more information about the Queue Analysis page and operations that you can perform on this page, see Queues.

11.4.11.4.3. Queues

Apsara Big Data Manager (ABM) allows you to view the information about the queues in Realtime Compute, including the queue names, queue statuses, minimum numbers of CPU cores and minimum memory capacity guaranteed for the queues, maximum numbers of CPU cores and maximum memory capacity available for the queues, and numbers of jobs running in the queues.

Queues

On the **Business** page, click **Queues** in the left-side navigation pane. The **Queues** page for Realtime Compute appears.



BlinkCluster	roc[redacted]	RUNNING	0	1	1	0
BlinkCluster	roc[redacted]	RUNNING	0	5	5	0
BlinkCluster	roc[redacted]	RUNNING	0	10	10	0
BlinkCluster	roc[redacted]	RUNNING	4	60	60	2
BlinkCluster	roc[redacted]	RUNNING	0	1	1	1
BlinkCluster	roc[redacted]	RUNNING	0	2	2	0
BlinkCluster	roc[redacted]	RUNNING	0	10	10	0
BlinkCluster	roc[redacted]	RUNNING	13	16	16	2
BlinkCluster	roc[redacted]	RUNNING	0	10	10	0

The **Queues** page displays information about the queues in Realtime Compute, including the clusters to which the queues belong, queue names, queue statuses, requested compute units (CUs), minimum CUs guaranteed, maximum CUs available, and numbers of jobs running in the queues.

Go to the Queue Analysis page

The Queue Analysis page displays the status and resource usage of a queue, and information about jobs running in the queue, so that you can learn the running status of the queue.

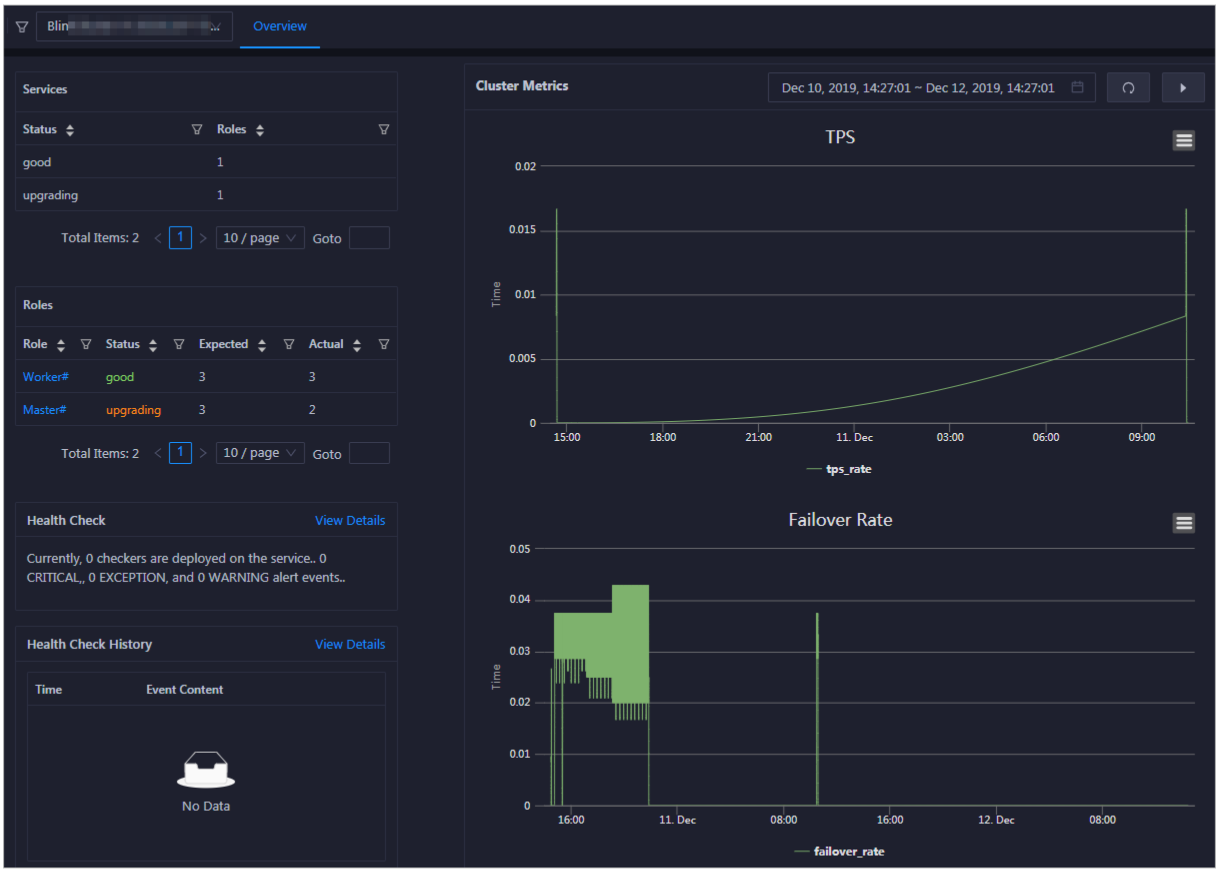
On the **Queues** page, click a queue in the Queue column. The **Queue Analysis** page of the queue appears. For more information about the Queue Analysis page and operations that you can perform on this page, see Queues.

11.4.11.5. Service O&M

11.4.11.5.1. Blink

Apsara Big Data Manager (ABM) allows you to view the overview of the Blink service in Realtime Compute.

On the **Services** page, click **Blink** in the left-side navigation pane. The **Overview** page for the Blink service appears.



Blin[redacted] | Overview

Services

Status	Roles
good	1
upgrading	1

Total Items: 2 < 1 > 10 / page Goto

Roles

Role	Status	Expected	Actual
Worker#	good	3	3
Master#	upgrading	3	2

Total Items: 2 < 1 > 10 / page Goto

Health Check View Details

Currently, 0 checkers are deployed on the service.. 0 CRITICAL,, 0 EXCEPTION, and 0 WARNING alert events..

Health Check History View Details

Time	Event Content

No Data

Cluster Metrics Dec 10, 2019, 14:27:01 ~ Dec 12, 2019, 14:27:01

The **Overview** page displays the overview, status, health check result, and health check history, as well as two core cluster metrics, transactions per second (TPS) and failover rate, of the Blink service.

11.4.11.5.2. Yarn

Apsara Big Data Manager (ABM) allows you to view the overview and health status of the YARN service in Realtime Compute.

Overview

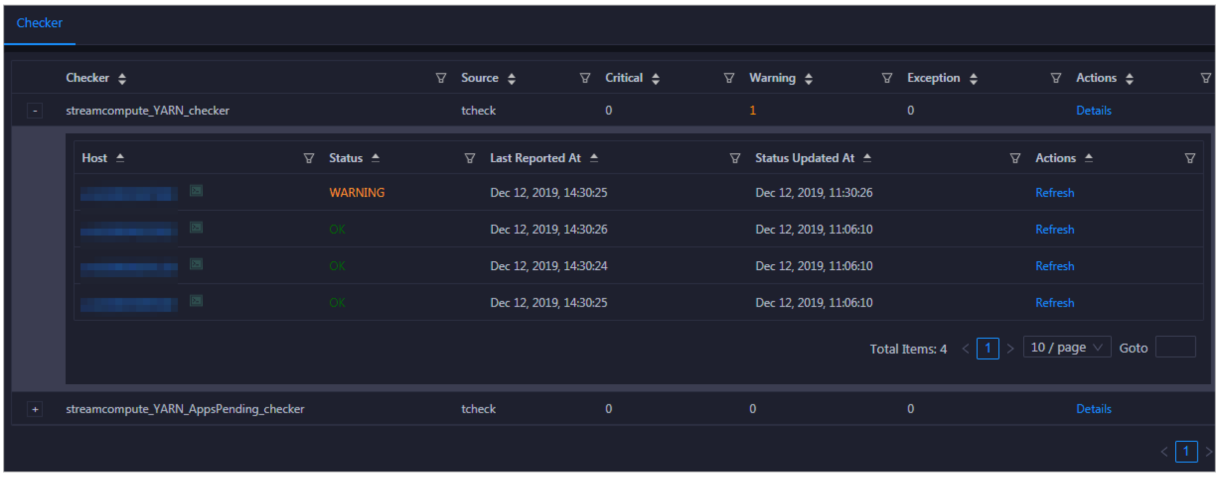
On the **Services** page, click **Yarn** in the left-side navigation pane. The **Overview** page for the YARN service appears.

The **Overview** page displays the health check result, health check history, application status, container status, node status, logical CPU usage, and logical memory usage for the YARN service.

Click **View Details** in the **Health Check** or **Health Check History** section. The **Health Status** page for the YARN service appears. On this page, you can view more details about the health check.

Heath status

On the **Services** page, click **Yarn** in the left-side navigation pane. Click the **Health Status** tab on the top of the Services page. The **Health Status** page for the YARN service appears.



Checker

	Checker	Source	Critical	Warning	Exception	Actions
-	streamcompute_YARN_checker	tcheck	0	1	0	Details
+	streamcompute_YARN_AppsPending_checker	tcheck	0	0	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
[redacted]	WARNING	Dec 12, 2019, 14:30:25	Dec 12, 2019, 11:30:26	Refresh
[redacted]	OK	Dec 12, 2019, 14:30:26	Dec 12, 2019, 11:06:10	Refresh
[redacted]	OK	Dec 12, 2019, 14:30:24	Dec 12, 2019, 11:06:10	Refresh
[redacted]	OK	Dec 12, 2019, 14:30:25	Dec 12, 2019, 11:06:10	Refresh

Total Items: 4 < 1 > 10 / page Goto

On the **Health Status** page, you can view all checkers of the YARN service and the check results for all hosts. The following alerts may be reported on a host: **Critical**, **Warning**, and **Exception**. The alerts are repesented in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

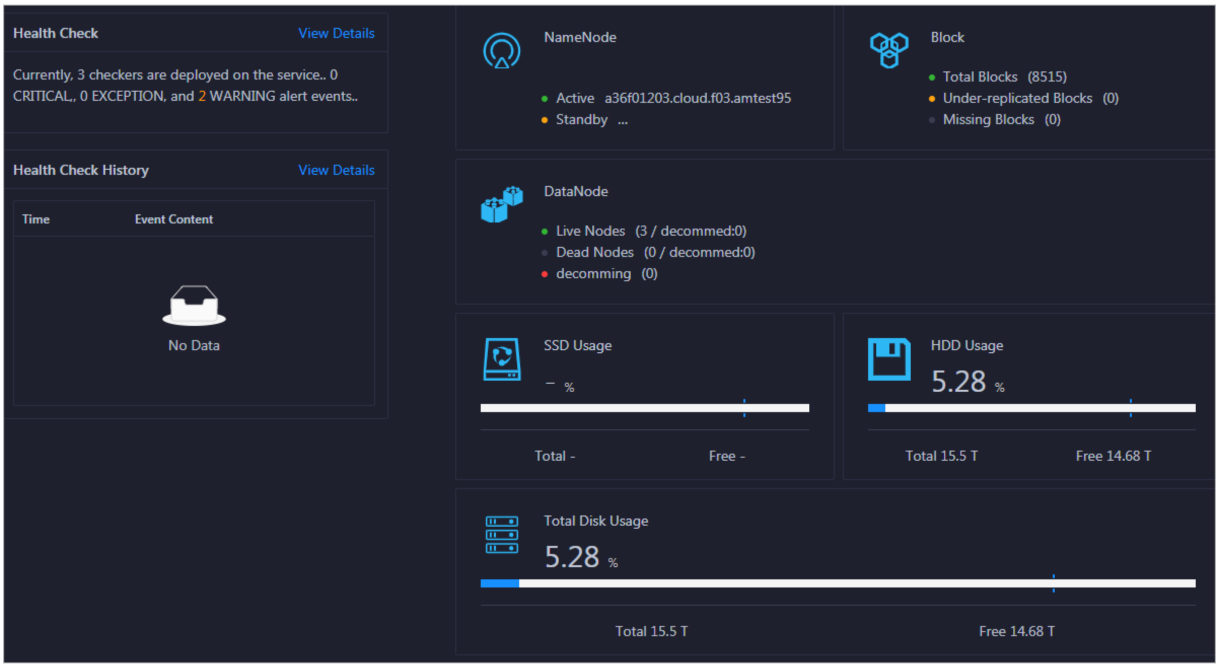
The operations you can perform on the **Health Status** page for the YARN service are the same as those on the Health Status page for Realtime Compute clusters. For more information, see Cluster health.

11.4.11.5.3. HDFS

Apsara Big Data Manager (ABM) allows you to view the overview and health status of the Hadoop Distributed File System (HDFS) service in Realtime Compute.

Overview

On the **Services** page, click **HDFS** in the left-side navigation pane. The **Overview** page for the HDFS service appears.



Health Check — View Details

Currently, 3 checkers are deployed on the service.. 0 CRITICAL,, 0 EXCEPTION, and 2 WARNING alert events..

Health Check History — View Details

Time	Event Content

No Data

NameNode

- Active a36f01203.cloud.f03.amtest95
- Standby ...

Block

- Total Blocks (8515)
- Under-replicated Blocks (0)
- Missing Blocks (0)

DataNode

- Live Nodes (3 / decommed:0)
- Dead Nodes (0 / decommed:0)
- decomming (0)

SSD Usage: - % — Total - Free -

HDD Usage: 5.28 % — Total 15.5 T Free 14.68 T

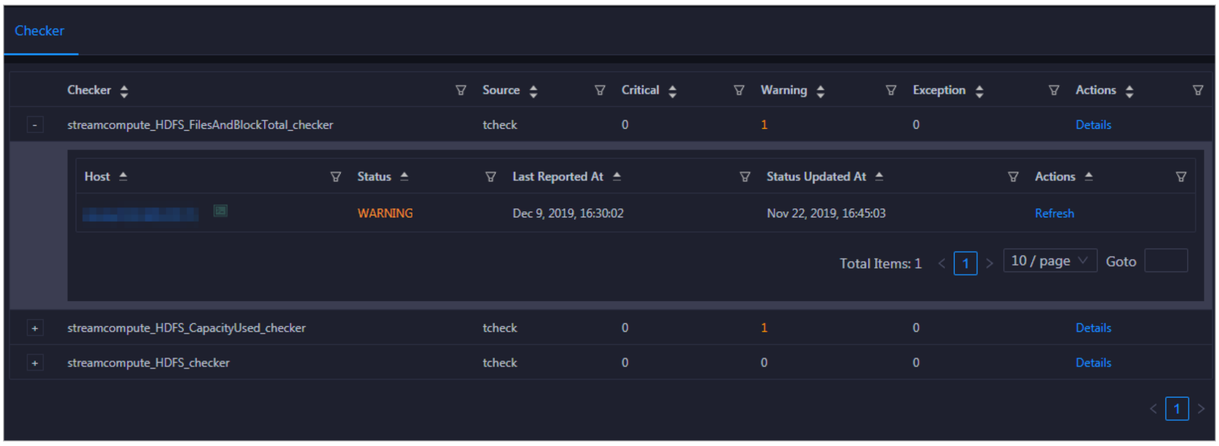
Total Disk Usage: 5.28 % — Total 15.5 T Free 14.68 T

The **Overview** page displays the health check result, health check history, the information of NameNode, blocks, and DataNode, solid-state disk (SSD) usage, hard disk drive (HDD) usage, and total disk usage.

Click **View Details** in the **Health Check** or **Health Check History** section. The **Health Status** page for the HDFS service appears. On this page, you can view more details about the health check.

Health status

On the **Services** page, click **HDFS** in the left-side navigation pane. Click the **Health Status** tab on the top of the Services page. The **Health Status** page for the HDFS service appears.



Checker

	Checker	Source	Critical	Warning	Exception	Actions
-	streamcompute_HDFS_FilesAndBlockTotal_checker	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
[redacted]	WARNING	Dec 9, 2019, 16:30:02	Nov 22, 2019, 16:45:03	Refresh

Total Items: 1 < 1 > 10 / page Goto

	Checker	Source	Critical	Warning	Exception	Actions
+	streamcompute_HDFS_CapacityUsed_checker	tcheck	0	1	0	Details
+	streamcompute_HDFS_checker	tcheck	0	0	0	Details

< 1 >

On the **Health Status** page, you can view all checkers of the HDFS service and the check results for all hosts in the cluster. The following check results can be returned: **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

The operations you can perform on the **Health Status** page for the HDFS service are the same as those on the Health Status page for Realtime Compute clusters. For more information, see Cluster health.

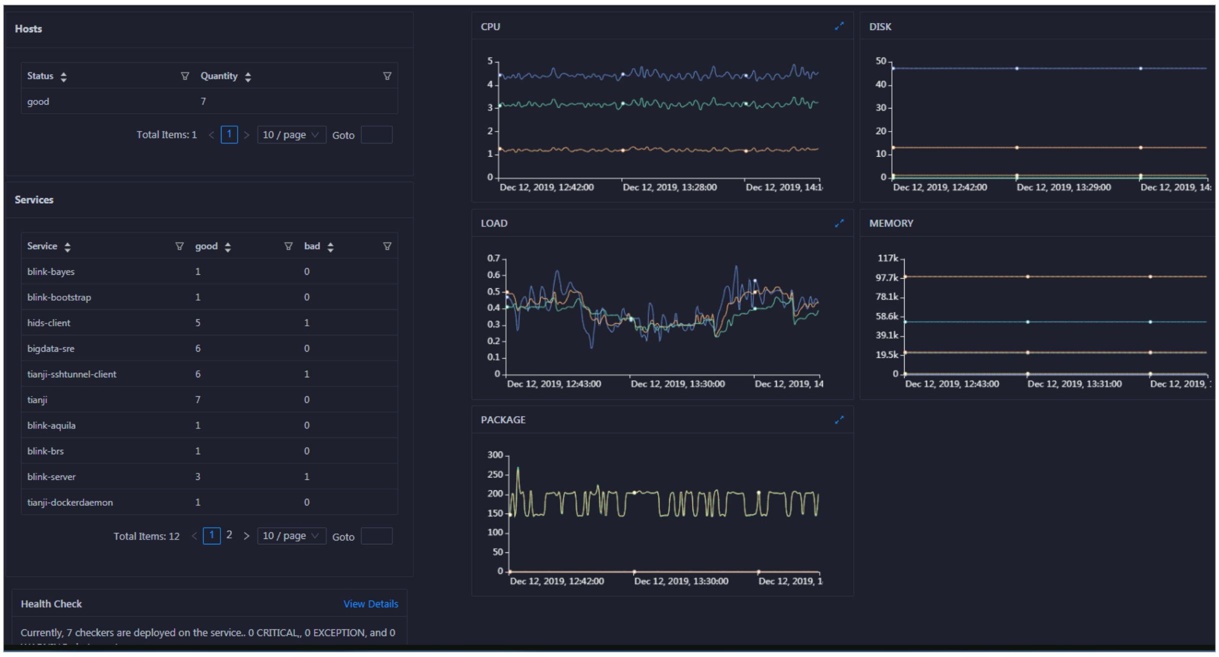
11.4.11.6. Cluster O&M

11.4.11.6.1. Cluster overview

The cluster overview page displays the overall running and health check information about a cluster. On this page, you can view the health check result and health check history of the cluster. You can also view the trend charts of CPU usage, disk usage, memory usage, load, and packet transmission for the cluster.

Entry

On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Overview** tab. The **Overview** page for the cluster appears.



Hosts

Status	Quantity
good	7

Total Items: 1 < 1 > 10 / page Goto

Services

Service	good	bad
blink-bayes	1	0
blink-bootstrap	1	0
hids-client	5	1
bigdata-sre	6	0
tianji-sshtunnel-client	6	1
tianji	7	0
blink-aquila	1	0
blink-brs	1	0
blink-server	3	1
tianji-dockerdaemon	1	0

Total Items: 12 < 1 2 > 10 / page Goto

Health Check View Details

Currently, 7 checkers are deployed on the service.. 0 CRITICAL,, 0 EXCEPTION, and 0

Hosts

This section displays all host statuses and the number of hosts in each status. The host statuses include **good** and **bad**.

Services

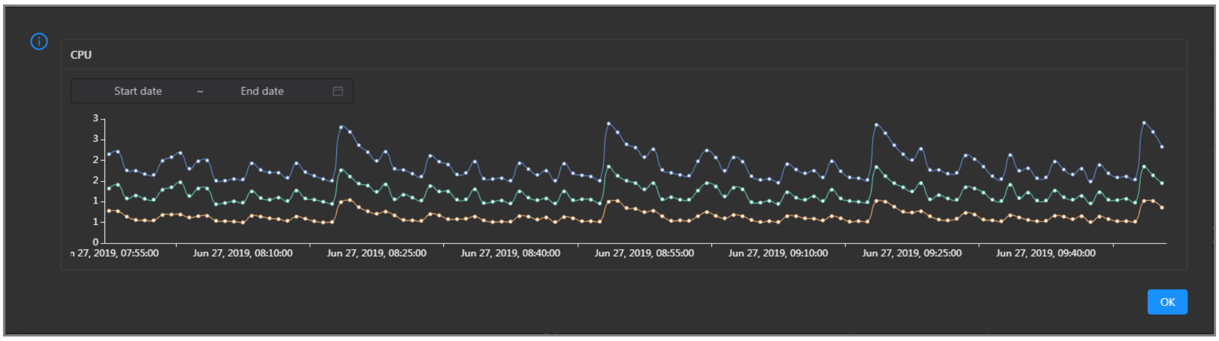
This section displays all services deployed in the cluster and the respective number of available and unavailable services.

CPU

This chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

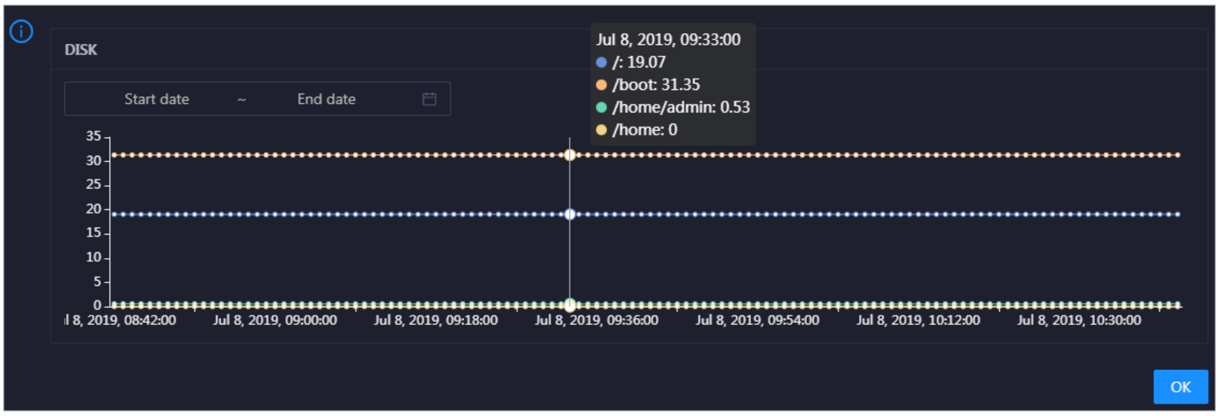
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the cluster in the specified period.



DISK

This chart shows the trend lines of the storage usage on the */*, */boot*, */home/admin*, and */home* directories for the cluster over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

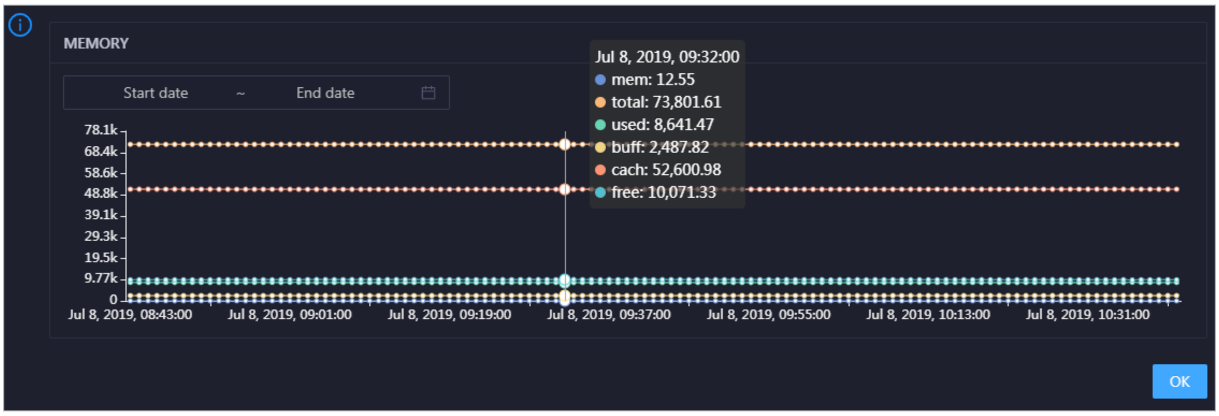


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

MEMORY

This chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

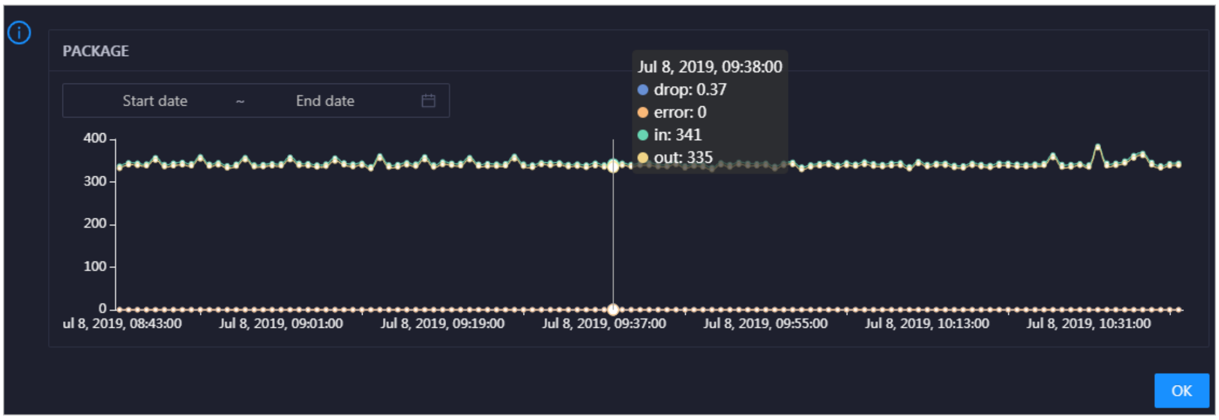


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the cluster in the specified period.

PACKAGE

This chart shows the trend lines of the numbers of dropped packets (drop), error packets (error), received packets (in), and sent packets (out) for the cluster in different colors. These trend lines reflect the data transmission status of the cluster.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

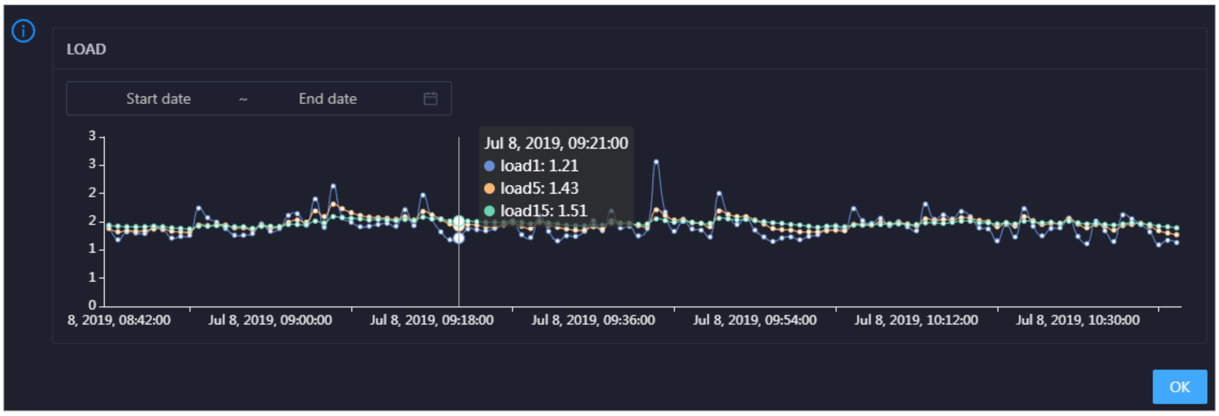


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the cluster in the specified period.

LOAD

This chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the cluster in different colors.

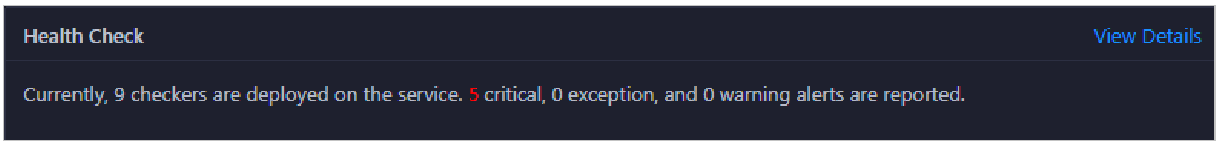
In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the cluster in the specified period.

Health Check

This section displays the number of checkers deployed for the cluster and the respective number of Critical, Warning, and Exception alerts.



Currently, 9 checkers are deployed on the service. 5 critical, 0 exception, and 0 warning alerts are reported.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Cluster health.

Health Check History

This section displays a record of the health checks performed on the cluster.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Cluster health.

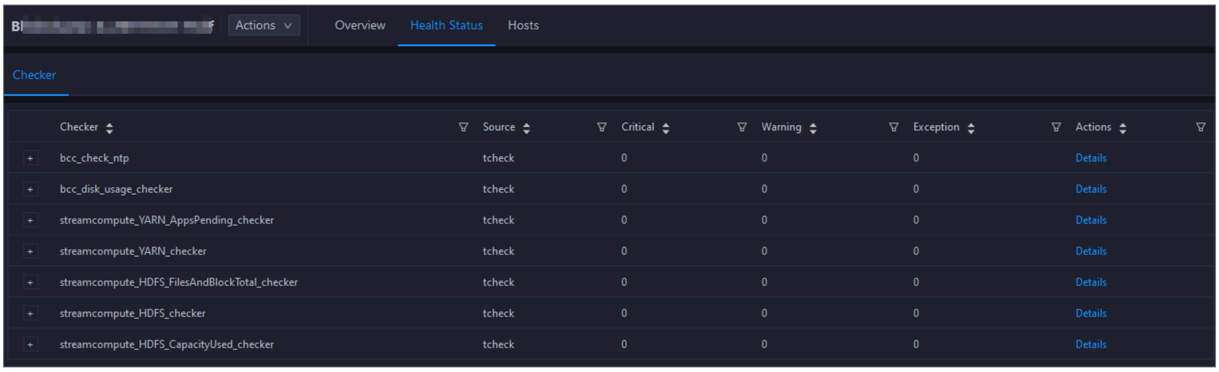
You can click the event content of a check to view the exception items.

11.4.11.6.2. Cluster health

On the Health Status page, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Entry

On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Health Status** tab. The Health Status page for the cluster appears.

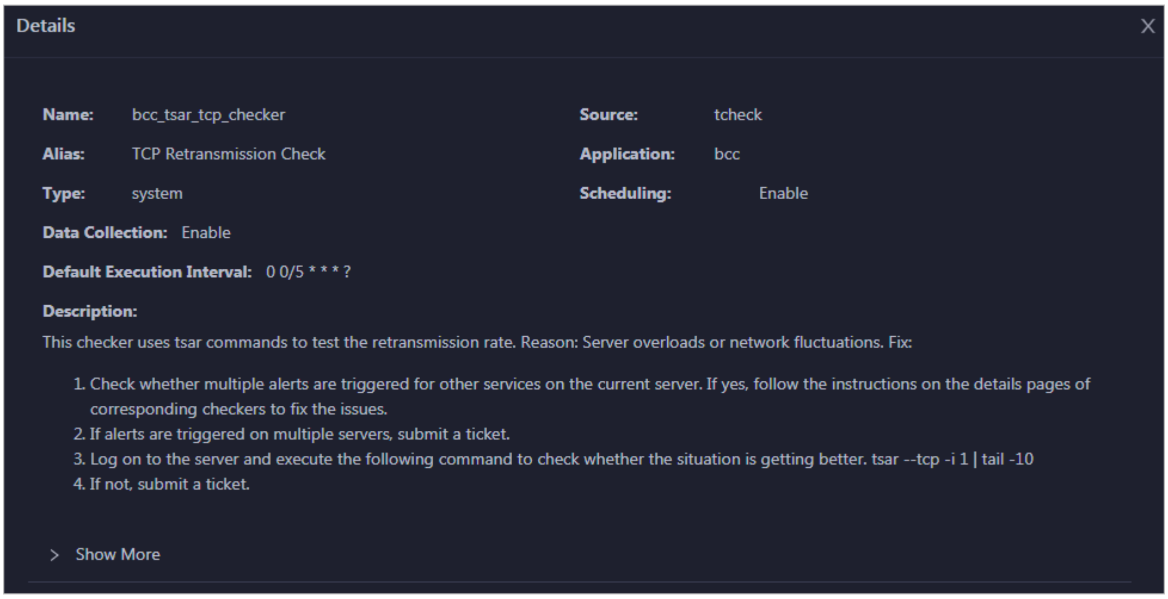


	Checker	Source	Critical	Warning	Exception	Actions
+	bcc_check_ntp	tcheck	0	0	0	Details
+	bcc_disk_usage_checker	tcheck	0	0	0	Details
+	streamcompute_YARN_AppsPending_checker	tcheck	0	0	0	Details
+	streamcompute_YARN_checker	tcheck	0	0	0	Details
+	streamcompute_HDFS_FilesAndBlockTotal_checker	tcheck	0	0	0	Details
+	streamcompute_HDFS_checker	tcheck	0	0	0	Details
+	streamcompute_HDFS_CapacityUsed_checker	tcheck	0	0	0	Details

On the **Health Status** tab, you can view all checkers for the cluster and the check results for the hosts in the cluster. The following alerts may be reported on a host: **CRITICAL**, **WARNING**, and **EXCEPTION**. The alerts are represented in different colors. You must handle the alerts in a timely manner, especially the **CRITICAL** and **WARNING** alerts.

View checker details

1. On the Health Status tab, click **Details** in the Actions column of a checker. On the Details page, view checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

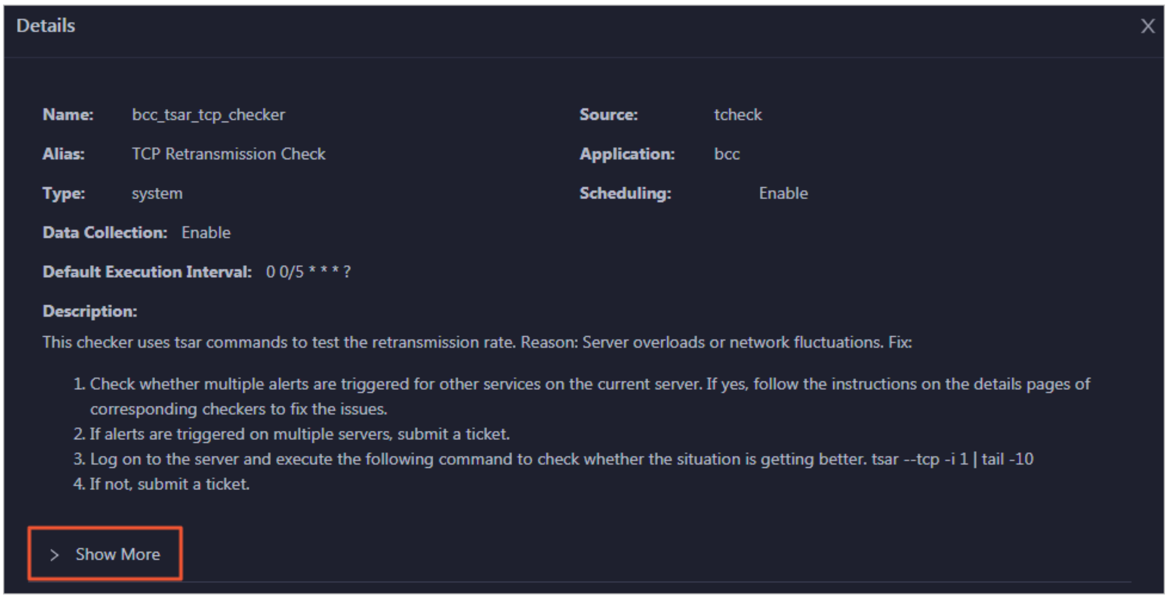
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include **Name**, **Source**, **Alias**, **Application**, **Type**, **Scheduling**, **Data Collection**, **Default Execution Interval**, and **Description**. The schemes to clear alerts are provided in the description.

2. Click **Show More** to view more information about the checker.


Details

Name: bcc_tsar_tcp_checker

Alias: TCP Retransmission Check

Type: system

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Source: tcheck

Application: bcc

Scheduling: Enable

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

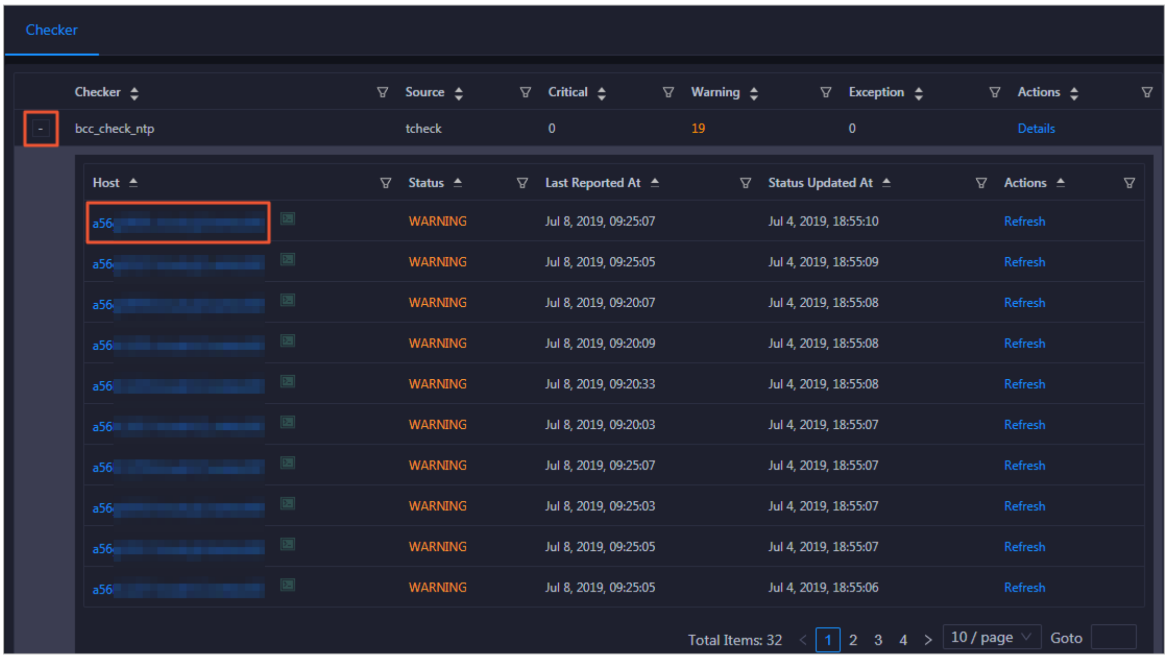
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about **Script**, **Target (TianJi)**, **Default Threshold**, and **Mount Point**.

View the hosts for which alerts are reported and causes for the alerts

You can view the check history and check results of a checker on a host.

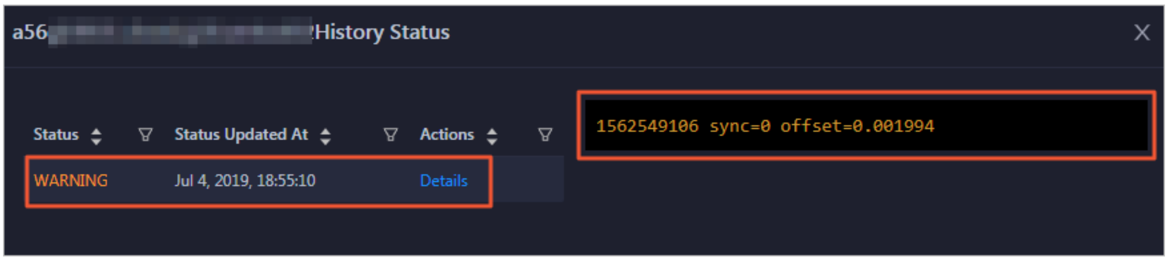
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported. You can view all hosts where the checker is run.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:06	Refresh

2. Click a hostname. In the panel that appears, click **Details** in the Actions column of a check result to view the cause of the alert.



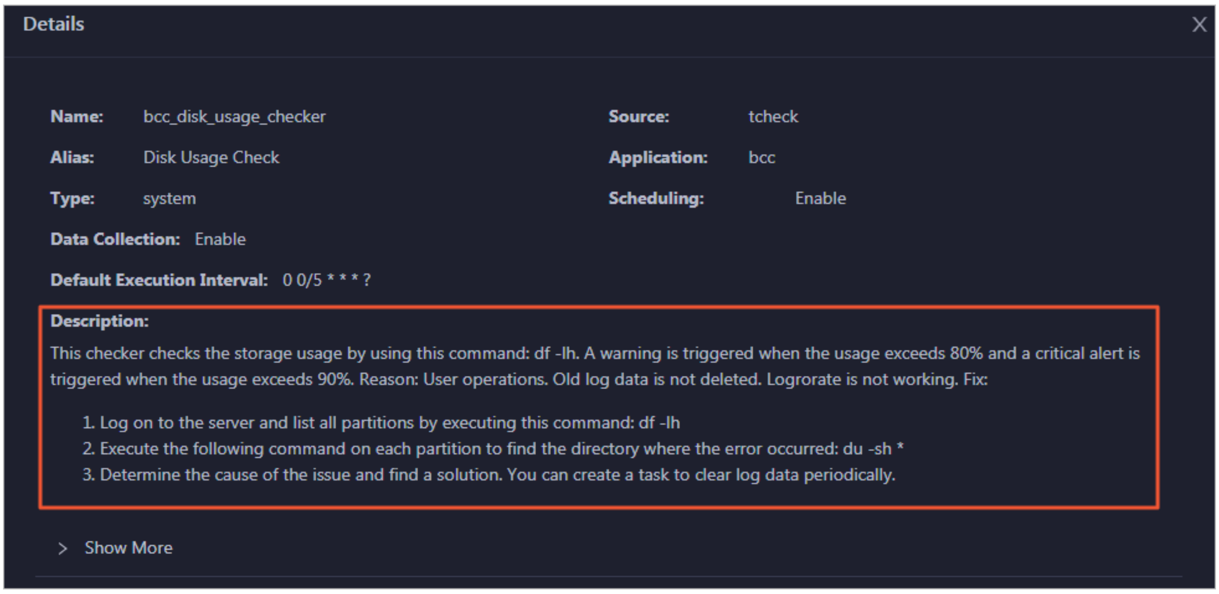
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status tab, click **Details** in the Actions column of a checker for which alerts are reported. On the Details page, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

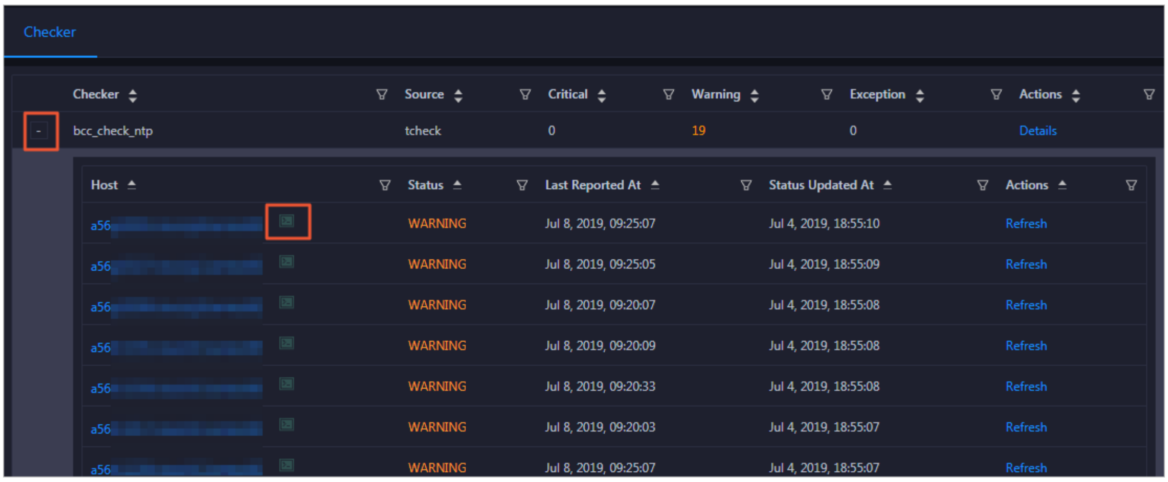
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

You may need to log on to a host to handle alerts or other issues that occurred on the host.

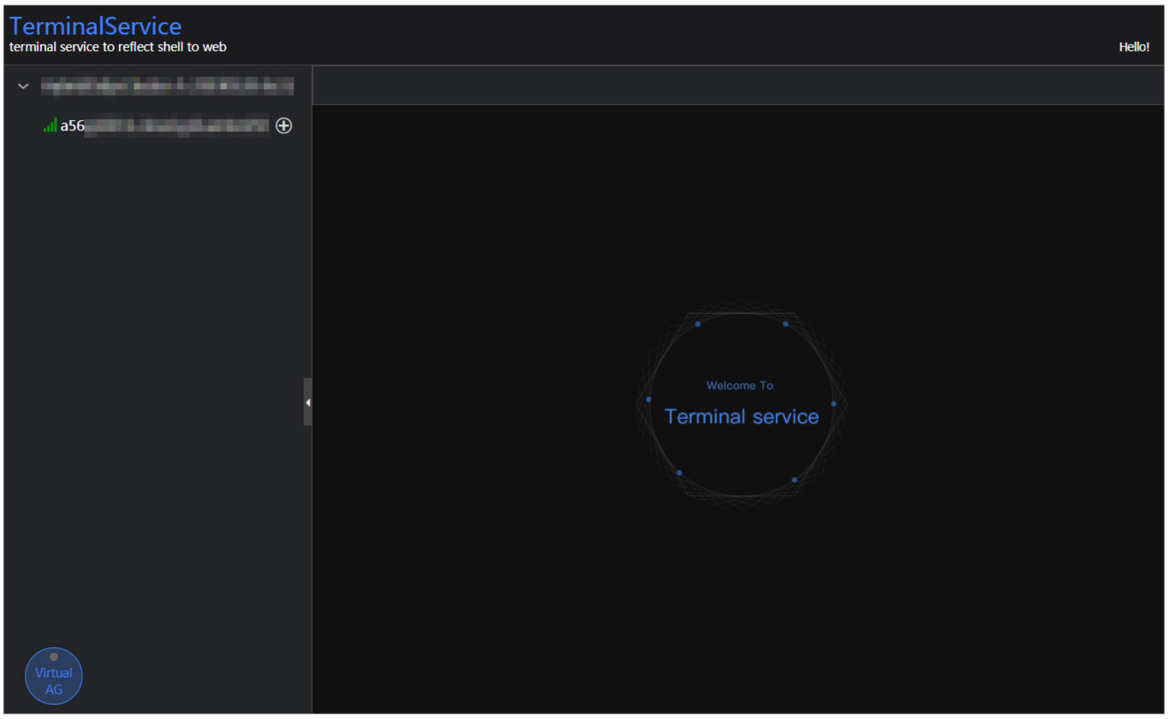
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported.



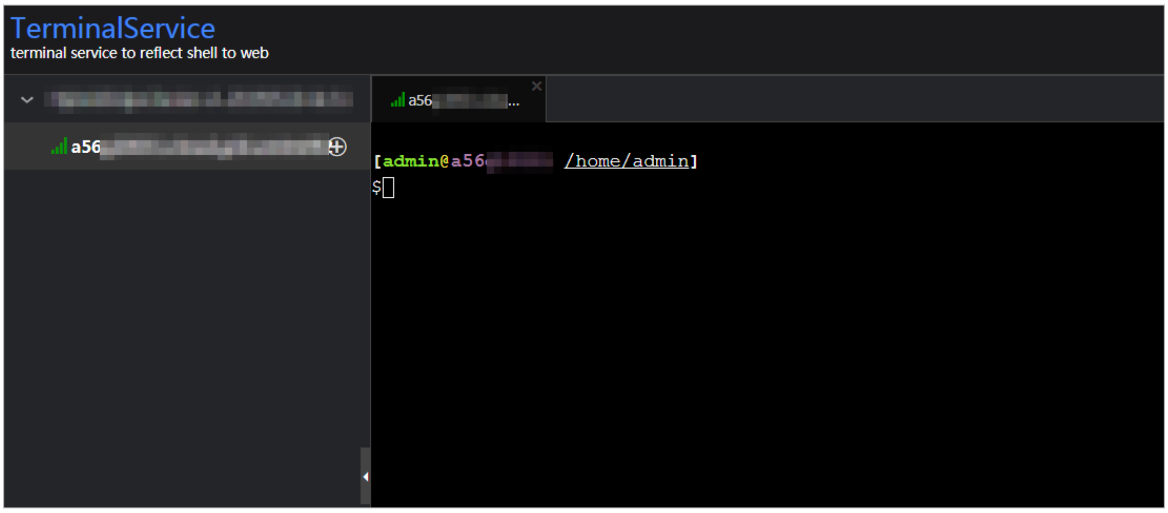
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

2. Click the **Login in** icon of a host. The **TerminalService** page appears.



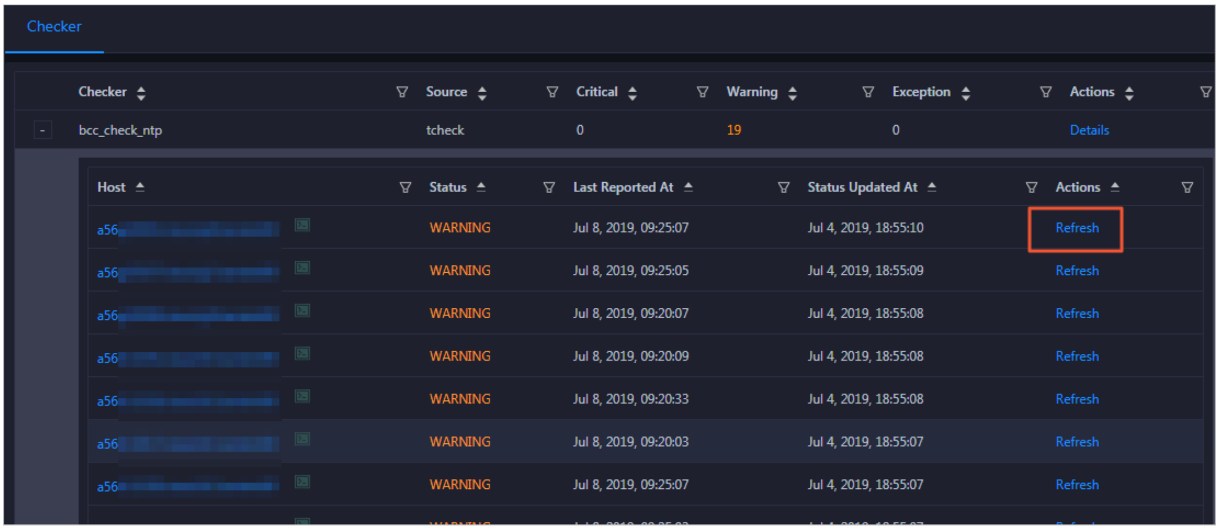
3. On the **TerminalService** page, click the hostname in the left-side navigation pane to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. This way, you can check whether the alert is cleared.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

11.4.11.6.3. Hosts

The Hosts page displays information about hosts, including the hostname, IP address, role, type, CPU usage, total memory size, available memory size, load, root disk usage, packet loss rate, and packet error rate.

On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Hosts** tab. The **Hosts** page for the cluster appears.

To view more information about a host, click the name of the host. The Overview tab of the Hosts page appears. For more information, see Host overview.

11.4.11.6.4. Cluster scale-out

Apsara Big Data Manager (ABM) allows you to scale out a Realtime Compute cluster by adding physical hosts. Cluster scale-out refers to the process of adding physical hosts in the default cluster of Apsara Infrastructure Management Framework to a Realtime Compute cluster. You can perform the scale-out operation only for **worker** nodes in a Realtime Compute cluster.

Prerequisites

- Your ABM account is granted the required permissions to perform O&M operations on Realtime Compute.
- Hosts whose service type is **blink** are deployed in the default cluster of Apsara Infrastructure Management Framework.

Background information

In Apsara Stack, scaling out a cluster involves complex operations. You need to configure a new physical host on Deployment Planner so that it can be added to the default cluster of Apsara Infrastructure Management Framework. The default cluster of Apsara Infrastructure Management Framework can be considered as a resource pool that can provide resources for scaling out business clusters. To scale out a cluster, add physical hosts in the default cluster of Apsara Infrastructure Management Framework to the cluster. To scale in a cluster, remove physical hosts from the cluster to the default cluster of Apsara Infrastructure Management Framework.

Step 1: Obtain the name of the host that is to be added to a Realtime Compute cluster

Before the scale-out operation, obtain the name of the available host in the default cluster of Apsara Infrastructure Management Framework.

1. Log on to the ABM console.
2. Click the ⊞ icon in the upper-left corner, and click **TIANJI** to log on to the Apsara Infrastructure Management Framework console.
3. In the top navigation bar of the page that appears, choose **Operations > Machine Operations**.
4. On the **Machine Operations** page, search for a host whose service type is **blink** in the default cluster. Copy the name of the host.

Step 2: Add the host to a Realtime Compute cluster

You can add multiple hosts to a Realtime Compute cluster at a time to scale out the cluster. To achieve this, you must specify an existing host as the template host. When you scale out the Realtime Compute cluster, the hosts copy configurations from the template host so that they can be added to the cluster at a time.

1. Log on to the ABM console.
2. Click the ⊞ icon in the upper-left corner, and click **StreamCompute**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Business** page appears by default.
4. Click the **Clusters** tab. On the page that appears, click the **Hosts** tab, and select a host whose Role is **Worker** as the template host.
5. Choose **Actions > Scale out Cluster** in the upper-left corner. In the **Scale out Cluster** pane, configure the required parameters.

   You must configure the following parameters in this step:

   - **Refer Hostname**: the name of the template host. By default, the name of the selected host is used.
   - **Hostname**: the name of the host that you want to add to the Realtime Compute cluster. The drop-down list displays all available hosts in the default cluster for scale-out. You can select one or more hosts from the drop-down list.
6. Click **Run**. A message appears, indicating that the action is submitted.
7. View the scale-out status.

   Move the pointer over **Actions** in the upper-left corner, and click **Execution History** next to **Scale out Cluster** to view the scale-out history.

   It may take some time for the cluster to be scaled out. In the Current Status column, **RUNNING** indicates that the scale-out operation is in progress, **SUCCESS** indicates that the scale-out operation succeeds, and **FAILED** indicates that the scale-out operation fails.

Step 3: View the scale-out progress

If the status is **RUNNING**, click **Details** in the Details column to check the current step and progress of the scale-out operation.

Step 4: Optional. Locate the cause of a scale-out failure

If the status is **FAILED**, click **Details** in the Details column to locate the failure cause.

You can also view information about parameter settings, host details, scripts, and execution parameters to locate the failure cause.

11.4.11.6.5. Cluster scale-in

Apsara Big Data Manager (ABM) allows you to remove physical hosts to scale in a Realtime Compute cluster. Cluster scale-in refers to the process of removing physical hosts from a Realtime Compute cluster to the default cluster of Apsara Infrastructure Management Framework. Scale-in operations can be performed only on the **worker** nodes in a Realtime Compute cluster.

Prerequisites

- Your ABM account is granted the required permissions to perform O&M operations on Realtime Compute.
- More than three **worker** nodes are deployed in the current cluster. A Realtime Compute cluster creates three replicas for data by default. At least three **worker** nodes are required. Make sure that the cluster has at least three worker nodes after scale-in.
- Resources of the cluster, including the disk, CPU, and memory, are checked and still sufficient if the cluster is scaled in. For more information about how to check CPU and memory usage, see Yarn. You can run the **df** command to check disk usage.

> **Notice** Scale-in triggers a job failover on hosts. If the cluster resources are insufficient after scale-in, the failover fails. This leads to negative effects on your business.

Background information

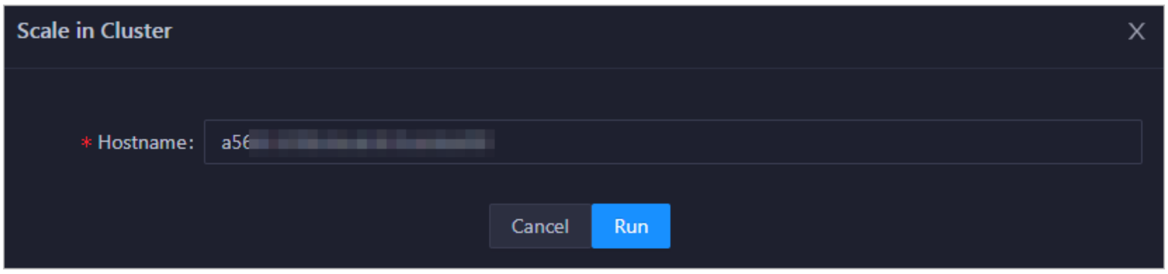
In Apsara Stack, scaling out a cluster involves complex operations. You must configure a new physical host on Deployment Planner so that it can be added to the default cluster of Apsara Infrastructure Management Framework. The default cluster of Apsara Infrastructure Management Framework can be considered as an available resource pool that provides resources for scaling out business clusters. ABM allows you to scale in or out a cluster for your business. To scale out a cluster, add physical hosts in the default cluster of Apsara Infrastructure Management Framework to the cluster. To scale in a cluster, remove physical hosts from the cluster to the default cluster of Apsara Infrastructure Management Framework.

You can remove multiple hosts from a Realtime Compute cluster at a time to scale in the cluster.

Procedure

(Optional)

1. On the O&M page of the ABM console, click the **Clusters** tab. On the page that appears, select a cluster in the left-side navigation pane. Click the **Hosts** tab and select one or more hosts whose role is **Worker**.
2. On the Clusters page, choose **Actions > Scale in Cluster**. The **Scale in Cluster** pane appears.


Scale in Cluster

* Hostname: a56[redacted]

Hostname: the name of the host to be removed from the cluster. The name of the selected host is used by default.

3. Click **Run**. A message appears, indicating that the action has been submitted.
4. View the scale-in status.

   Move the pointer over **Actions** in the upper-left corner, and then click **Execution History** next to **Scale in Cluster** to view the scale-in history.

   It may take some time for the cluster to be scaled in. In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution succeeds, and **FAILED** indicates that the execution fails.
5. (Optional)View the scale-in progress.

   If the status is **RUNNING**, click **Details** in the Details column to view the steps and progress of the scale-in operation.
6. Locate the cause of a scale-in failure.

   If the status is **FAILED**, click **Details** in the Details column to locate the failure cause.

   You can also view information about parameter settings, host details, script, and execution parameters to locate the failure cause.

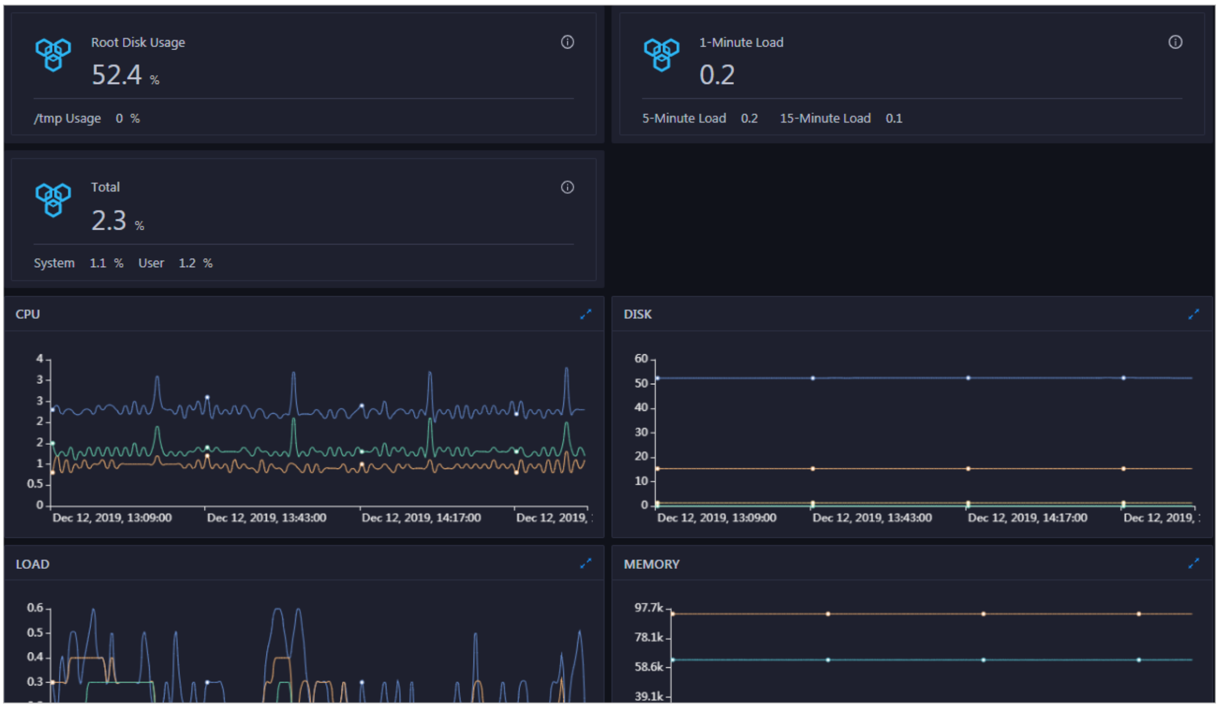
11.4.11.7. Host O&M

11.4.11.7.1. Host overview

The host overview page displays the overall running information about a host in a Realtime Compute cluster. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.

Entry

On the **Hosts** page, select a host in the left-side navigation pane. The **Overview** page for the host appears.



Root Disk Usage 52.4 %

/tmp Usage 0 %

1-Minute Load 0.2

5-Minute Load 0.2 15-Minute Load 0.1

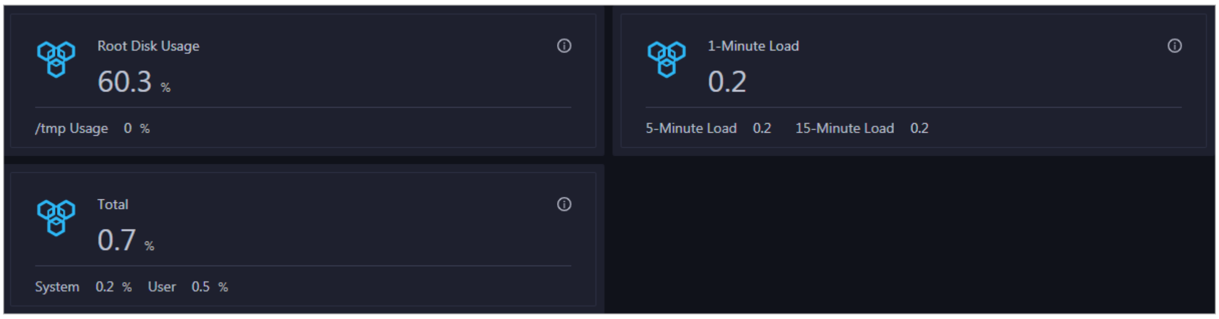
Total 2.3 %

System 1.1 % User 1.2 %

On the **Overview** page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.

Root Disk Usage, Total, and 1-Minute Load

These sections display the root disk usage, total usage, and 1-minute load for the selected host. The Root Disk Usage section provides the usage of the */tmp* directory. The Total section provides the system usage and user usage. The 1-Minute Load section provides the 1-minute, 5-minute, and 15-minute load averages.



Root Disk Usage 60.3 %

/tmp Usage 0 %

1-Minute Load 0.2

5-Minute Load 0.2 15-Minute Load 0.2

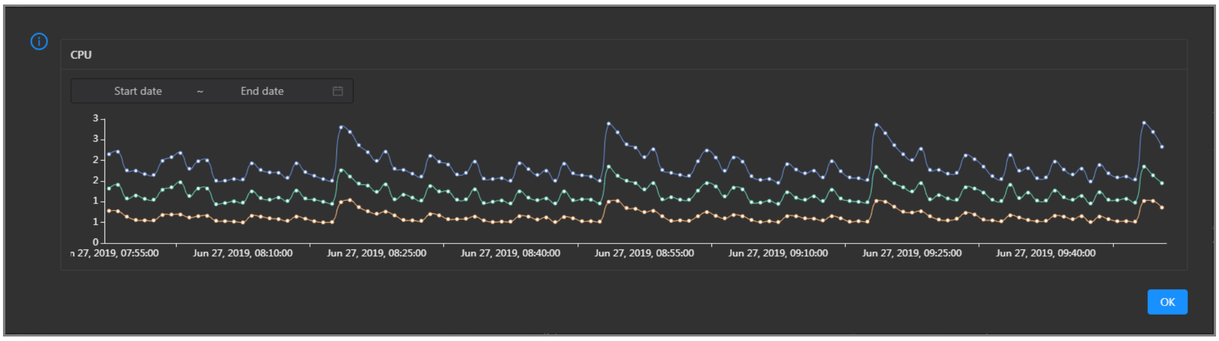
Total 0.7 %

System 0.2 % User 0.5 %

CPU

The CPU chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) of the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

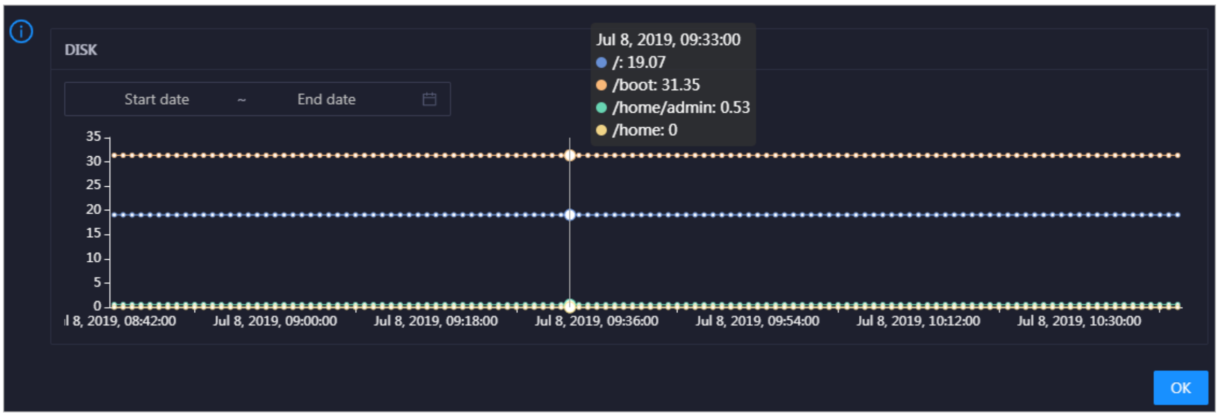


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the host in the specified period.

DISK

The DISK chart shows the trend lines of the storage usage in the */*, */boot*, */home/admin*, and */home* directories for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

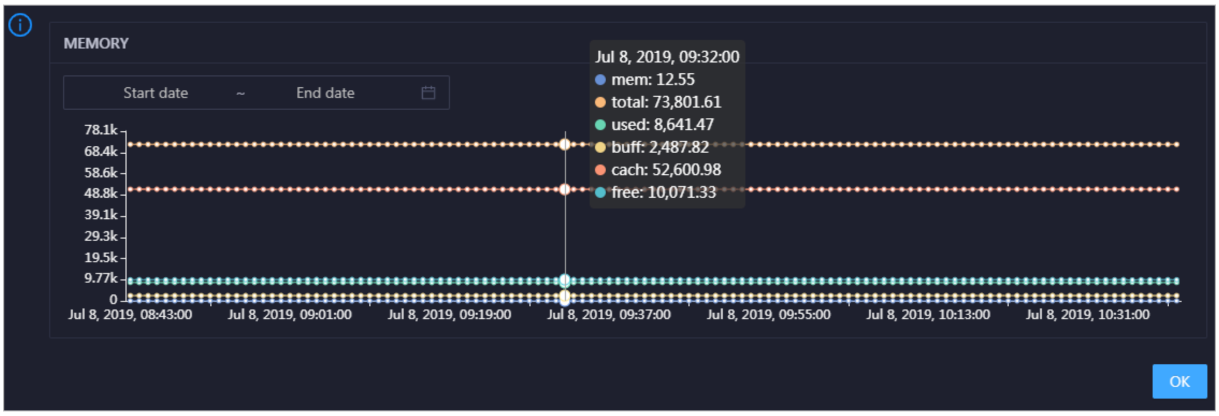


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the host in the specified period.

MEMORY

The MEMORY chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

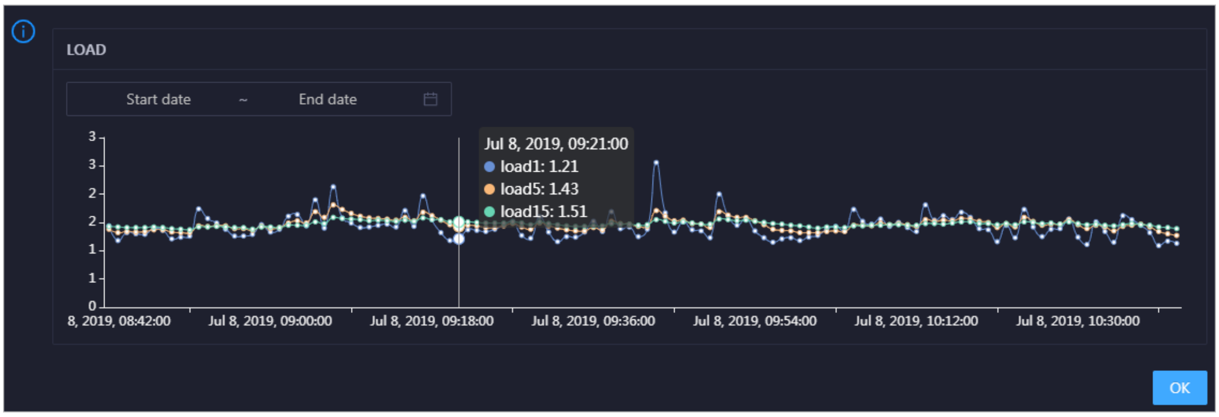


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the host in the specified period.

LOAD

The LOAD chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

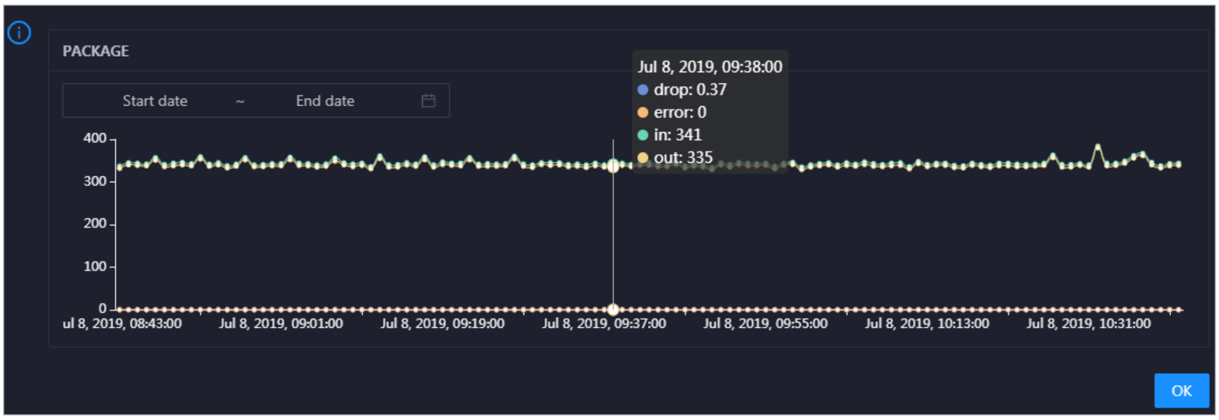


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the host in the specified period.

PACKAGE

The PACKAGE chart shows the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the host over time in different colors. These trend lines reflect the data transmission status of the host.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

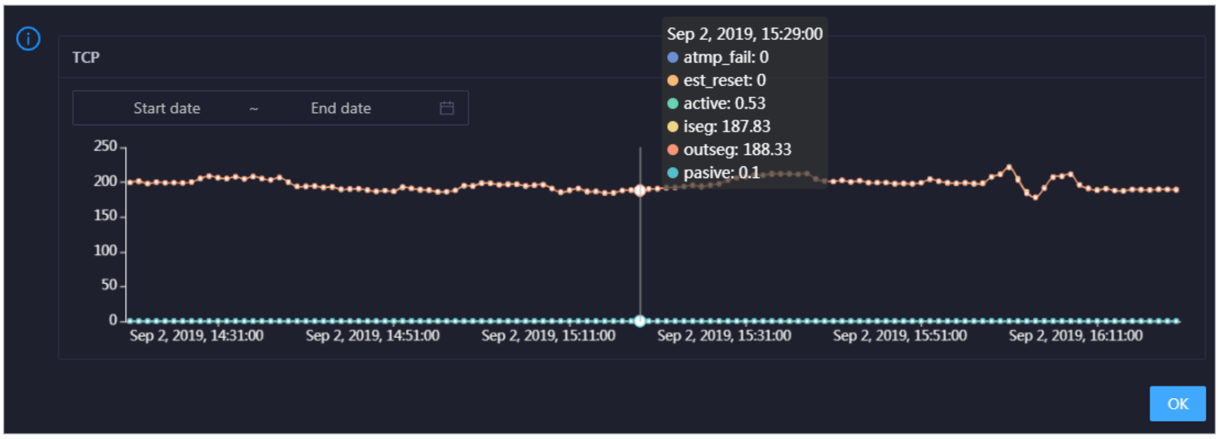


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the host in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the host over time in different colors. These trend lines reflect the TCP connection status of the host.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

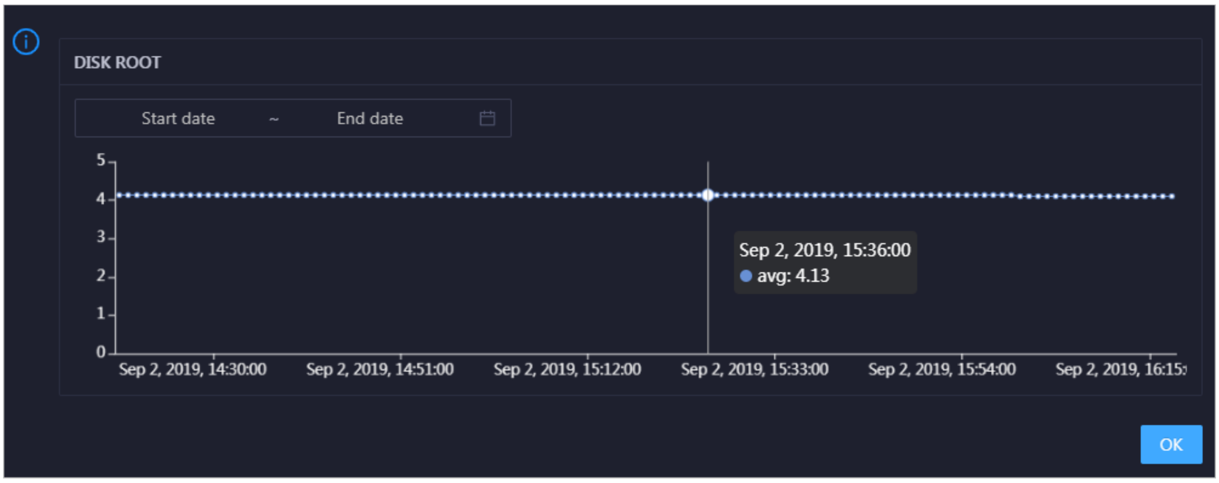


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the host in the specified period.

DISK ROOT

This chart displays the trend line of the average usage of the root disk (/) for the host over time.

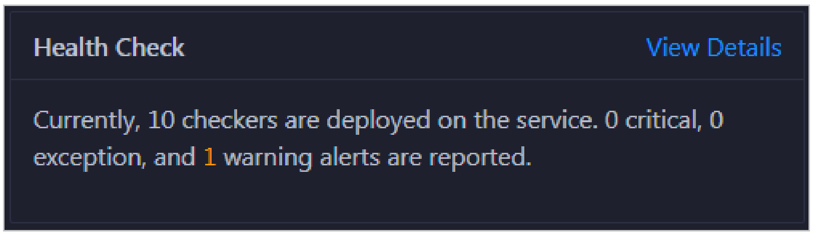
Click ⤢ in the upper-right corner of the chart to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the host in the specified period.

Health Check

This section displays the number of checkers deployed for the host and the respective number of Critical, Warning, and Exception alerts.



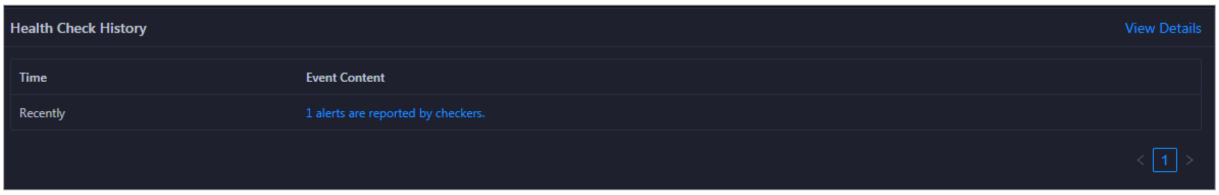
Health Check
View Details

Currently, 10 checkers are deployed on the service. 0 critical, 0 exception, and 1 warning alerts are reported.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Host health.

Health Check History

This section displays a record of the health checks performed on the host.

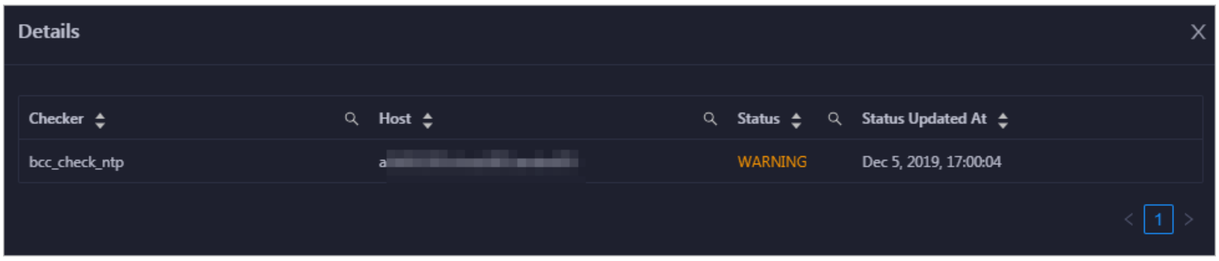


Health Check History
View Details

Time	Event Content
Recently	1 alerts are reported by checkers.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Host health.

You can click the event content of a check to view the exception items.



Details

Checker	Host	Status	Status Updated At
bcc_check_ntp	a[redacted]	WARNING	Dec 5, 2019, 17:00:04

11.4.11.7.2. Host health

On the Health Status page, you can view the checkers of the selected host, including the checker details, check results, and schemes to clear alerts (if any). In addition, you can log on to the host and perform manual checks on the host.

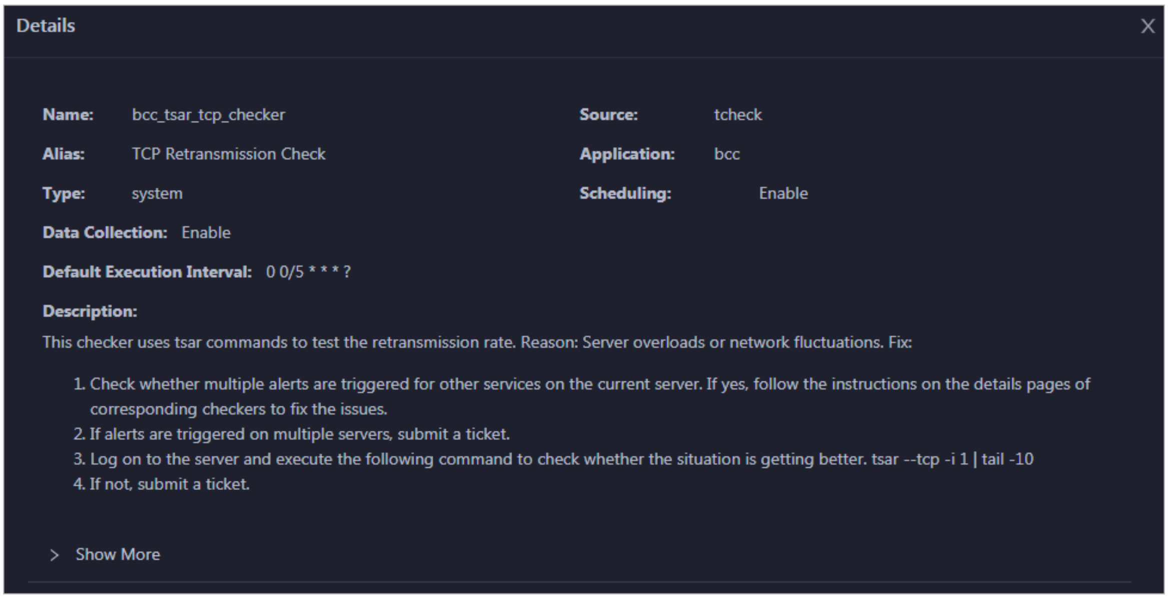
Entry

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Health Status** tab. The **Health Status** page for the host appears.

On the **Health Status** page, you can view all checkers and the check results for the host. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

View checker details

1. On the Health Status page, click **Details** in the Actions column of a checker. In the dialog box that appears, view the checker details.



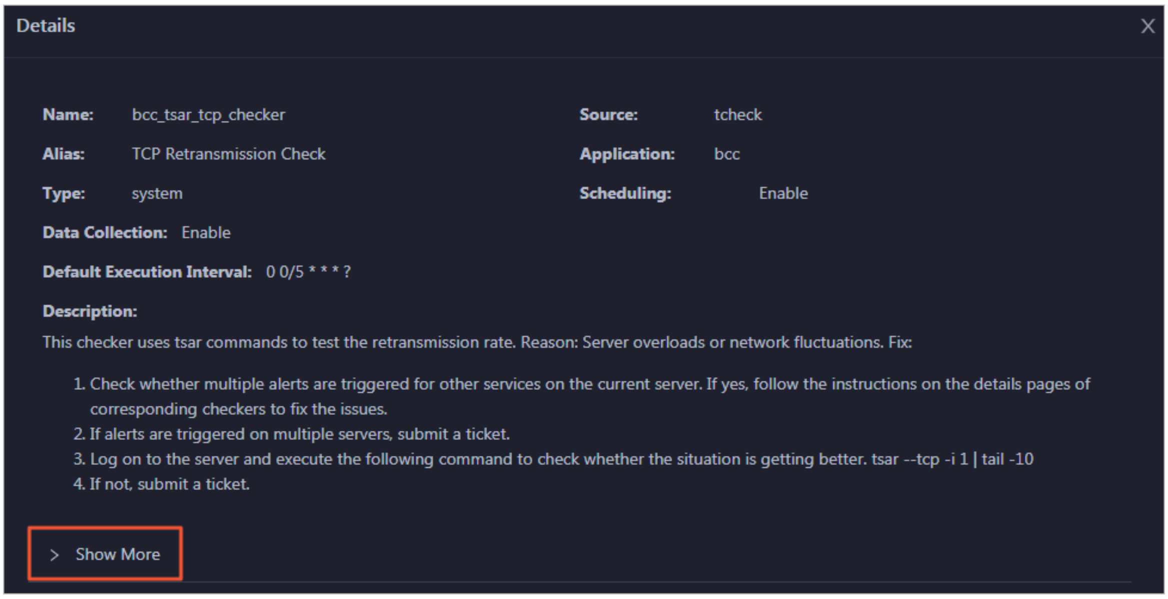
Details

Name: bcc_tsar_tcp_checker
Source: tcheck
Alias: TCP Retransmission Check
Application: bcc
Type: system
Scheduling: Enable
Data Collection: Enable
Default Execution Interval: 0 0/5 * * * ?
Description:
This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include the name, source, alias, application, type, default execution interval, and description of the checker, whether scheduling is enabled, and whether data collection is enabled. The schemes to clear alerts are provided in the description.

2. Click **Show More** at the bottom to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker
Source: tcheck
Alias: TCP Retransmission Check
Application: bcc
Type: system
Scheduling: Enable
Data Collection: Enable
Default Execution Interval: 0 0/5 * * * ?

Description:
This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

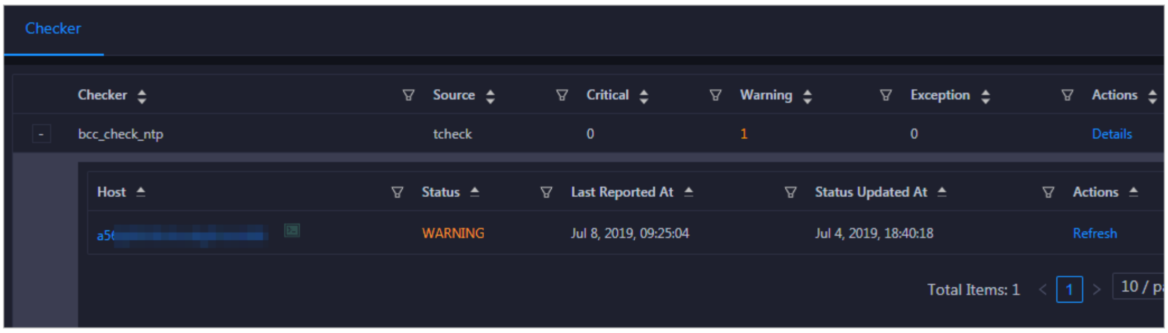
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about the execution script, execution target, default threshold, and mount point for data collection.

View alert causes

You can view the check history and check results of a checker.

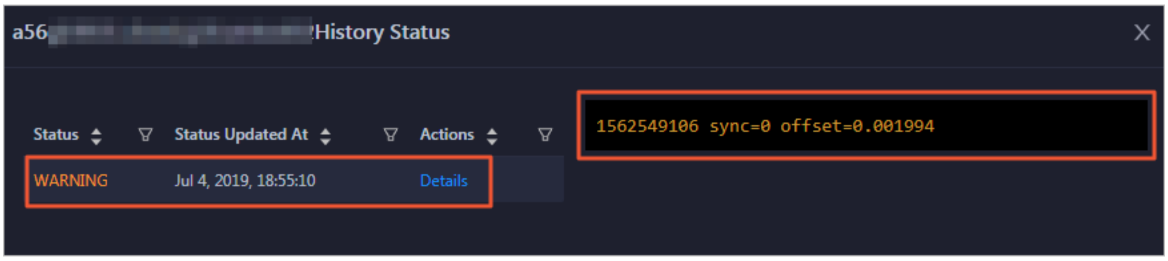
1. On the Health Status page, click **+** to expand a checker with alerts.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

2. Click the hostname. In the dialog box that appears, click **Details** in the Actions column of a check result to view the alert causes.



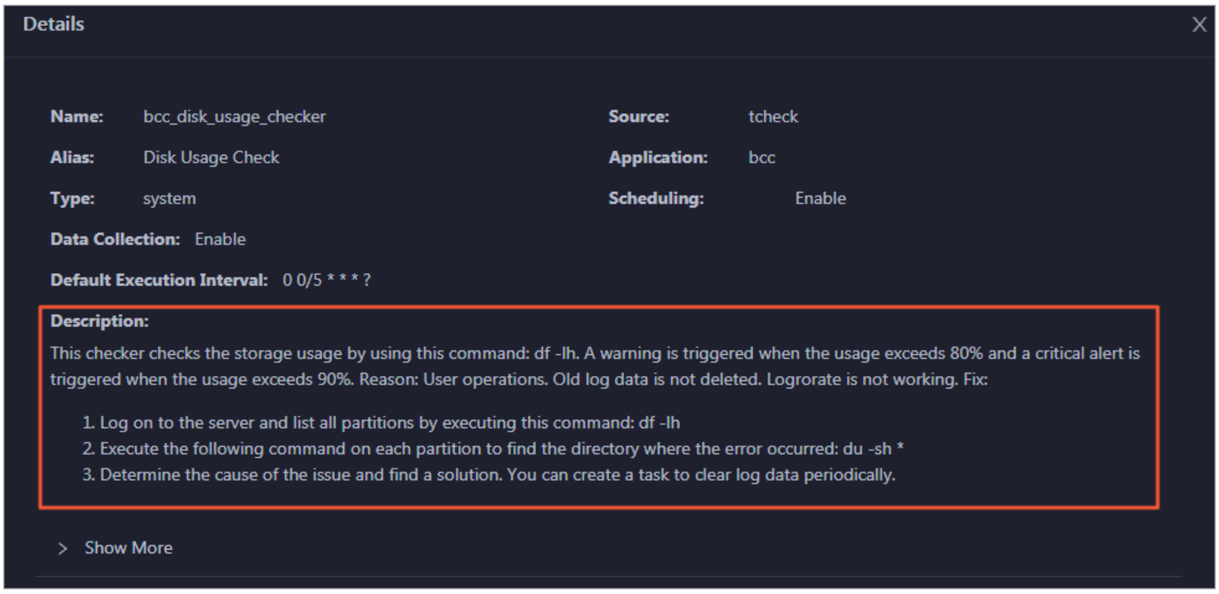
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status page, click **Details** in the Actions column of a checker with alerts. In the dialog box that appears, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker

Alias: Disk Usage Check

Type: system

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Source: tcheck

Application: bcc

Scheduling: Enable

Description:

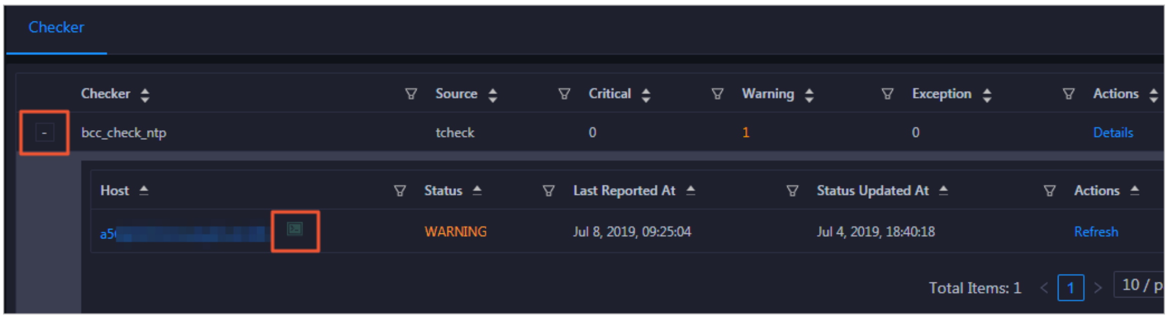
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

To log on to a host to clear alerts or perform other operations, follow these steps:

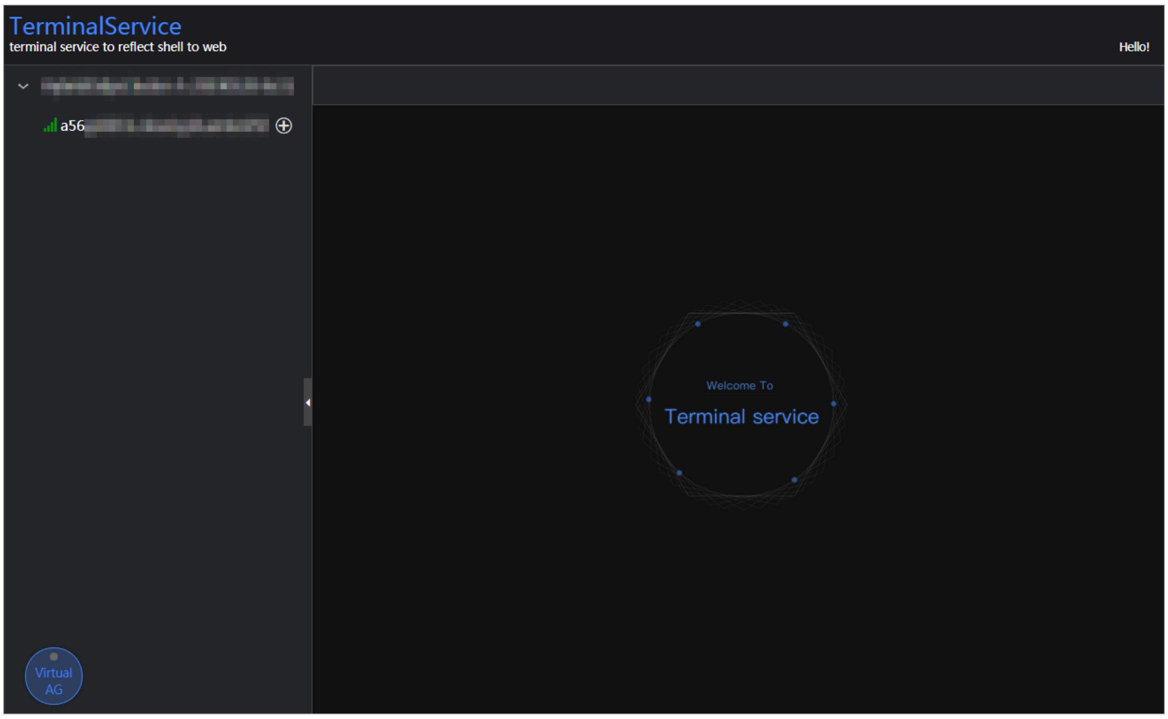
1. On the Health Status page, click **+** to expand a checker with alerts.



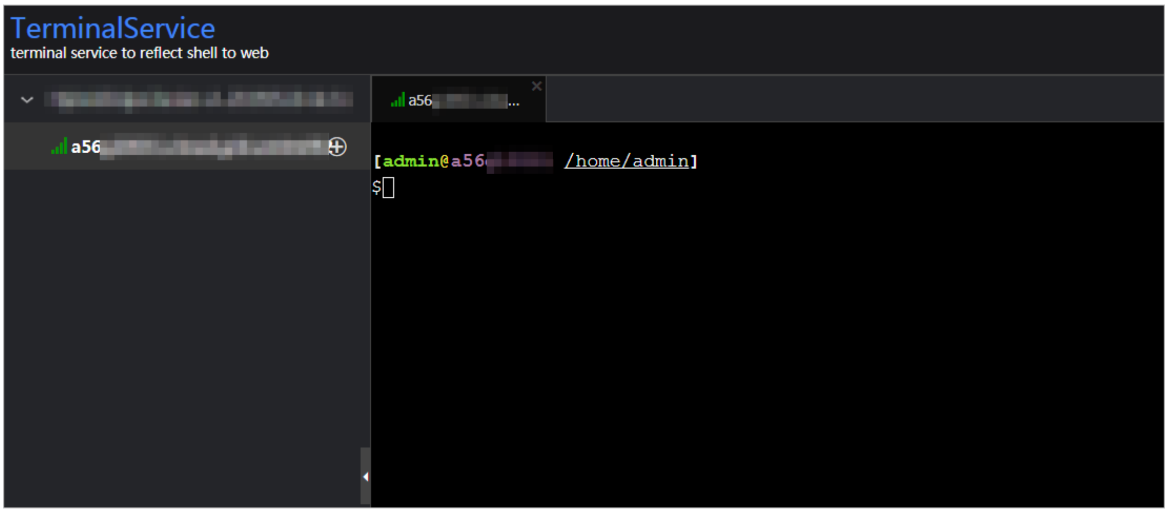
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

2. Click the **Log On** icon of a host. The **TerminalService** page appears.



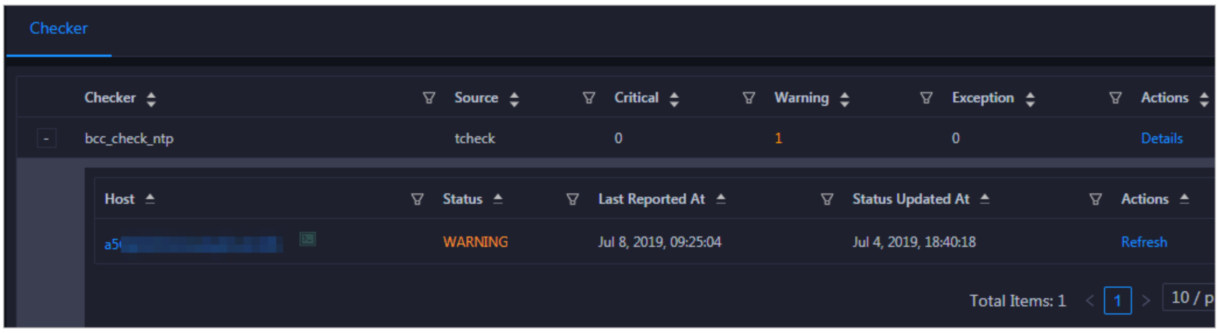
3. On the **TerminalService** page, click the hostname on the left to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. In this way, you can check whether the alert is cleared.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

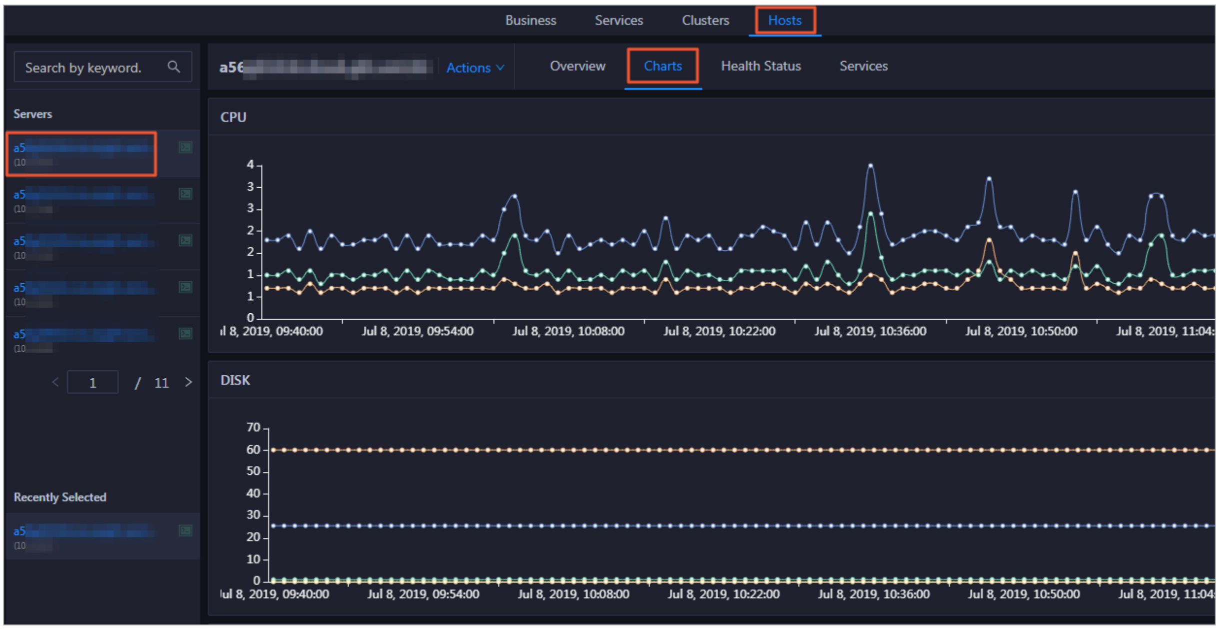
Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

11.4.11.7.3. Host charts

On the host chart page, you can view the enlarged trend charts of CPU usage, memory usage, storage usage, load, and packet transmission.

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Charts** tab. The **Charts** page for the host appears.

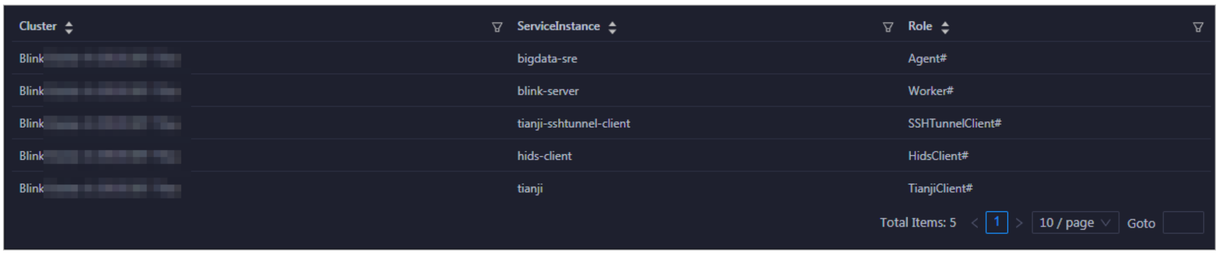


The **Charts** page displays trend charts of CPU usage, disk usage, memory usage, load, and packet transmission for the host. For more information, see Host overview.

11.4.11.7.4. Host services

On the host service page, you can view information about service instances and service instance roles of a host.

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Services** tab. The **Services** page for the host appears.



Cluster	ServiceInstance	Role
Blink[redacted]	bigdata-sre	Agent#
Blink[redacted]	blink-server	Worker#
Blink[redacted]	tianji-sshtunnel-client	SSHTunnelClient#
Blink[redacted]	hids-client	HidsClient#
Blink[redacted]	tianji	TianjiClient#

Total Items: 5 < 1 > 10 / page Goto

On the **Services** page, you can view the cluster, service instances, and service instance roles of the host.

11.4.11.8. Job and queue analysis

11.4.11.8.1. Job analysis

The job analysis feature allows you to diagnose jobs to quickly troubleshoot job failures.

Prerequisites

Jobs are in the running state.

Context

Job analysis has two steps, namely, **Failover** and **Blink Metric**. In the **Blink Metric** step, the system checks the latency, garbage collection (GC) time, transactions per second (TPS), the number of times of GC, data skew, and back pressure nodes of a job.

Procedure

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner, and then click **StreamCompute**.
3. On the page that appears, click **Analyze** in the upper-right corner. The **Job Analysis** page appears.

   You can also click Business on the O&M page, click **Jobs** in the left-side navigation pane, and then click a job name in the Name column to go to the **Job Analysis** page.
4. Select the job to be diagnosed and analyzed from the **Select Job** drop-down list.
5. In the **Diagnosis** section, click **Start Diagnosis**.

   After the diagnosis starts, the system automatically evaluates the time required for the diagnosis. Wait until the diagnosis is completed.
6. After the diagnosis is completed, click **View Log** to view the log details if the diagnosis result appears in red.

   The following table lists the metrics for job diagnosis.

Metric	Sub-metric	Description
Failover	N/A	Checks whether a failover is triggered for a job in a specified period and displays the information about the failover.
Blink Metric	**Job Latency**	Checks whether the latency of a subtask exceeds 10 minutes.
	Job GC	Checks whether the GC time of a Concurrent Low Pause Collector (CMS) exceeds 100 ms. This metric applies to all containers.
	Job TPS	Checks whether the TPS of a subtask is 0.
	Number of GC Times	Checks whether the number of the GC times exceeds 15 per minute. This metric applies to all containers.
	Data Skew	Checks whether the deviation of the input data size of each subtask in a task to the average input data size of all subtasks in the task exceeds 30%.

Metric	Sub-metric	Description
	Back Pressure Nodes	Checks whether each task has back pressure and finds the nodes that cause back pressure.

11.4.11.8.2. Queue analysis

The queue analysis page displays the basic information, resource information, and job list of a queue, so that you can quickly know the resource usage of the queue and locate job exceptions.

Procedure

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner, and then click **StreamCompute**.
3. On the page that appears, click **Analyze** in the upper-right corner. Then click **Queue Analysis** in the left-side navigation pane.

   You can also click Business on the O&M page, click **Queues** or **Jobs** in the left-side navigation pane, and then click a queue in the Queue column to go to the **Queue Analysis** page.

   The **Queue Analysis** page displays the following queue information:

   - Basic information: the status and name of the queue, the cluster and partition to which the queue belongs, and the number of jobs running in the queue.
   - Resource information: the minimum number of CPU cores and minimum memory capacity guaranteed as well as the maximum number of CPU cores and maximum memory capacity available for the queue.
   - Job list: information about all jobs in the queue, including the job names, users who created the jobs, projects to which the jobs belong, transactions per second (TPS) in the inbound direction, job latency, requested compute units (CUs), failover frequency, and start time.
4. On the **Queue Analysis** page, select a cluster and queue respectively from the **Select Cluster** and **Select Queue** drop-down lists at the top to view the details of the specified queue.

11.5. Apsara Big Data Manager (ABM)

11.6. Quick BI

11.6.1. Introduction to O&M and tools

11.6.1.1. O&M overview

Quick BI Operations and Maintenance Guide provides guidance for you to perform daily inspection, monitoring, and maintenance on Quick BI, and detect and rectify faults. These operations ensure the availability, stability, and security of Quick BI.

You can use the Apsara Infrastructure Management Framework console to resolve the unavailability issues of Quick BI.

Onsite engineers can use Apsara Big Data Manager (ABM) to manage big data products. In the ABM console, they can view metrics, modify configurations, and check and handle alerts of big data products.

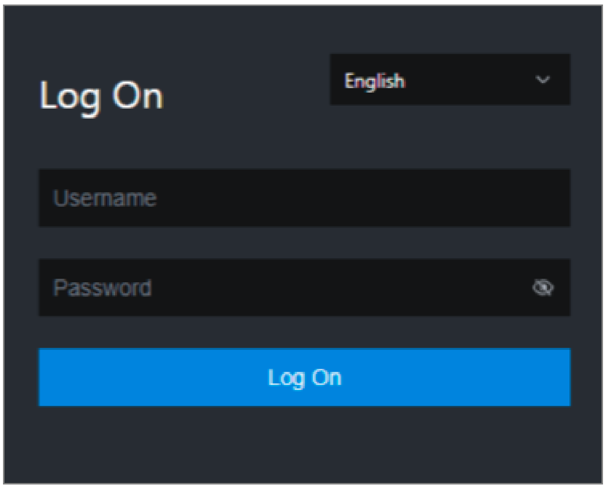
11.6.1.2. Check the Quick BI status in the Apsara Infrastructure Management Framework console

The Apsara Infrastructure Management Framework console is a tool that allows you to perform O&M on Quick BI. You can handle the unavailability issues of Quick BI in the console.

Procedure

1. Log on to the Apsara Infrastructure Management Framework console. Make sure that you have obtained the URL of the Apsara Uni-manager Operations Console, and the username and password used for logging on to the console from a deployment engineer or administrator.

   i. Open a browser, enter the URL in the address bar, and press Enter. The URL is in the format of *ops*.asconsole.*intranet-domain-id*.com.

   > Note We recommend that you use the Google Chrome browser.
   >
   > You can select a language from the drop-down list in the upper-right corner of the page.

   ii. Enter your username and password. If you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   For security concerns, your password must contain the following characters:

   - Letters
   - Digits
   - Special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%)
   - The password must be 10 to 20 characters in length.

   iii. Click **Log On**.

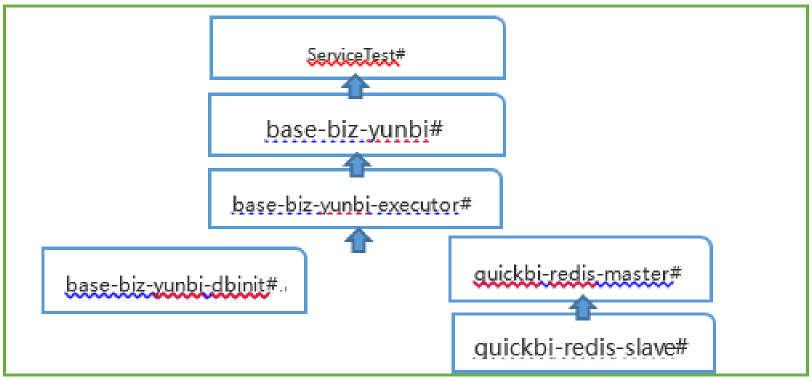
   iv. In the top navigation bar, click **O&M**.

   v. In the left-side navigation pane, choose **Product Management > Products**.

- vi. In the Apsara Stack O&M section, choose **Basic O&M > Apsara Infrastructure Management Framework**.
- vii. In the left-side navigation pane of Infra. Operation Platform, choose Operations > Cluster Operations.

2. On the homepage of the Apsara Infrastructure Management Framework console, enter the keywords of the name of the Quick BI cluster in the search box, select the cluster from the drop-down list, and click **Operations** next to the cluster.
3. On the **Cluster Operations** page, check the status of the Quick BI cluster. Check whether the cluster is at desired state:
   - If the cluster is at desired state, the system is running properly.
   - If the cluster is not at desired state, go to the next step.
4. On the Services tab, click the name of the service whose status is abnormal in the **Service** column or an exception number in the **Server Role** column to check the details of the service instance.
5. Click Details in the **Server Role Status** column to view the exception information.
6. (Optional)If a service instance is not at desired state, resolve the issue. Dependencies exist between server roles. If an upstream server role does not reach the desired state, its downstream server roles cannot reach the desired state. We recommend that you first troubleshoot the upstream server role. The following figure Dependencies between Quick BI server roles shows the dependencies between Quick BI server roles.

   Dependencies between Quick BI server roles



   For example, if server role **base-biz-yunbi-executor#** does not reach the desired state, **base-biz-yunbi#** and **ServiceTest#** cannot reach the desired state. In this case, you must make sure that server role **base-biz-yunbi-executor#** reaches the desired state. After **base-biz-yunbi-executor#** reaches the desired state, **base-biz-yunbi#** and **ServiceTest#** will reach the desired state sequentially in normal cases.

11.6.1.3. Perform O&M on Quick BI in the ABM console

Apsara Big Data Manager (ABM) allows you to perform O&M on big data products from the perspectives of business, service, cluster, and host. You can also update big data products, customize alert configurations, and view the O&M history in the ABM console.

ABM, formerly known as BCC, is an operations and management platform tailored for big data products.

For more information about how to log on to ABM and perform O&M operations on Quick BI, see *Quick BI O&M*.

11.6.2. Routine maintenance

11.6.2.1. Introduction to Quick BI components

You can use container monitoring and inspection management to check whether server roles related to Quick BI components are at desired state, so as to perform routine maintenance. This topic describes Quick BI operations and maintenance (O&M) components, including their server roles and functions.

The following table lists Quick BI O&M components, related server roles, and component functions.

Component	Server role	Function
Database initialization component	base-biz-yunbi-dbinit#	Initializes Quick BI metadata. The server role must be at desired state. Otherwise, Quick BI cannot run properly.
Cache component	quickbi-redis-master#	Caches Quick BI data to improve query performance.
	quickbi-redis-slave#	
Runtime component	base-biz-yunbi-executor#	Retrieves table metadata and data from data sources.
Web service component	base-biz-yunbi #	Provides web services. The server role allows frontend clients to visit Quick BI web pages.
Automated testing component	ServiceTest#	Checks the overall availability of Quick BI by running multiple test cases at a time.

> ? **Note** When you deploy or update Quick BI, the server roles are automatically started.

11.6.2.2. Database initialization components

This topic describes how to troubleshoot issues when you perform container monitoring on database initialization components.

In the Apsara Infrastructure Management Framework, you need to check whether the **base-biz-yunbi-dbinit#** service role is at the desired state.

> ? **Note** The service role that is related to database initialization components must be at the desired state before Quick BI is running as expected. If the check result indicates that the service role is not at the desired state, we recommend that you contact Quick BI Technical Support.

11.6.2.3. Cache components

This topic describes how to detect and troubleshoot issues when you perform container monitoring on cache components.

Container monitoring

In the Apsara Infrastructure Management Framework, you need to check whether the **quickbi-redis-master#** and **quickbi-redis-slave#** service roles are at the desired state.

> **Note** You can also check the redis process. If the redis process exists, it means that the preceding service roles are at the desired state.

Quick BI is unavailable if the check result indicates that the linked service roles are not at the desired state. Cause: The redis process is interrupted or not started.

Solution: You need to restart the linked service roles. You need to restart the **quickbi-redis-master#** service role and then restart the **quickbi-redis-slave#** service role.

Periodical detection

You can check the service availability based on the exit status that is returned after you run the **/checkRedis.sh** script. Quick BI is available if the value of the exit status is 0. Otherwise, Quick BI is unavailable. You can use the preceding script to check whether the redis process exists. The redis process exists if the value of the returned exit status is 0. Otherwise, the redis process does not exist. The detection interval is one second.

11.6.2.4. Runtime components

This topic describes how to detect and troubleshoot issues when you perform container monitoring on runtime components.

Container monitoring

In the Apsara Infrastructure Management Framework, you need to check whether the **base-biz-yunbi-executor#** service role is at the desired state.

Quick BI is unavailable if the check result indicates that the linked service role is not at the desired state. Cause: The runtime component process is interrupted or not started.

Solution: You need to restart the **base-biz-yunbi-executor#** service role.

Periodical detection

You can visit http://container:7001/checkpreload.htm at regular intervals to call the HTTP service. Quick BI is available if a status code of 200 is returned. Otherwise, Quick BI is unavailable. The detection interval is one second.

> **Note** The container in the preceding HTTP link is a variable. You must replace the variable with an IP address that is used by the **base-biz-yunbi#** service role.

11.6.2.5. Web service components

This topic describes how to detect and troubleshoot issues when you perform container monitoring for Web service components.

Container monitoring

Check whether the **base-biz-yunbi#** service role is at the desired state.

Quick BI is unavailable if the check result indicates that the linked service role is not at the desired state. Cause:

- The Java process is interrupted or not started. Symptom: You cannot visit http://container:7001/checkpreload.htm.
- No HTTPS certificate is issued and port 443 is inaccessible. Symptom: You cannot visit https://container/checkpreload.htm.

> **Note** The container in the preceding link is a variable. You must replace the variable with an IP address that is used by the **base-biz-yunbi#** service role.

Solutions:

- If the Java process is interrupted or not started, you need to restart the **base-biz-yunbi#** service role.
- If no HTTPS certificate is issued, you need to restart the **base-biz-yunbi#** service after the HTTPS certificate is issued.

Periodical detection

You can visit https://container/checkpreload.htm at regular intervals to call an HTTPS service. Quick BI is available if a value of 200 is returned. Otherwise, Quick BI is unavailable. The detection interval is five minutes.

> **Note** The container in the preceding HTTPS link is a variable. You must replace the variable with an IP address that is requested by the **base-biz-yunbi#** service role.

11.6.2.6. Automated testing components

This topic describes how to identify and troubleshoot issues when you perform container monitoring and inspection management on automated testing components.

Container monitoring

In the Apsara Infrastructure Management Framework console, check whether server role **ServiceTest#** is at desired state.

If the server role is not at desired state, a service error occurs. Causes:

- The service is unavailable. Symptom: You cannot visit https://container/checkpreload.htm or log on to the Quick BI console.

  > **Note** "container" in the link is a variable. You must replace it with the IP address that is used by server role **base-biz-yunbi#** .

- The service is available but an error occurs. Symptom: You can log on to the Quick BI console and search data. However, a logon error is reported in the Apsara Infrastructure Management Framework console. You can view the error message displayed in the Description column. For more information, see*the instance status monitoring description*in Quick BI Operations and Maintenance Guide.

Solutions:

- If the service is unavailable, check whether other server roles are at desired state. If they are not, resolve the issue.

- If the service is available but an error occurs, contact Quick BI technical support and provide error information.

Inspection management

You can execute test cases at regular intervals to check the availability of Quick BI. A service is available if the linked server role is at desired state. Otherwise, the service is unavailable. The detection interval is 30 minutes.

11.6.3. Quick BI O&M

11.6.3.1. Log on to the ABM console

This topic describes how to log on to the Apsara Big Data Manager (ABM) console.

Prerequisites

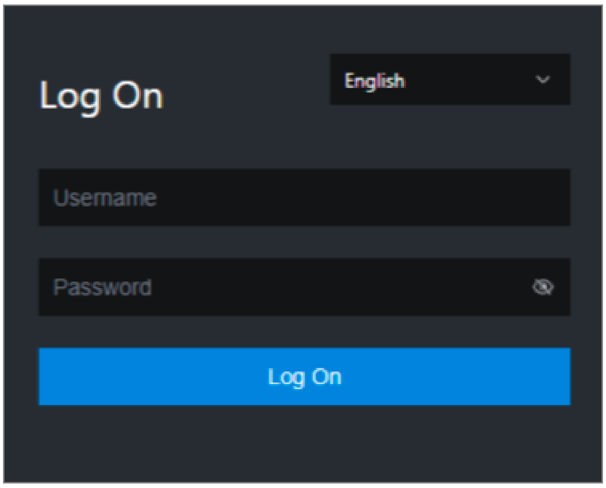
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.

   Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

> Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

For security reasons, your password must meet the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password must be 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Product Management** > **Products**.
7. In the **Big Data Services** section, choose **General-Purpose O&M** > **Apsara Big Data Manager**.

11.6.3.2. Quick BI O&M

This topic describes the features of Quick BI O&M supported by Apsara Big Data Manager (ABM) and how to access the Quick BI O&M page.

Quick BI O&M

Quick BI O&M includes service O&M, cluster O&M, and host O&M. The following table describes them in detail.

Module	Submodule or feature	Description
Services	Overview	Displays the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for each service in a cluster.
	Server	Displays the host list of each service in a cluster so that you can understand the service deployment on hosts.
Clusters	Overview	Displays the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for a cluster.
	Health Status	Displays all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts. In addition, you can log on to a host and perform manual checks on the host.

Module	Submodule or feature	Description
Hosts	Overview	Displays the overall running and health check information about a host. On this tab, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.
	Health Status	Displays the checkers of the selected host, including the checker details, check results, check history, and schemes to clear alerts. In addition, you can log on to the host and perform manual checks on the host.

Quick BI O&M

1. Log on to the ABM console.
2. Click ▦ in the upper-left corner, and then click **QuickBI**.
3. On the page that appears, click **O&M** in the upper-right corner. The **Clusters** page appears.

   The **O&M** page includes three modules: **Services**, **Clusters**, and **Hosts**.

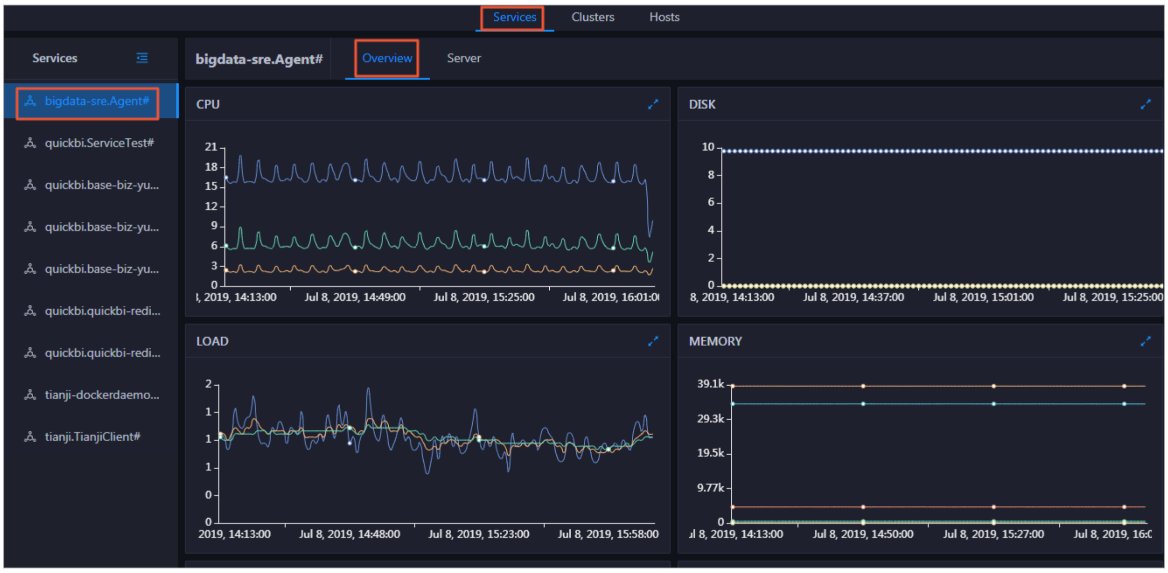
11.6.3.3. Service O&M

11.6.3.3.1. Service overview

The service overview page lists all Quick BI services in a cluster. You can view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for each service.

Entry

1. At the top of the **O&M** page, click **Services**.
2. On the **Services** page, search for a cluster in the search box above the left-side service list, and then select a service in the service list.
3. Click the **Overview** tab. The **Overview** page for the service appears.



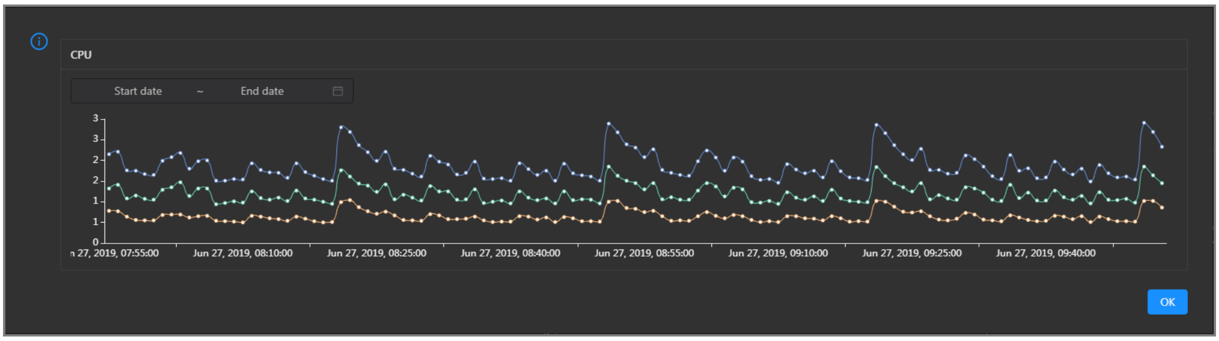
On the **Overview** page, you can view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the selected service.

CPU

This chart displays the trend lines of the total CPU usage (cpu), CPU usage for executing code in kernel space (sys), and CPU usage for executing code in user space (user) for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

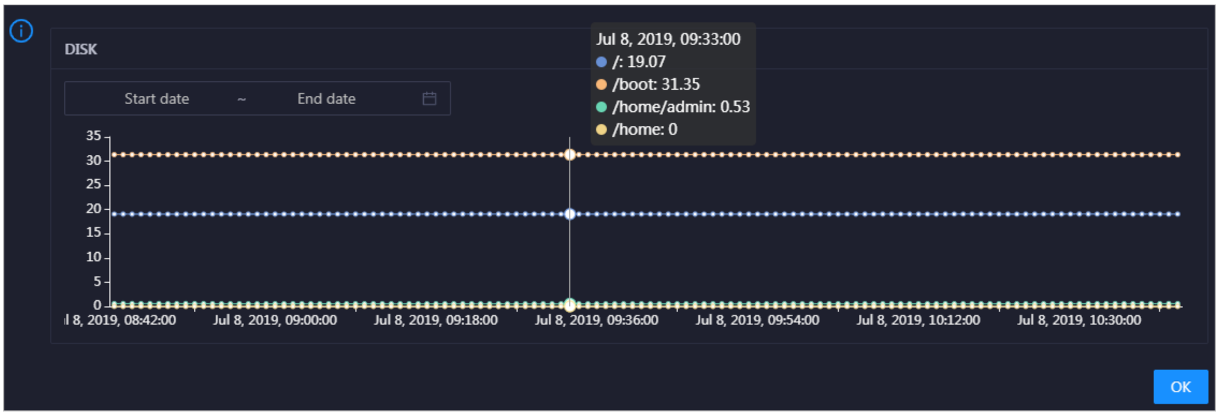
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU usage of the service in the specified period.



DISK

This chart displays the trend lines of the storage space usage on the */*, */boot*, */home/admin*, and */home* directories for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

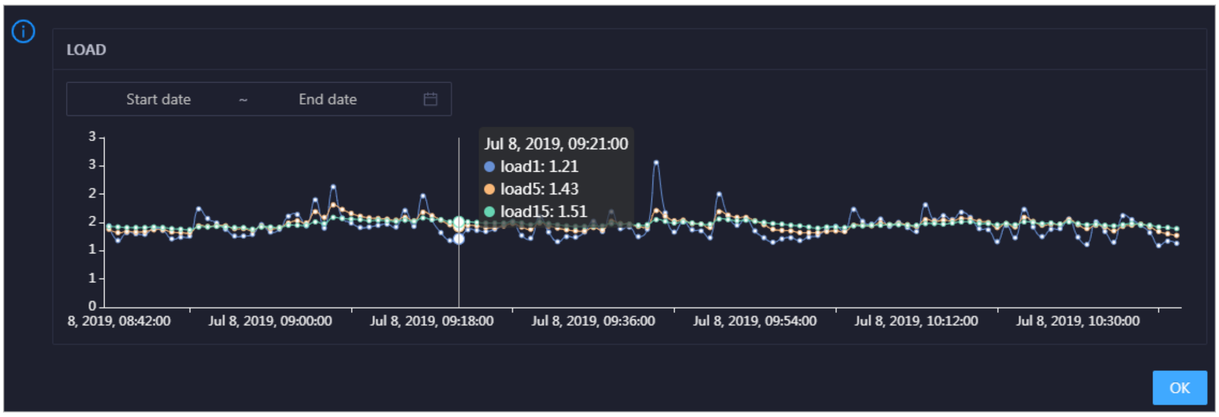


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage space usage of the service in the specified period.

LOAD

This chart displays the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

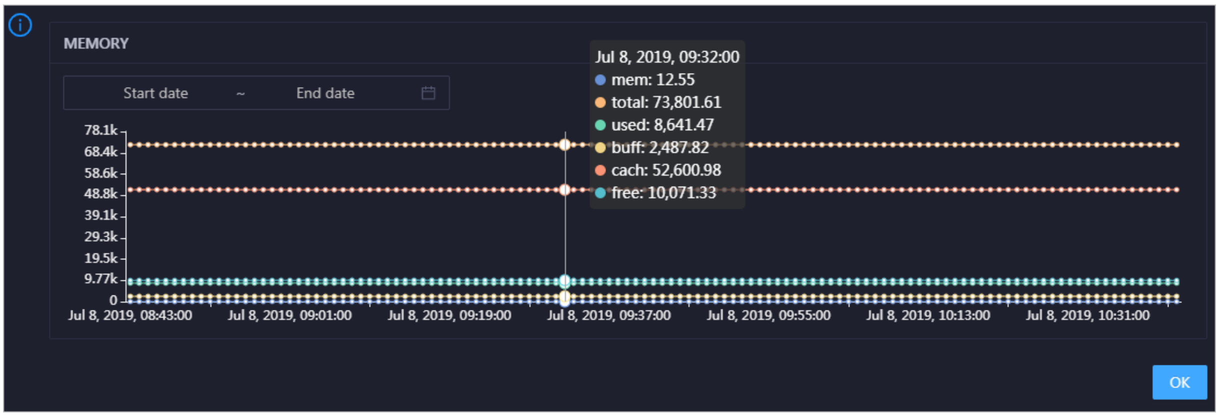


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the selected service in the specified period.

MEMORY

This chart displays the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

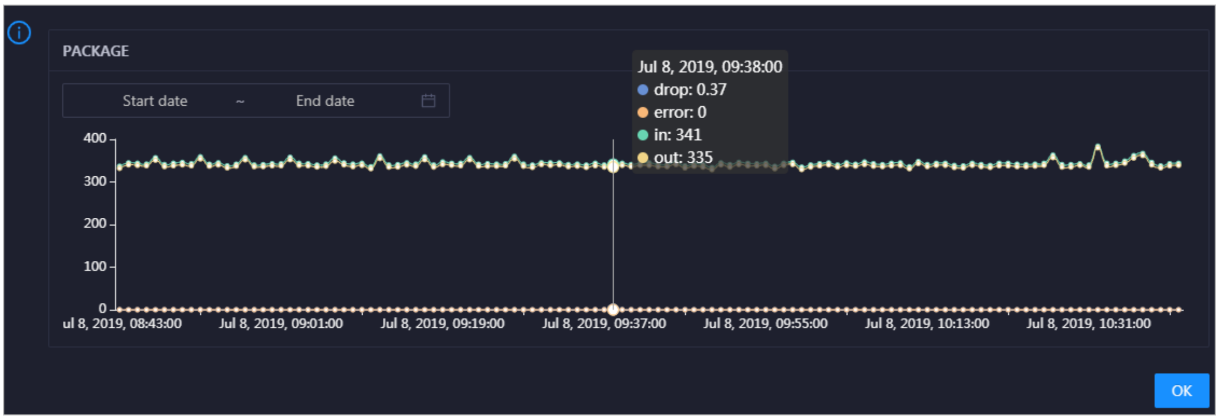


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the selected service in the specified period.

PACKAGE

This chart displays the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the selected service over time in different colors. These trend lines reflect the data transmission status of the service.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

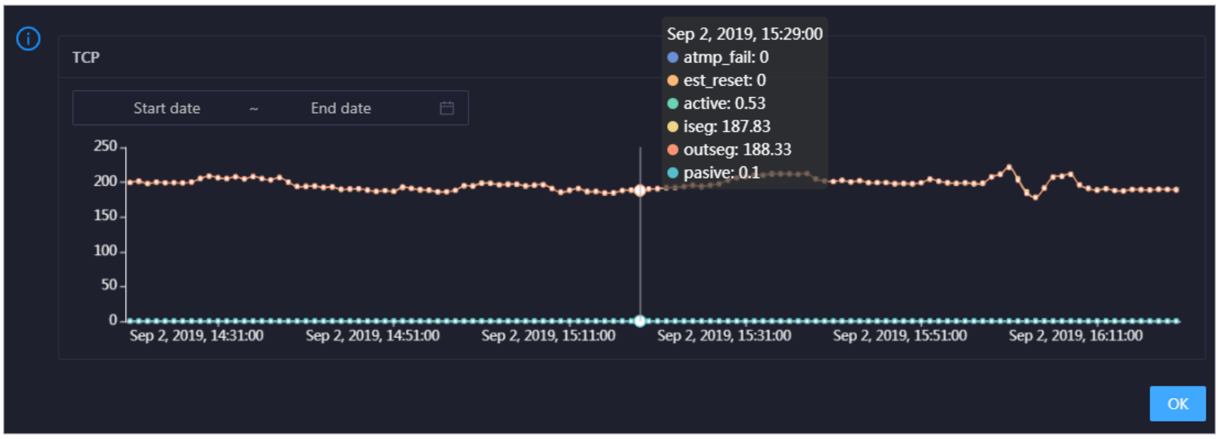


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the selected service in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the selected service over time in different colors. These trend lines reflect the TCP connection status of the service.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

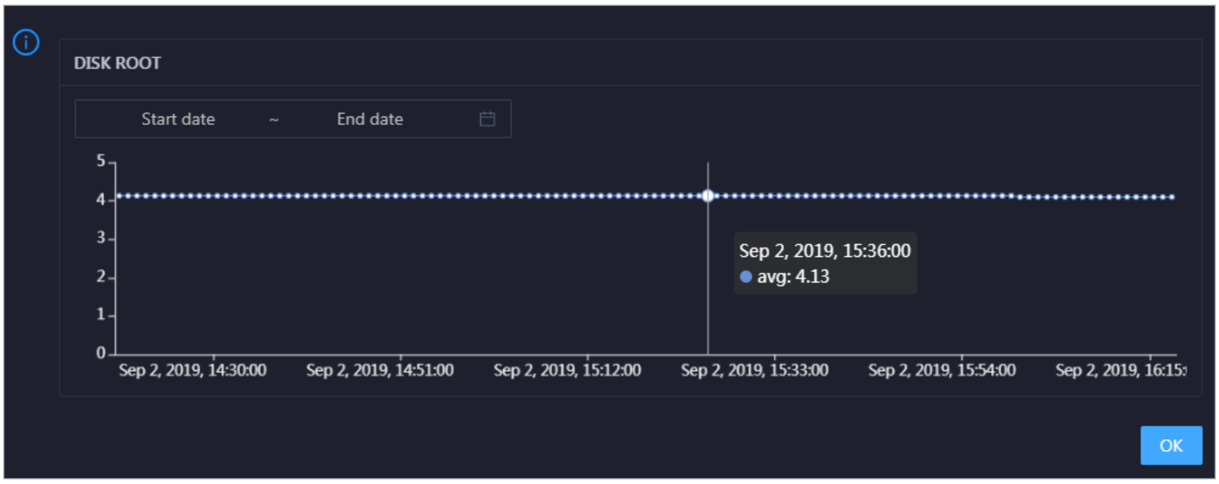


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the selected service in the specified period.

DISK ROOT

This chart displays the trend line of the average root disk usage (avg) for the selected service over time.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

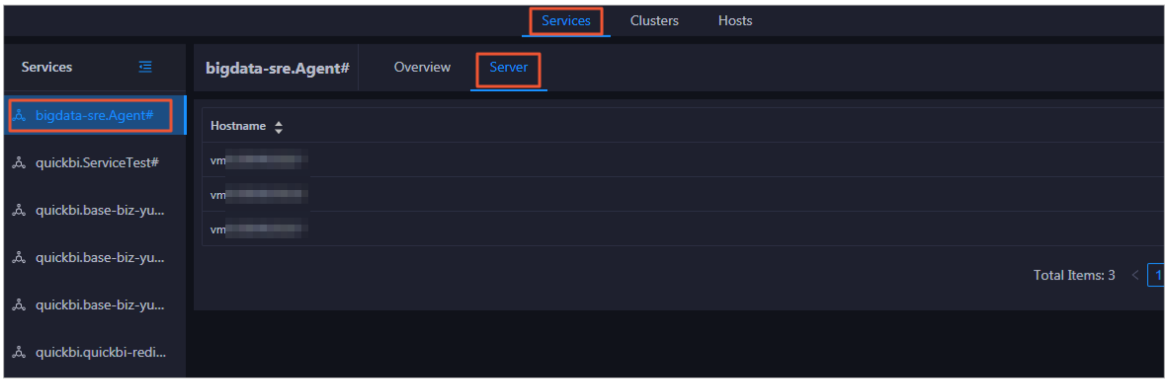


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the selected service in the specified period.

11.6.3.3.2. Quick BI service hosts

Apsara Big Data Manager (ABM) allows you to view the host list of each Quick BI service so that you can understand the service deployment on hosts.

1. At the top of the **O&M** page, click **Services**.
2. On the **Services** page, click your service in the left-side service list.
3. Click the **Server** tab.



Hostname
vm[redacted]
vm[redacted]
vm[redacted]

On the **Server** tab, you can view the hosts on which the selected service is running.

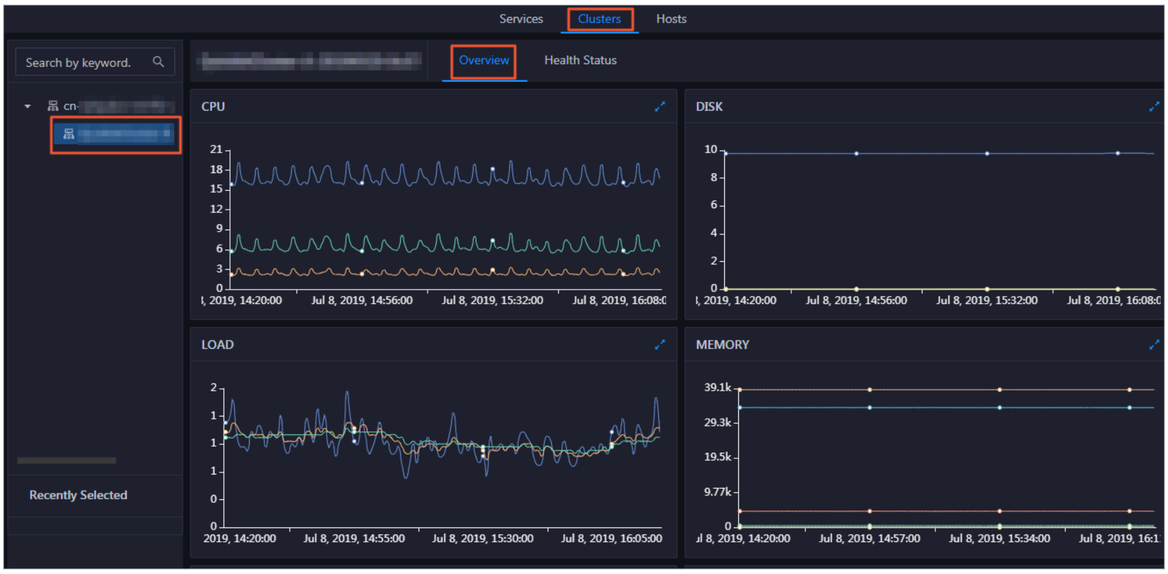
11.6.3.4. Cluster O&M

11.6.3.4.1. Cluster overview

The cluster overview page displays the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for a cluster.

Entry

1. At the top of the **O&M** page, click **Clusters**.
2. On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Overview** tab. The **Overview** page for the cluster appears.

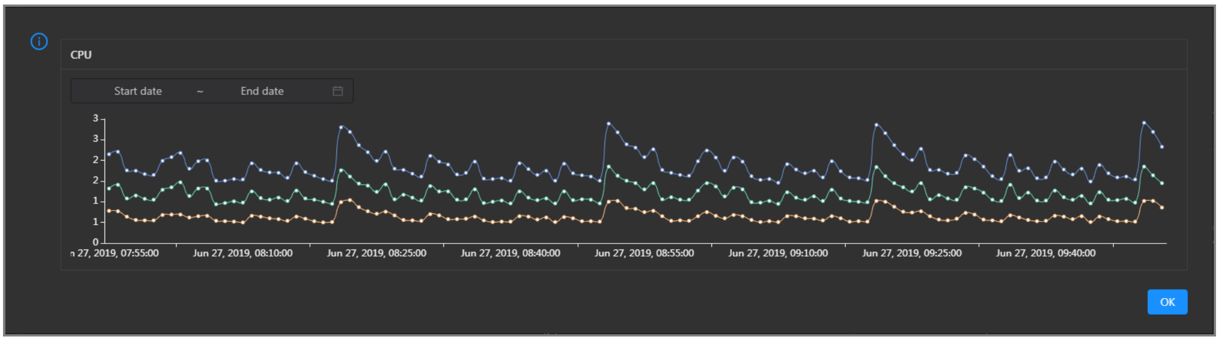


CPU

This chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

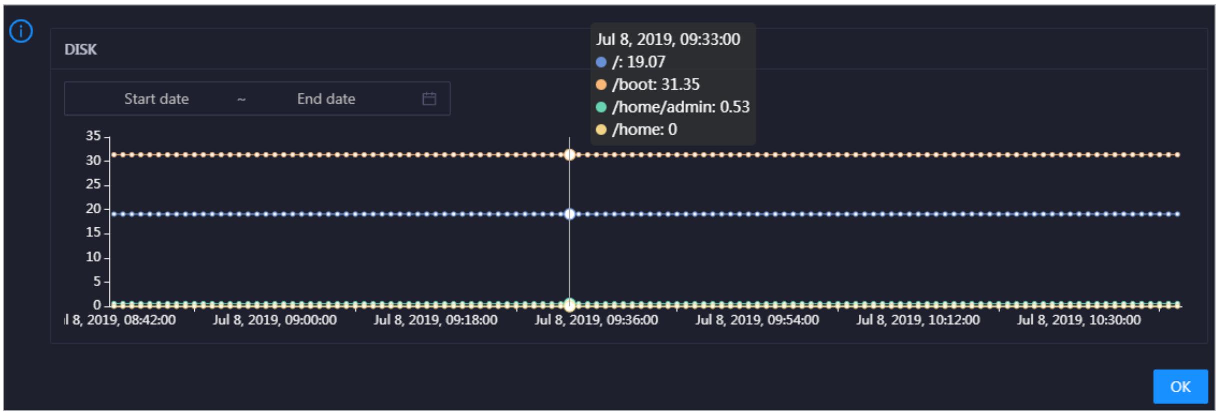
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the cluster in the specified period.



DISK

This chart shows the trend lines of the storage usage on the */*, */boot*, */home/admin*, and */home* directories for the cluster over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

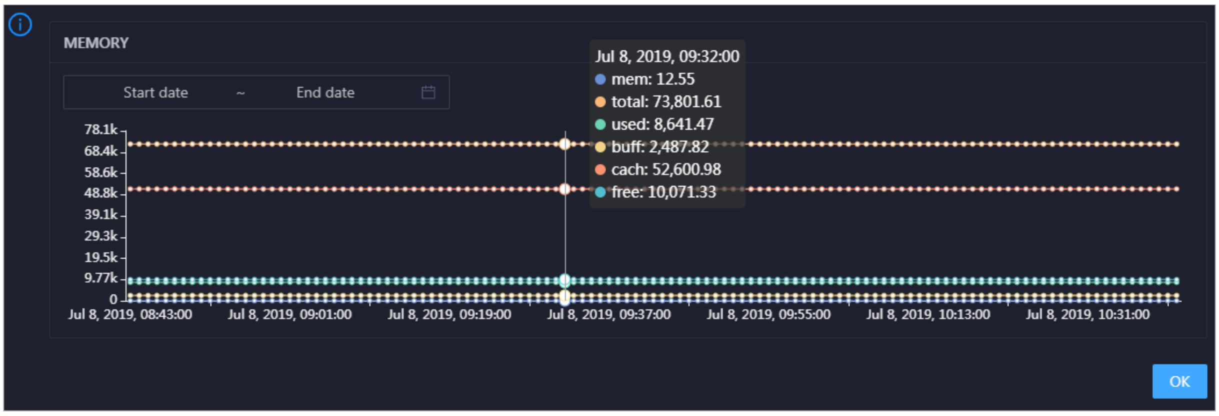


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

MEMORY

This chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

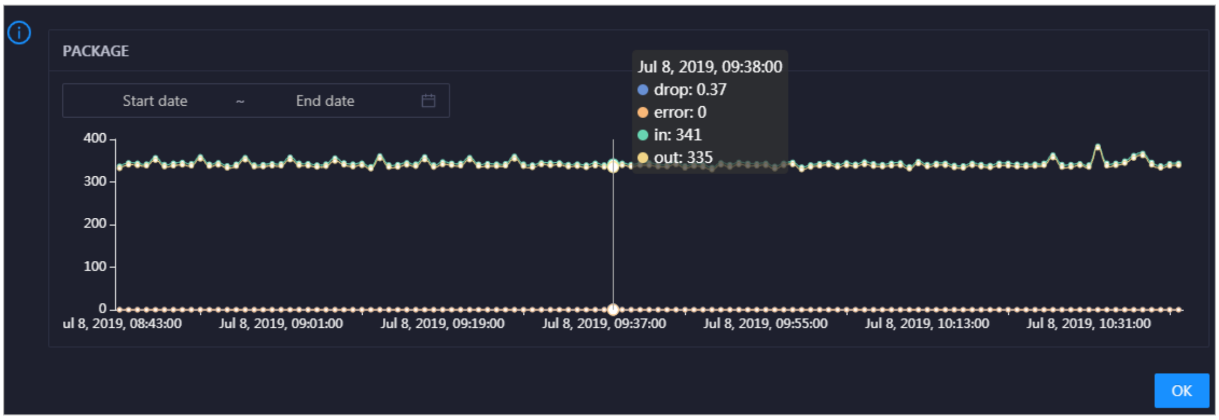


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the cluster in the specified period.

PACKAGE

This chart shows the trend lines of the numbers of dropped packets (drop), error packets (error), received packets (in), and sent packets (out) for the cluster in different colors. These trend lines reflect the data transmission status of the cluster.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

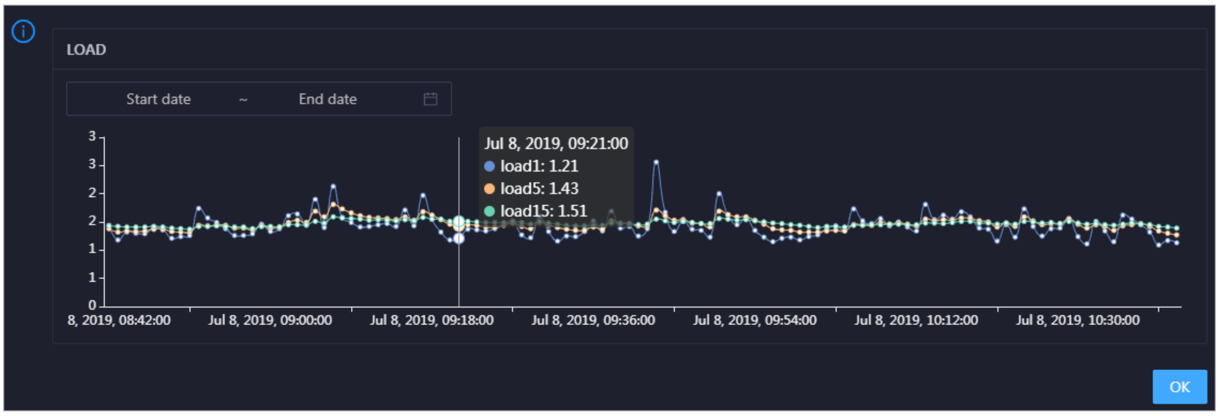


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the cluster in the specified period.

LOAD

This chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



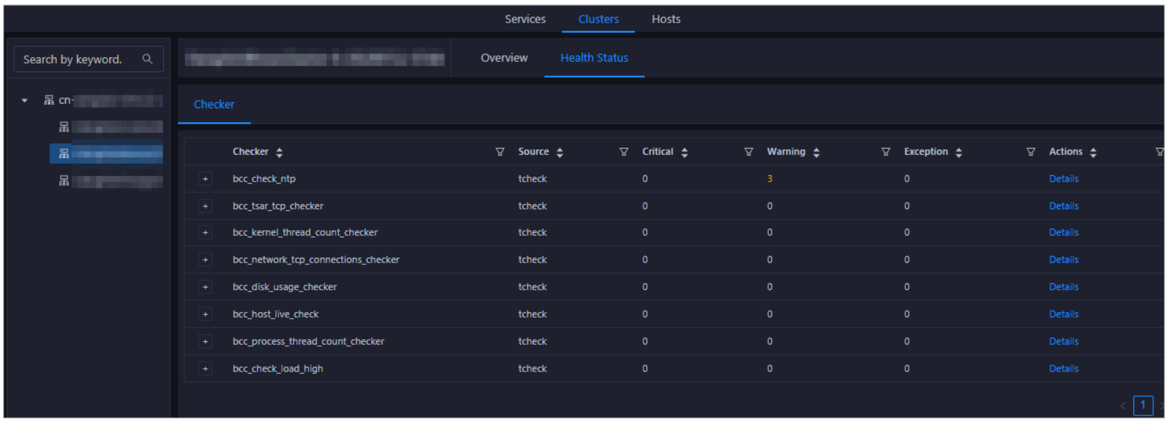
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the cluster in the specified period.

11.6.3.4.2. Cluster health

On the Health Status page, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Entry

1. At the top of the **O&M** page, click **Clusters**.
2. On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Health Status** tab. The **Health Status** page for the cluster appears.

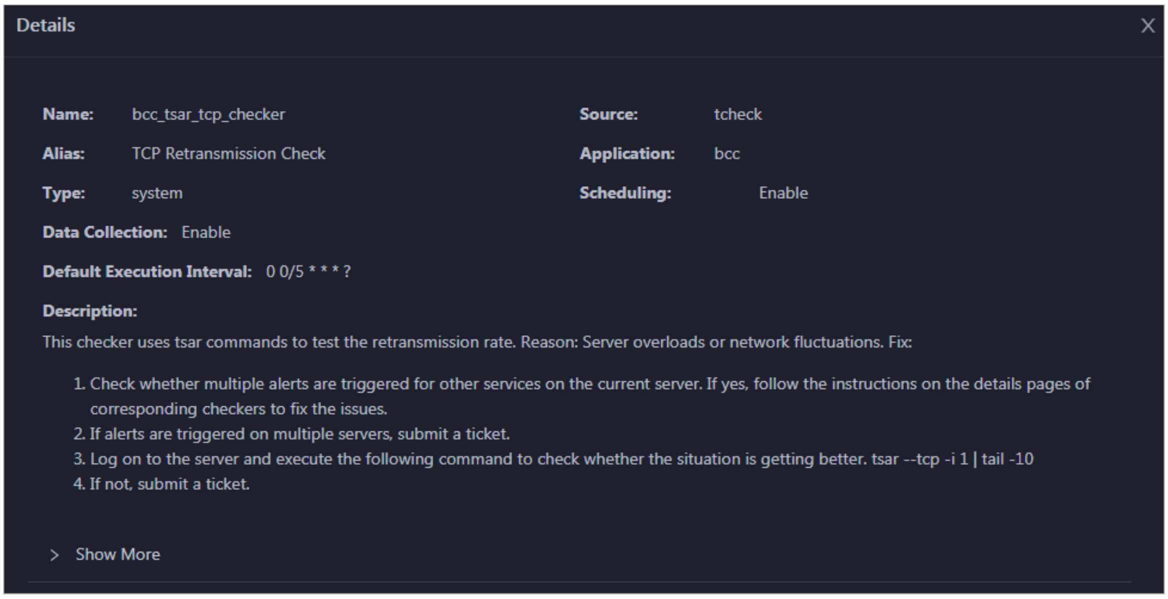


	Checker	Source	Critical	Warning	Exception	Actions
+	bcc_check_ntp	tcheck	0	3	0	Details
+	bcc_tsar_tcp_checker	tcheck	0	0	0	Details
+	bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
+	bcc_network_tcp_connections_checker	tcheck	0	0	0	Details
+	bcc_disk_usage_checker	tcheck	0	0	0	Details
+	bcc_host_live_check	tcheck	0	0	0	Details
+	bcc_process_thread_count_checker	tcheck	0	0	0	Details
+	bcc_check_load_high	tcheck	0	0	0	Details

On the **Health Status** tab, you can view all checkers for the cluster and the check results for the hosts in the cluster. The following alerts may be reported on a host: **CRITICAL**, **WARNING**, and **EXCEPTION**. The alerts are represented in different colors. You must handle the alerts in a timely manner, especially the **CRITICAL** and **WARNING** alerts.

View checker details

1. On the Health Status tab, click **Details** in the Actions column of a checker. On the Details page, view checker details.



Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

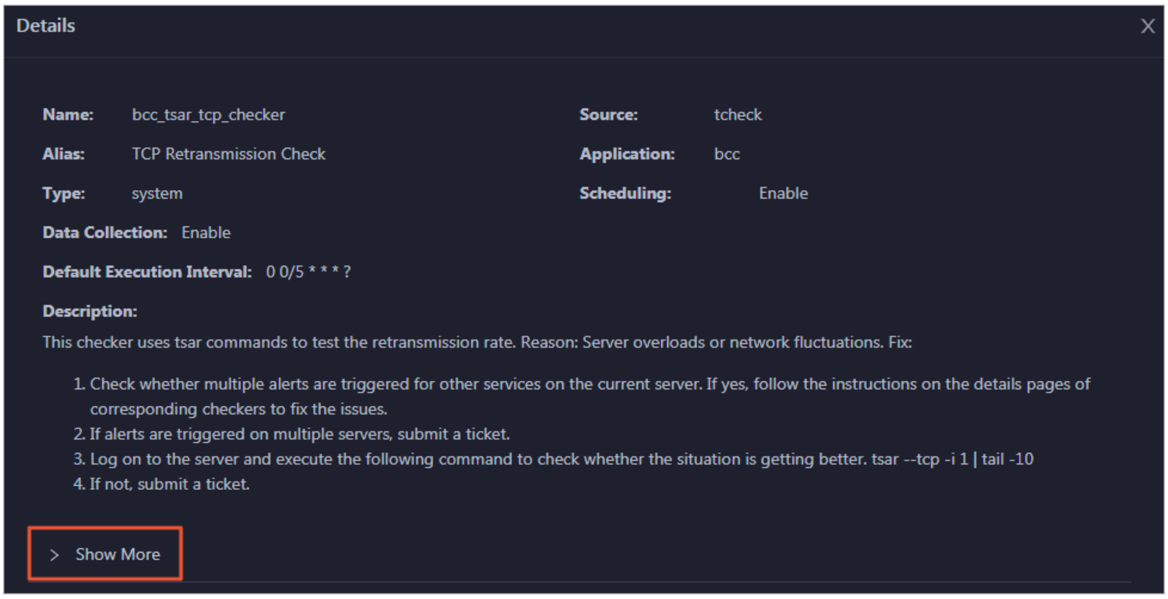
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include **Name**, **Source**, **Alias**, **Application**, **Type**, **Scheduling**, **Data Collection**, **Default Execution Interval**, and **Description**. The schemes to clear alerts are provided in the description.

2. Click **Show More** to view more information about the checker.



Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

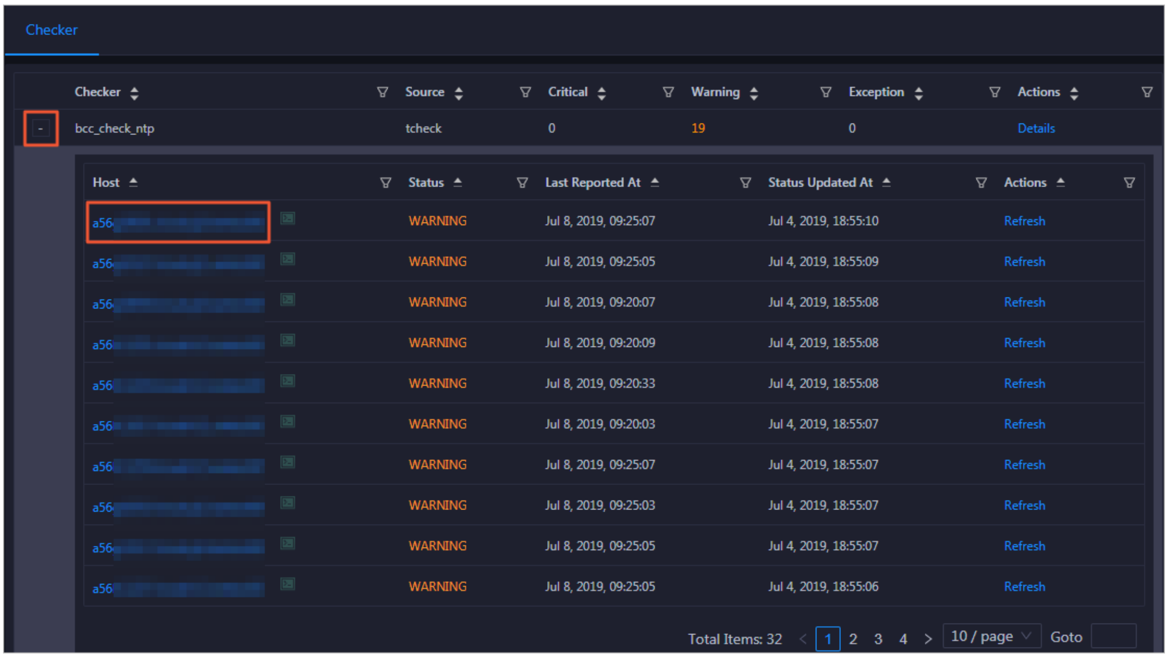
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about **Script**, **Target (TianJi)**, **Default Threshold**, and **Mount Point**.

View the hosts for which alerts are reported and causes for the alerts

You can view the check history and check results of a checker on a host.

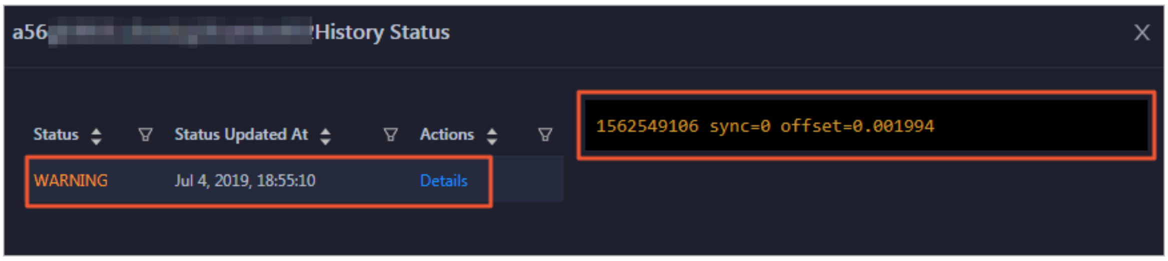
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported. You can view all hosts where the checker is run.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:06	Refresh

2. Click a hostname. In the panel that appears, click **Details** in the Actions column of a check result to view the cause of the alert.

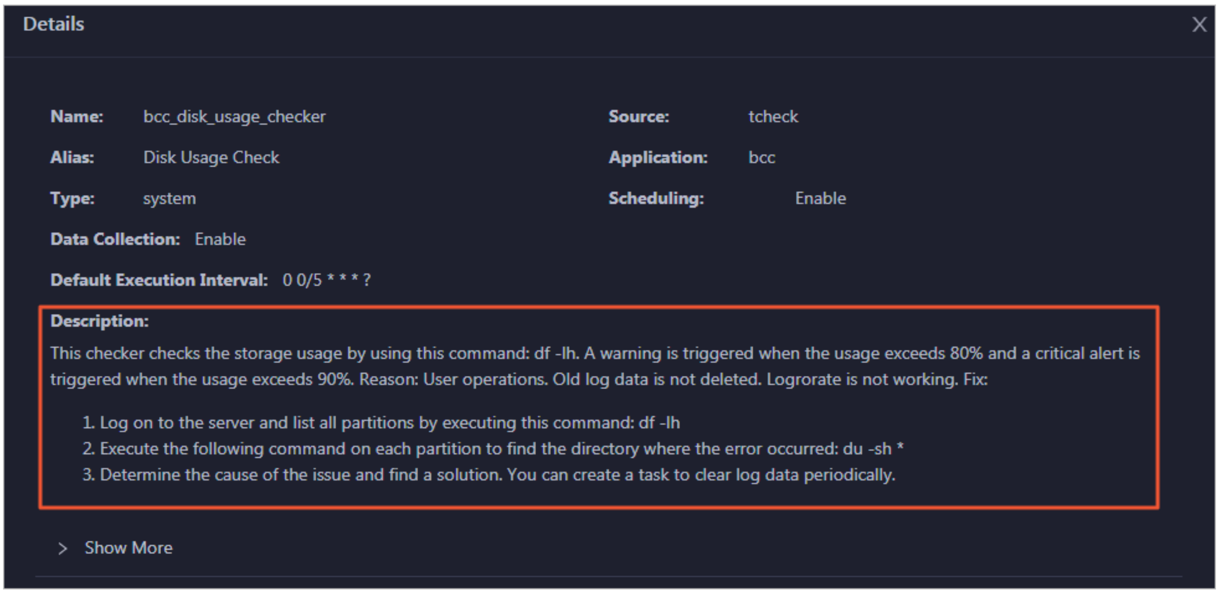

a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status tab, click **Details** in the Actions column of a checker for which alerts are reported. On the Details page, view the schemes to clear alerts.


Details

Name: bcc_disk_usage_checker
Source: tcheck
Alias: Disk Usage Check
Application: bcc
Type: system
Scheduling: Enable
Data Collection: Enable
Default Execution Interval: 0 0/5 * * * ?

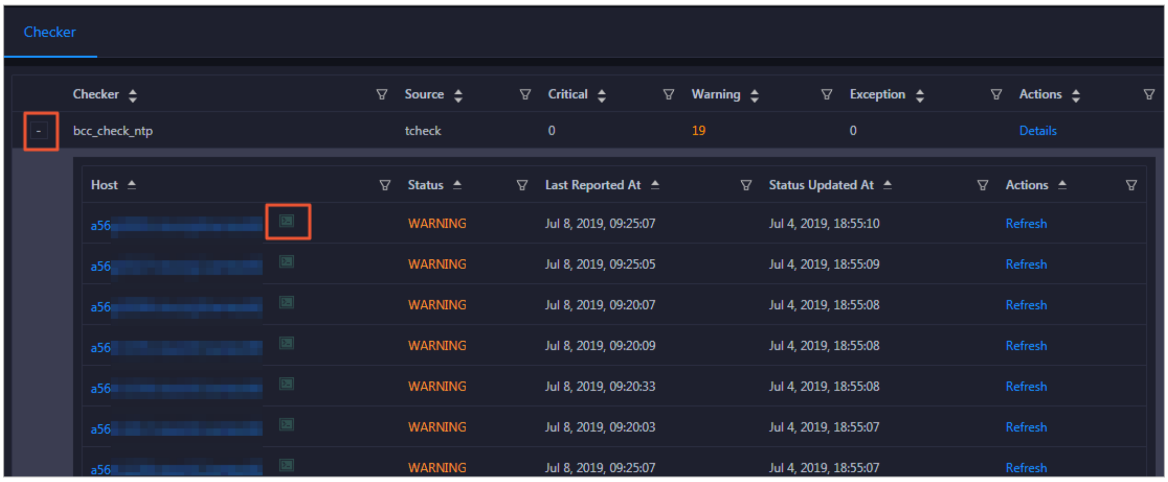
Description:
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

You may need to log on to a host to handle alerts or other issues that occurred on the host.

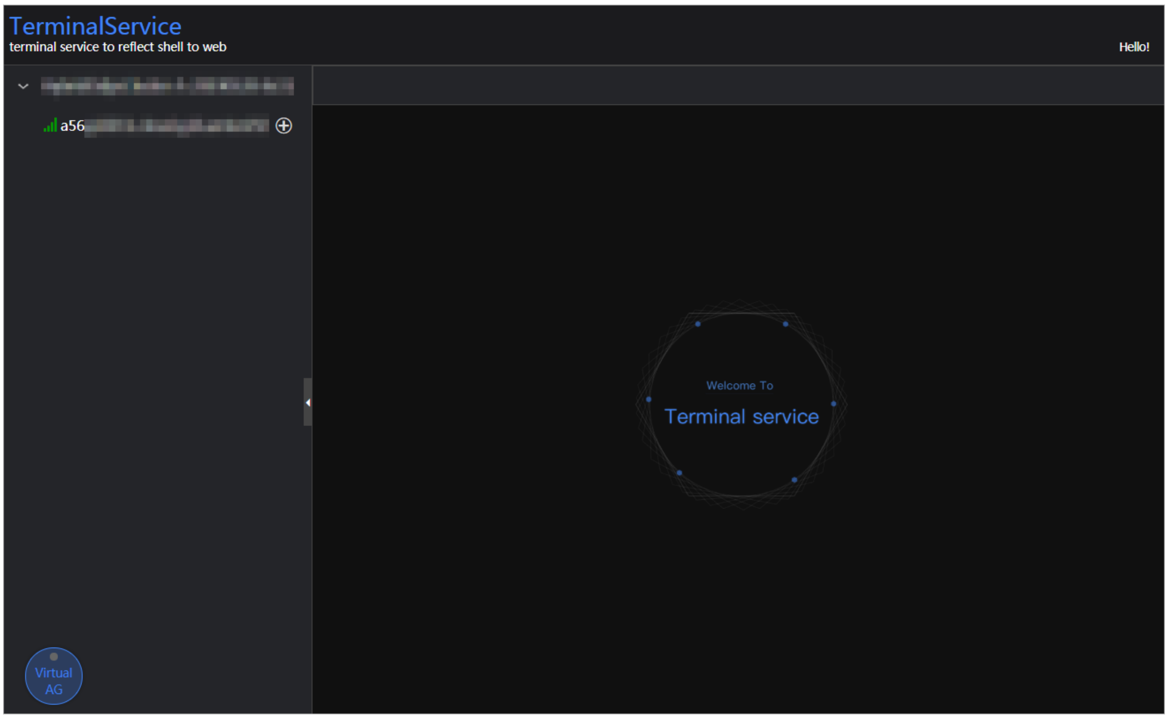
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported.



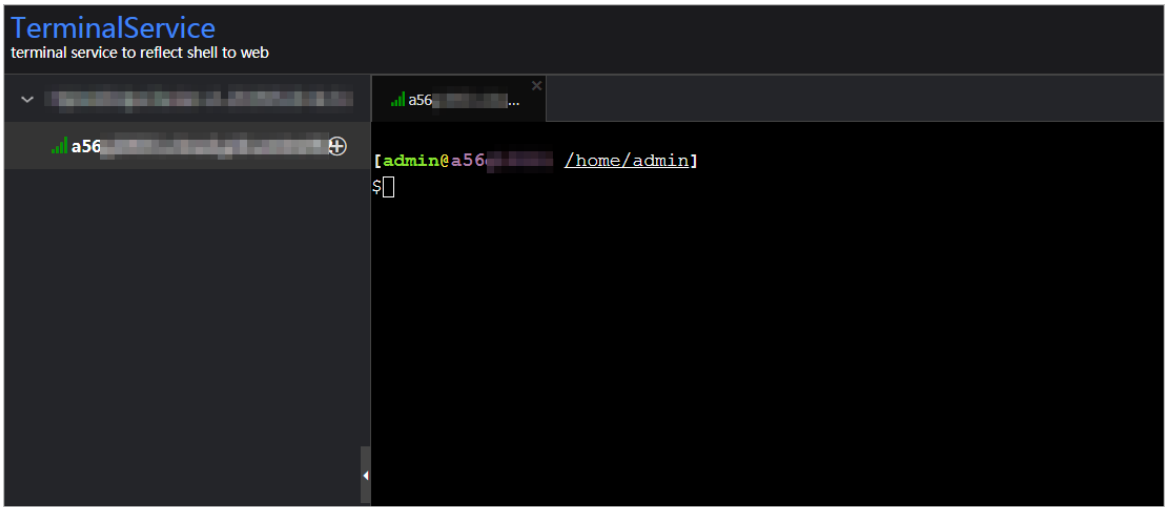
Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

2. Click the **Login in** icon of a host. The **TerminalService** page appears.



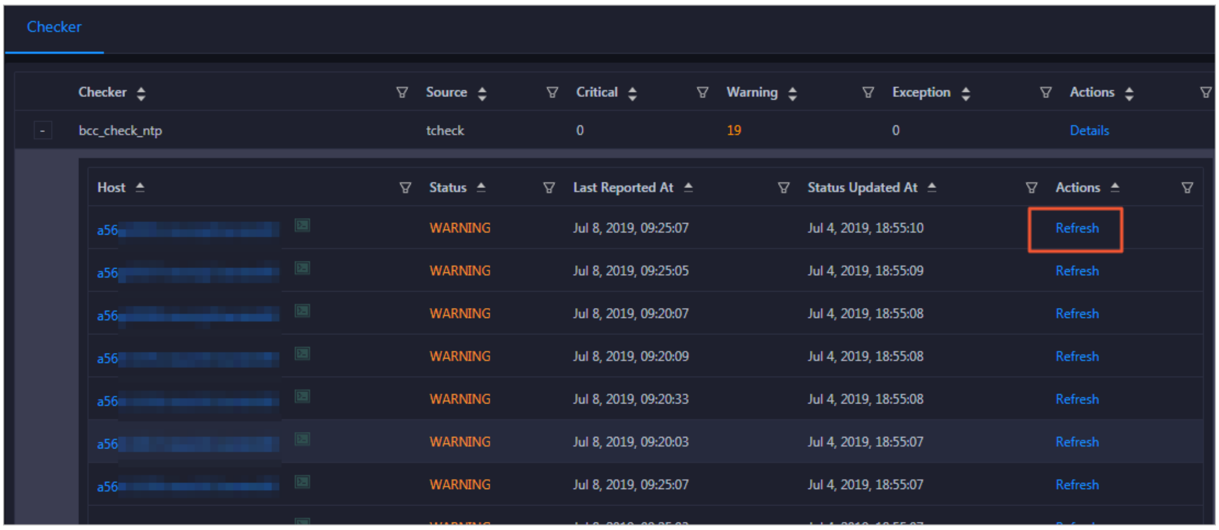
3. On the **TerminalService** page, click the hostname in the left-side navigation pane to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. This way, you can check whether the alert is cleared.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

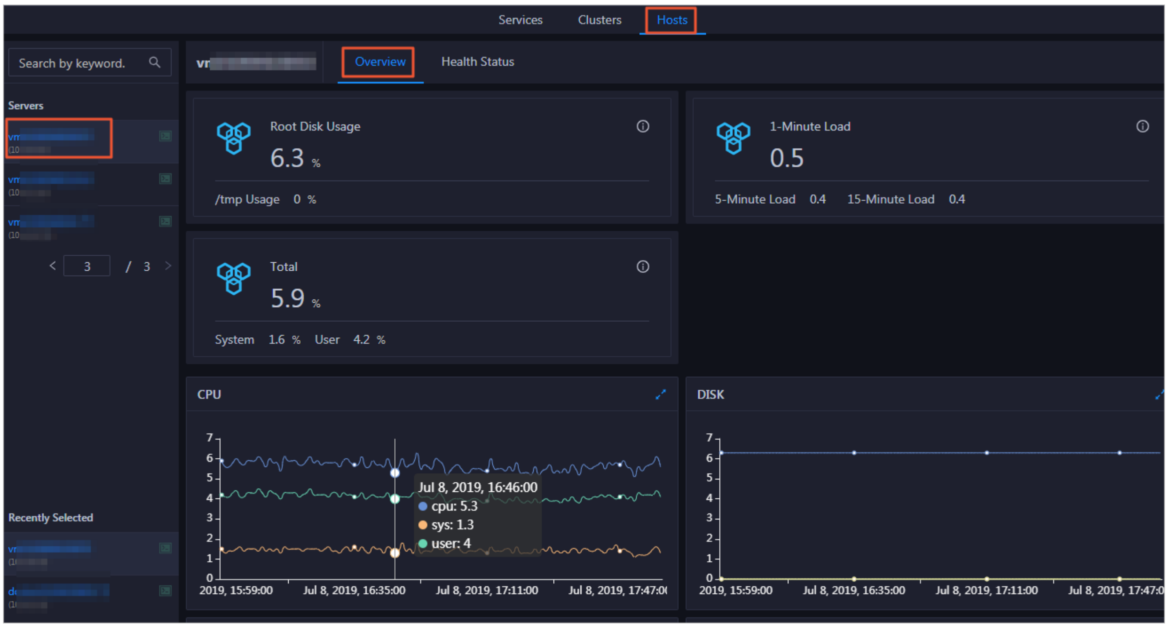
11.6.3.5. Host O&M

11.6.3.5.1. Host overview

The host overview page displays the overall running information about a host in an ElasticSearch cluster. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.

Entry

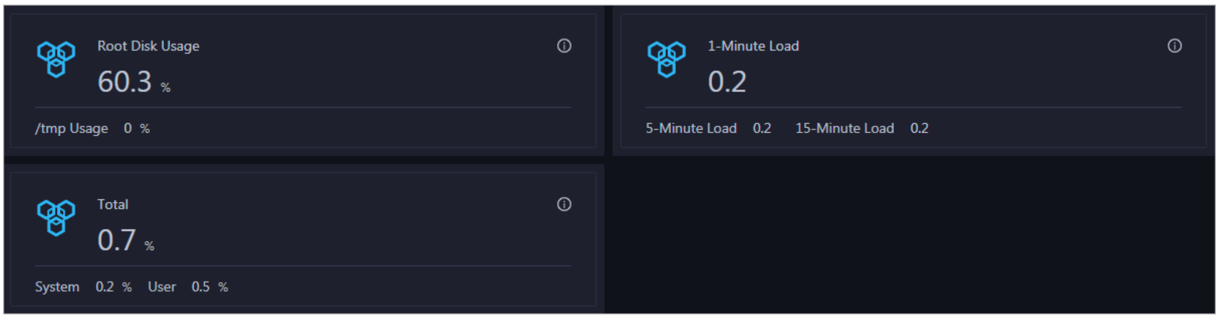
1. At the top of the **O&M** page, click **Hosts**.
2. On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Overview** tab. The **Overview** page for the host appears.



On the **Overview** page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.

Root Disk Usage, Total, and 1-Minute Load

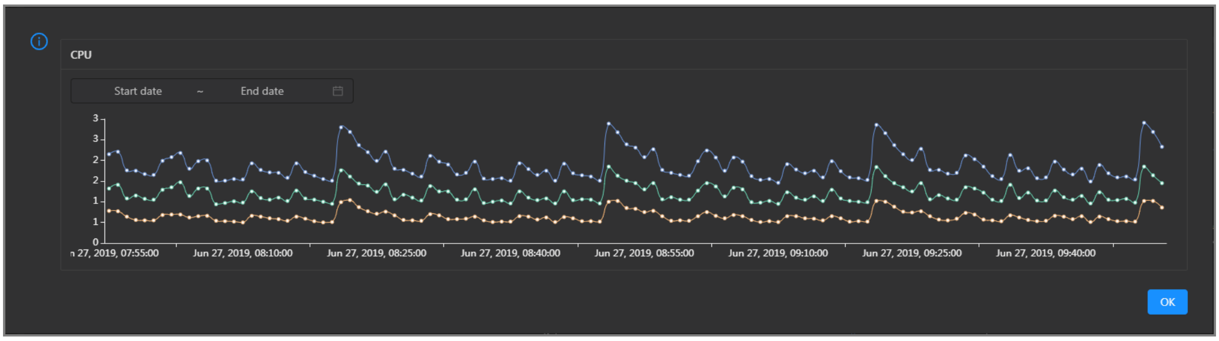
These sections display the root disk usage, total usage, and 1-minute load for the selected host. The Root Disk Usage section provides the usage of the */tmp* directory. The Total section provides the system usage and user usage. The 1-Minute Load section provides the 1-minute, 5-minute, and 15-minute load averages.



CPU

The CPU chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) of the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

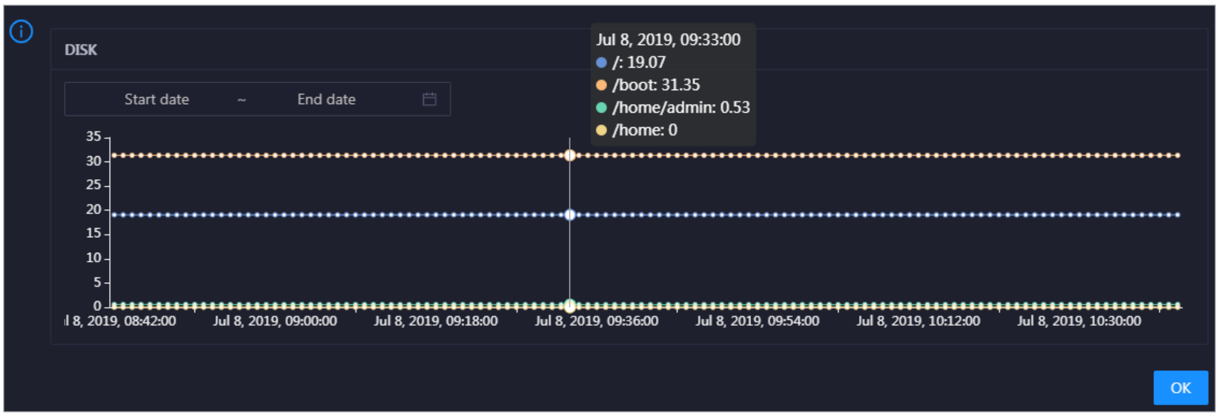


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the host in the specified period.

DISK

The DISK chart shows the trend lines of the storage usage in the */*, */boot*, */home/admin*, and */home* directories for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

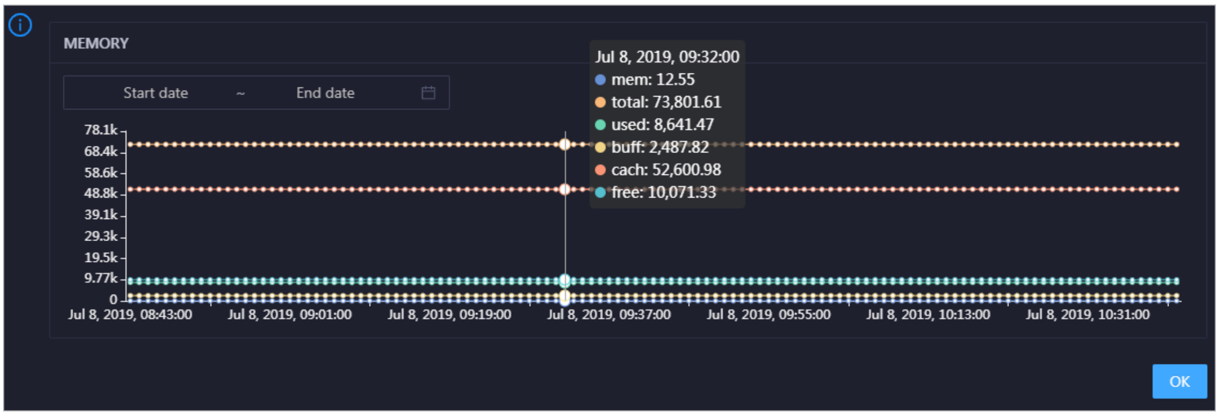


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the host in the specified period.

MEMORY

The MEMORY chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

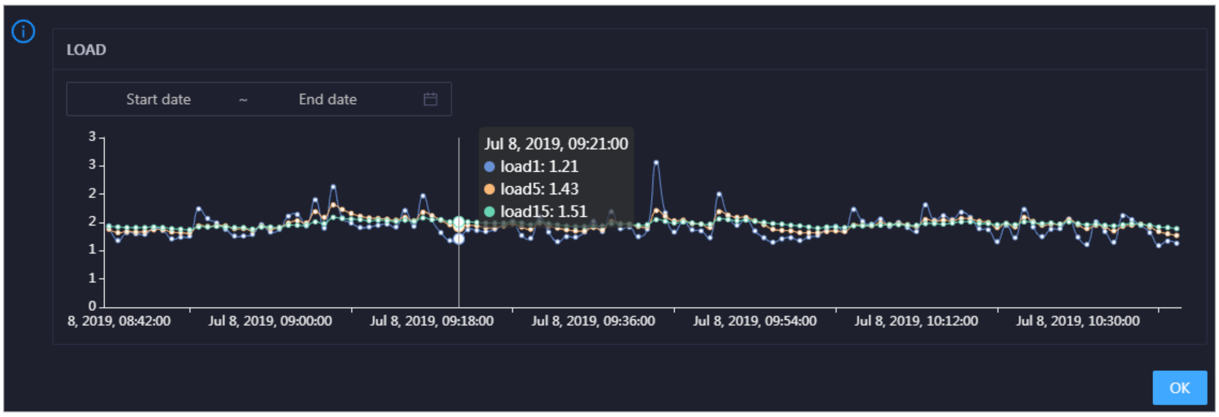


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the host in the specified period.

LOAD

The LOAD chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

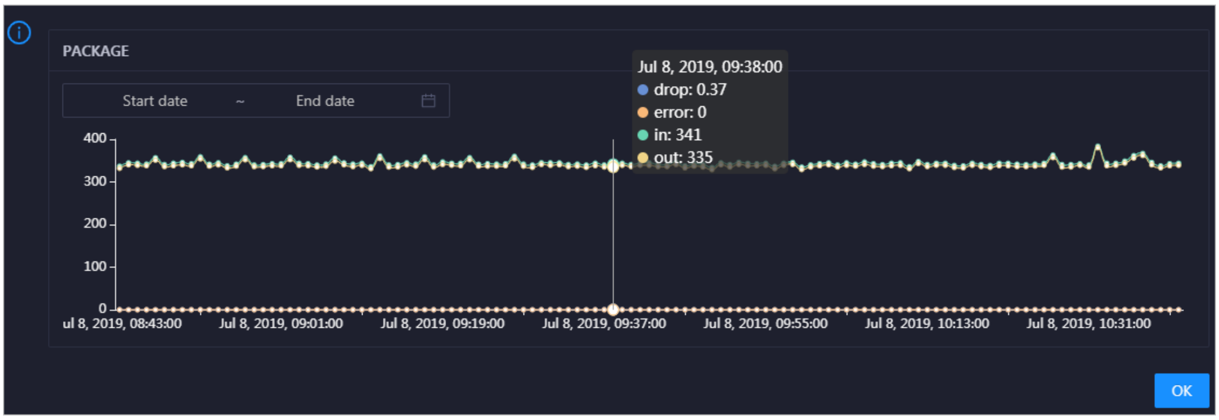


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the host in the specified period.

PACKAGE

The PACKAGE chart shows the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the host over time in different colors. These trend lines reflect the data transmission status of the host.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

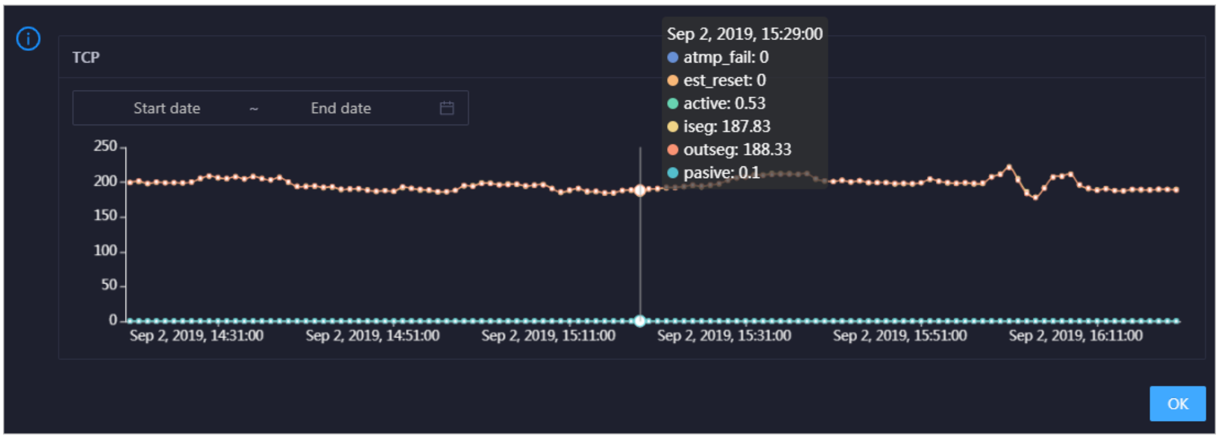


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the host in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the host over time in different colors. These trend lines reflect the TCP connection status of the host.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

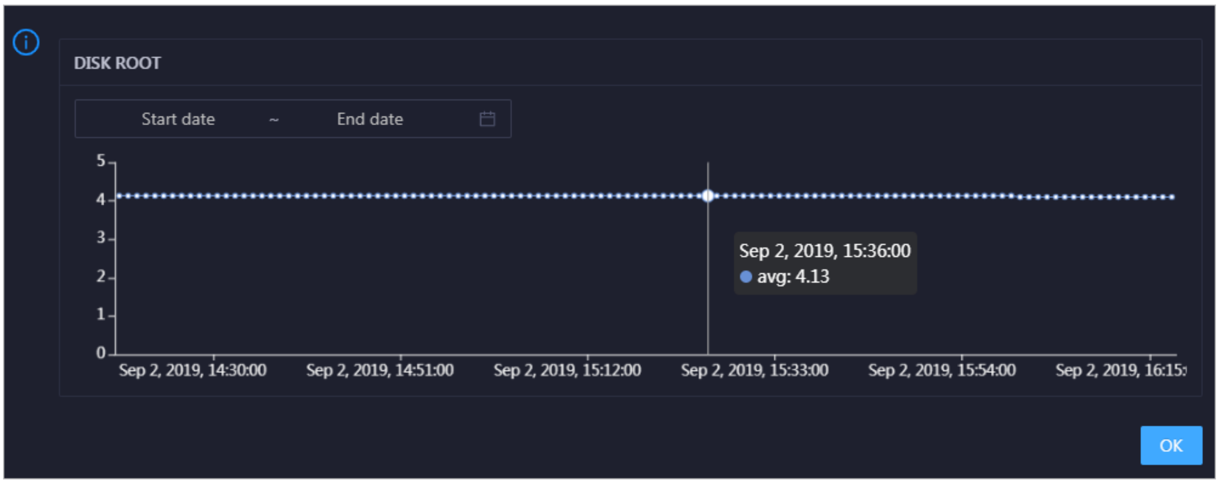


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the host in the specified period.

DISK ROOT

This chart displays the trend line of the average usage of the root disk (/) for the host over time.

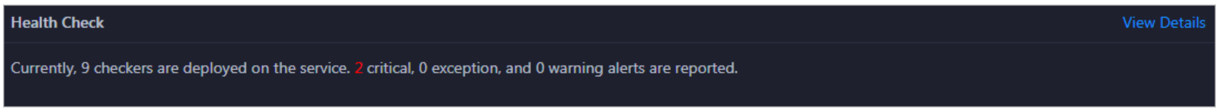
Click ⤢ in the upper-right corner of the chart to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the host in the specified period.

Health Check

This section displays the number of checkers deployed for the host and the respective number of Critical, Warning, and Exception alerts.

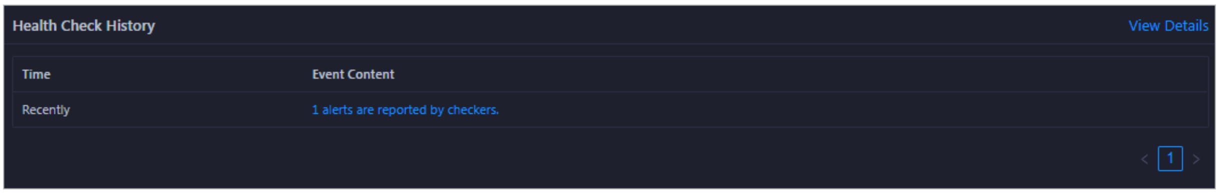


Currently, 9 checkers are deployed on the service. 2 critical, 0 exception, and 0 warning alerts are reported.

Click **View Details** to go to the Host health page. On this page, you can view the health check details.

Health Check History

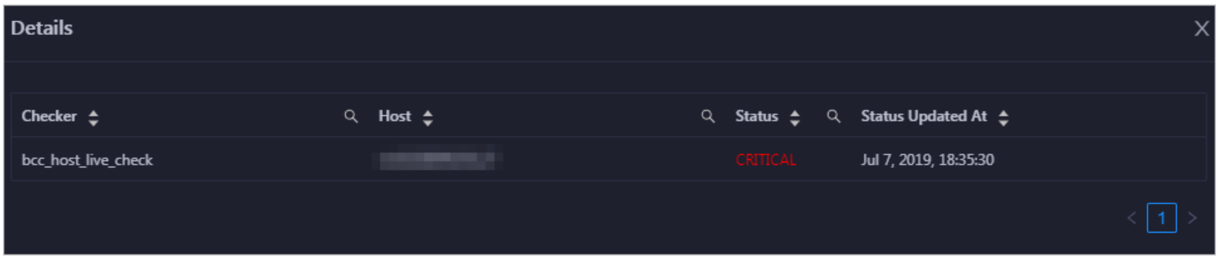
This section displays a record of the health checks performed on the host.



Time	Event Content
Recently	1 alerts are reported by checkers.

Click **View Details** to go to the Host health page. On this page, you can view the health check details.

You can click the event content of a check to view the exception items.



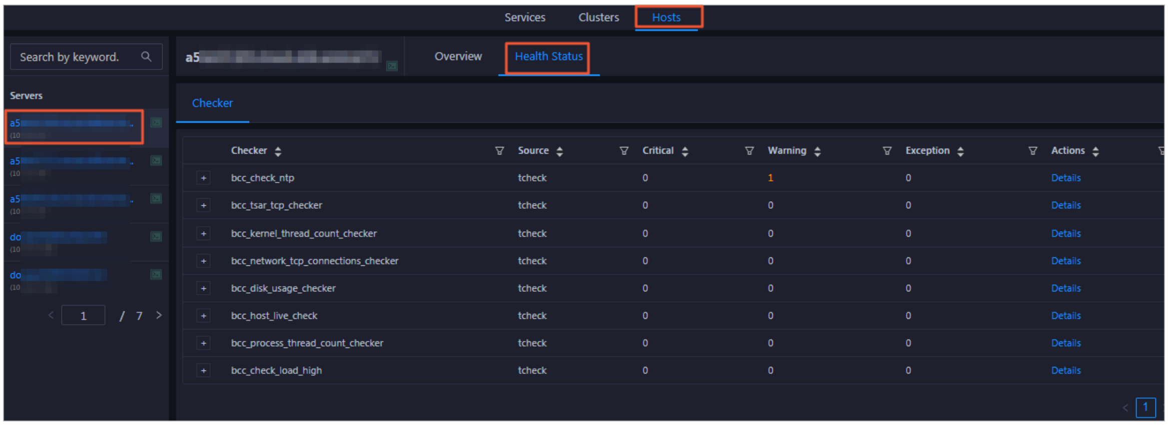
Checker	Host	Status	Status Updated At
bcc_host_live_check	[redacted]	CRITICAL	Jul 7, 2019, 18:35:30

11.6.3.5.2. Host health

On the Health Status page, you can view the checkers of the selected host, including the checker details, check results, and schemes to clear alerts (if any). In addition, you can log on to the host and perform manual checks on the host.

Entry

1. At the top of the **O&M** page, click **Hosts**.
2. On the page that appears, select a host in the left-side navigation pane, and then click the **Health Status** tab. The **Health Status** page for the host appears.

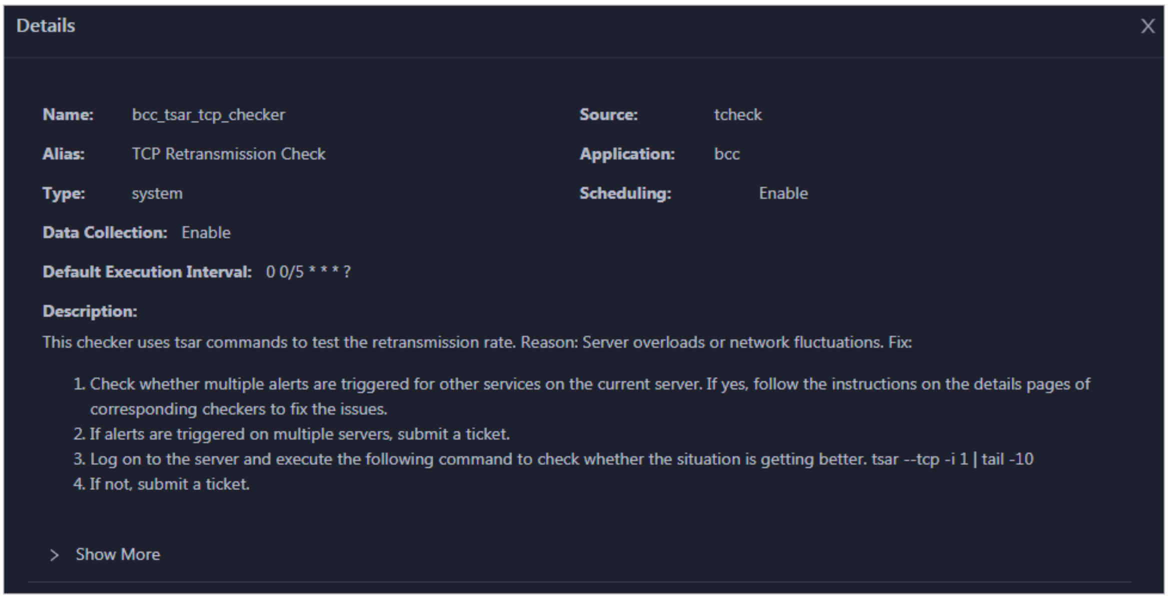


Checker	Source	Critical	Warning	Exception	Actions
+ bcc_check_ntp	tcheck	0	1	0	Details
+ bcc_tsar_tcp_checker	tcheck	0	0	0	Details
+ bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
+ bcc_network_tcp_connections_checker	tcheck	0	0	0	Details
+ bcc_disk_usage_checker	tcheck	0	0	0	Details
+ bcc_host_live_check	tcheck	0	0	0	Details
+ bcc_process_thread_count_checker	tcheck	0	0	0	Details
+ bcc_check_load_high	tcheck	0	0	0	Details

On the **Health Status** page, you can view all checkers and the check results for the host. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

View checker details

1. On the Health Status page, click **Details** in the Actions column of a checker. In the dialog box that appears, view the checker details.



Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

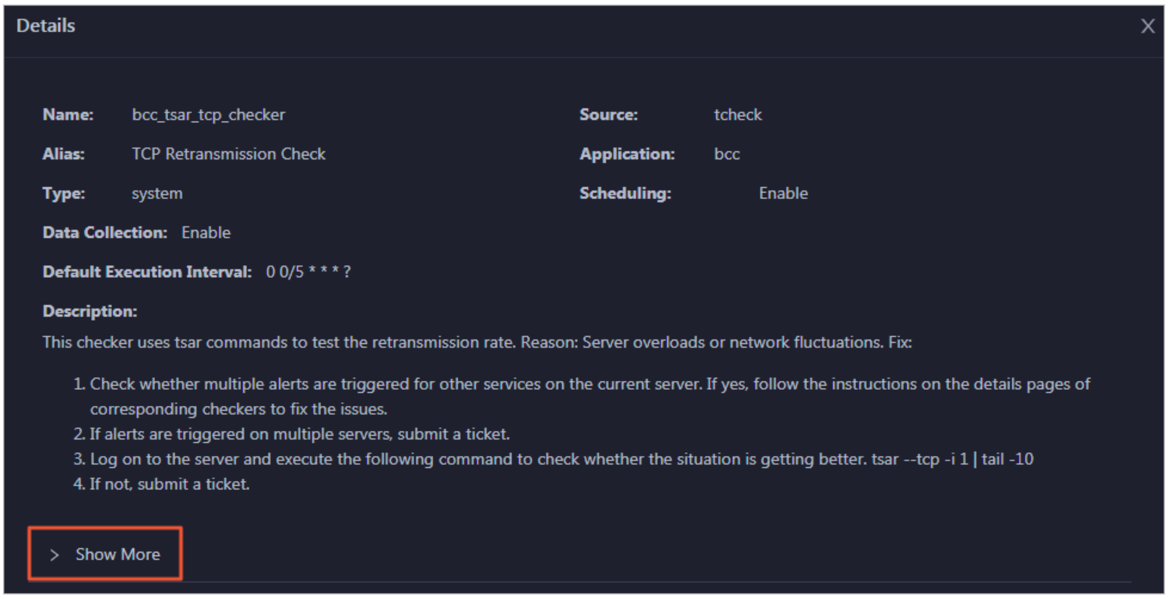
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include the name, source, alias, application, type, default execution interval, and description of the checker, whether scheduling is enabled, and whether data collection is enabled. The schemes to clear alerts are provided in the description.

2. Click **Show More** at the bottom to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

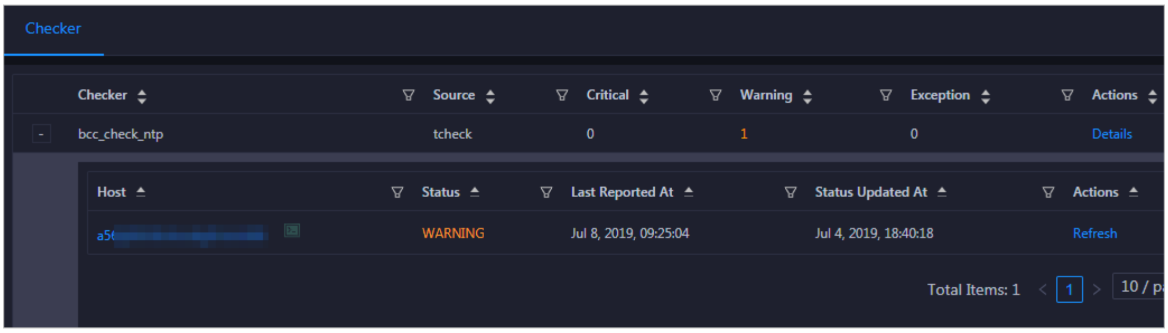
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about the execution script, execution target, default threshold, and mount point for data collection.

View alert causes

You can view the check history and check results of a checker.

1. On the Health Status page, click **+** to expand a checker with alerts.

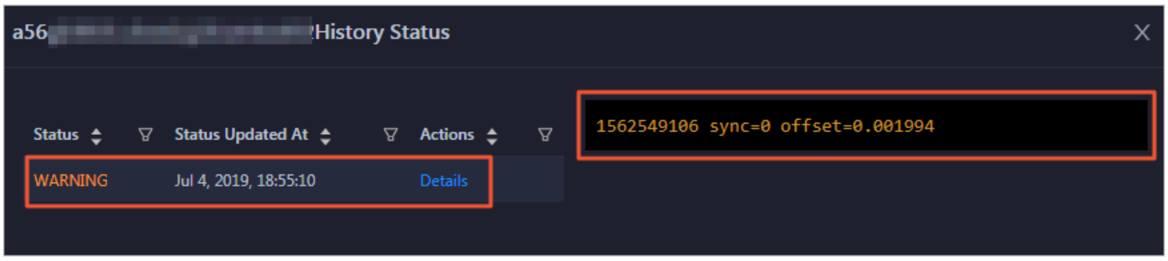


	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

2. Click the hostname. In the dialog box that appears, click **Details** in the Actions column of a check result to view the alert causes.



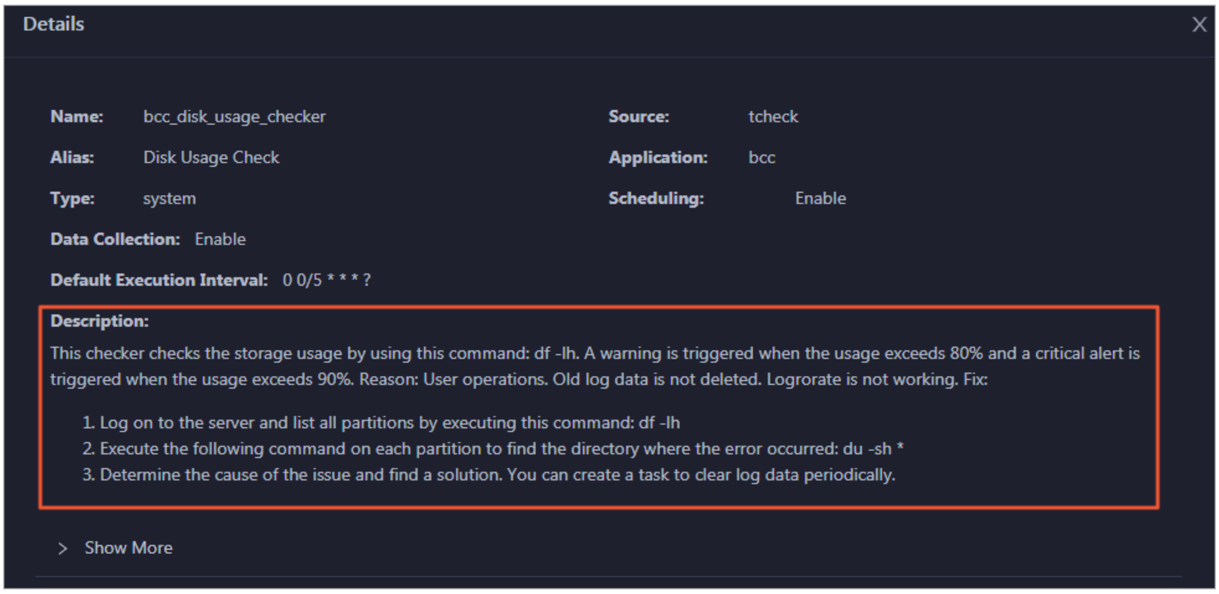
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status page, click **Details** in the Actions column of a checker with alerts. In the dialog box that appears, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker

Alias: Disk Usage Check

Type: system

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Source: tcheck

Application: bcc

Scheduling: Enable

Description:

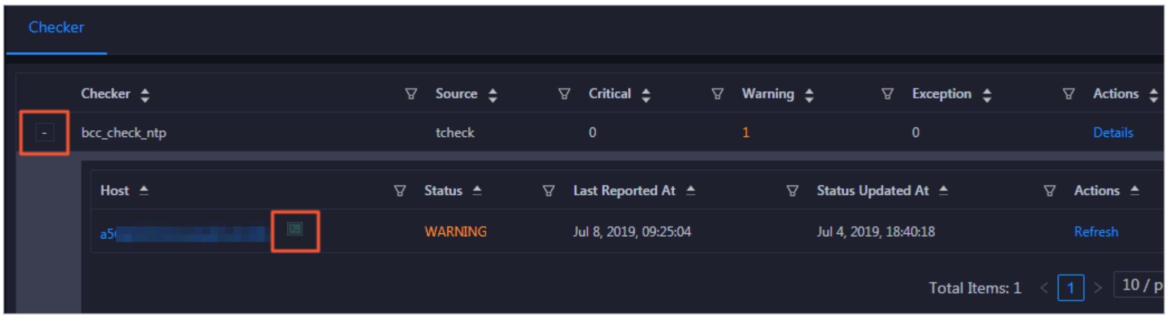
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

To log on to a host to clear alerts or perform other operations, follow these steps:

1. On the Health Status page, click **+** to expand a checker with alerts.

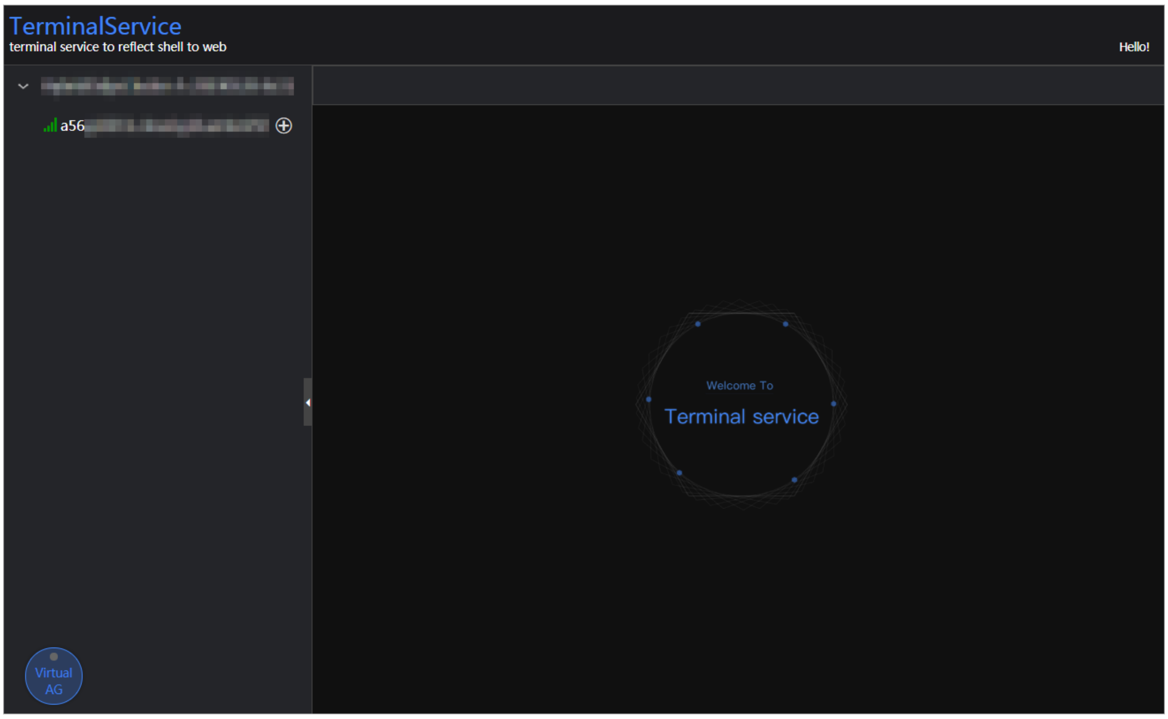


	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

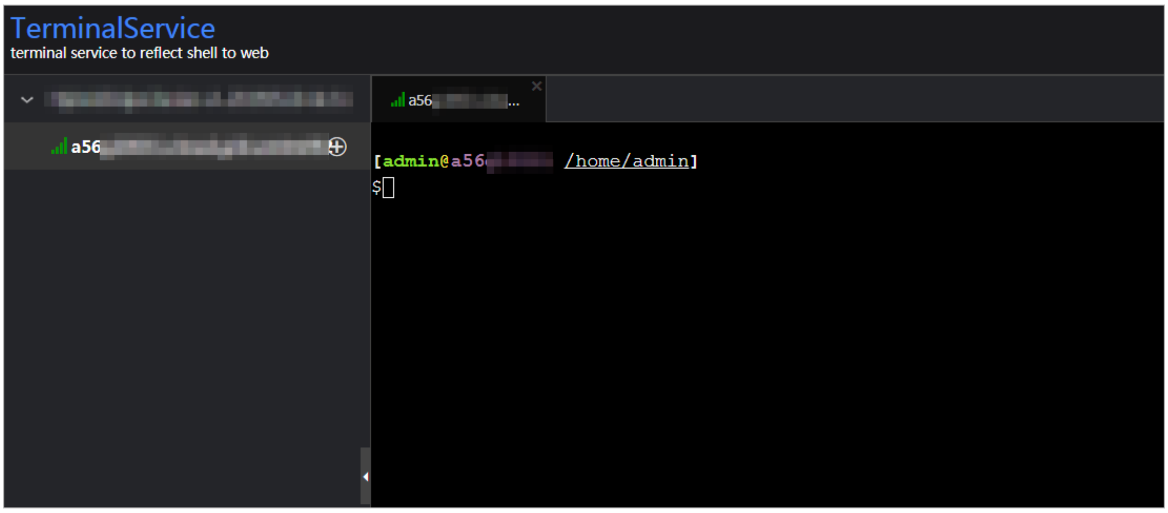
Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

2. Click the **Log On** icon of a host. The **TerminalService** page appears.



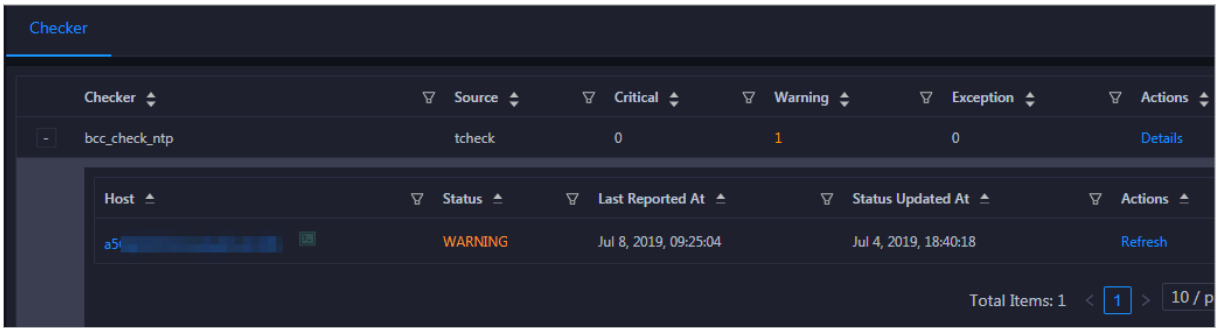
3. On the **TerminalService** page, click the hostname on the left to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. In this way, you can check whether the alert is cleared.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

11.7. Graph Analytics

11.7.1. Operations and maintenance tools and logon methods

11.7.1.1. Log on to the ABM console

This topic describes how to log on to the Apsara Big Data Manager (ABM) console.

Prerequisites

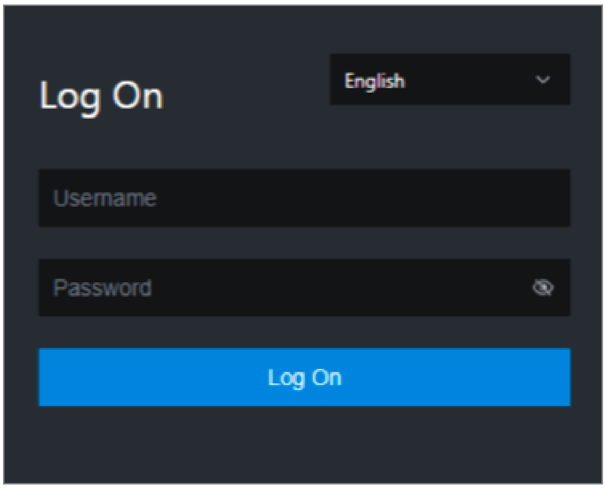
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.

   Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

   When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

For security reasons, your password must meet the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password must be 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Product Management > Products**.
7. In the **Big Data Services** section, choose **General-Purpose O&M > Apsara Big Data Manager**.

11.7.1.2. Log on to Apsara Infrastructure Management Framework

This topic describes how to log on to Apsara Infrastructure Management Framework. Apsara Infrastructure Management Framework supports operations and maintenance (O&M) management for Graph Analytics.

Prerequisites

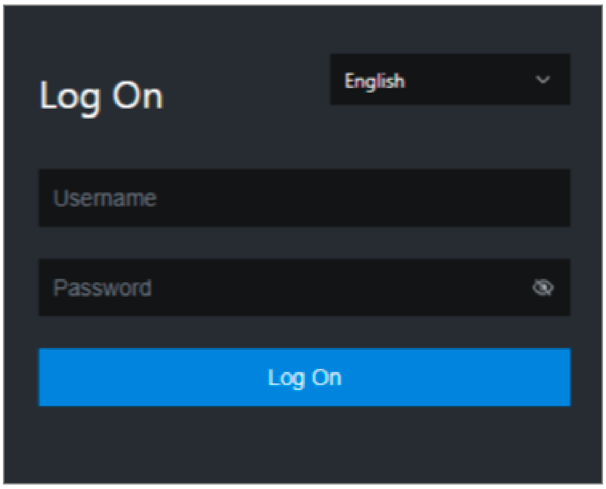
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.



> **Note** You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

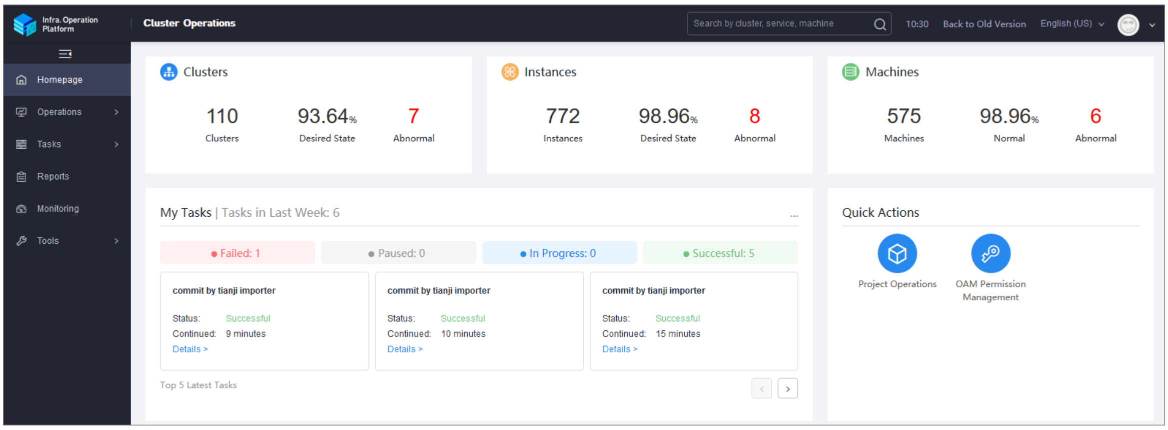
   > **Note** Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

   When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   For security reasons, your password must meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password must be 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Management Console, click **Operations**.
6. In the left-side navigation pane, choose **Products > Product List**.
7. On the Product List page, choose Apsara Stack O&M > Apsara Infrastructure Management Framework.



11.7.1.3. Log on to the Graph Analytics container

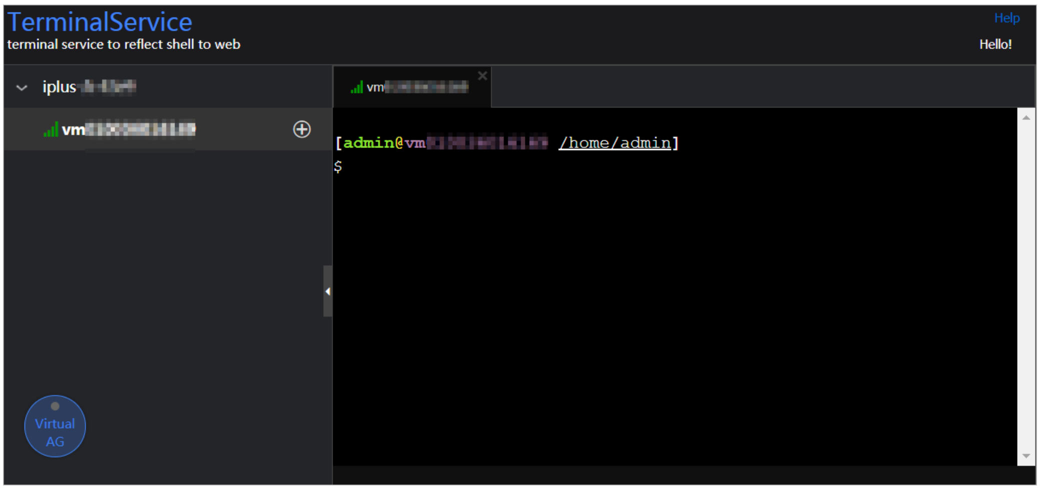
You can log on to the Graph Analytics container through Apsara Infrastructure Management Framework to perform operations and maintenance.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. In the left-side **Project** drop-down list, enter or select *iplus* to display Graph Analytics clusters.
3. Select a Graph Analytics cluster. On the **Services** page, double click **iplus-iplus_biz > IplusBizBackend#**. Click the More icon next to **vmxxxxxxxxxxxx** and then select **Terminal** in the menu that appears. The **TerminalService** page appears.

Operations and maintenance are typically performed on the virtual machines of **IplusBizBackend#** and **IplusBizBackendControl#**. You can use the same method to open the virtual machine where the **IplusBizBackendControl#** service is deployed.

TerminalService page

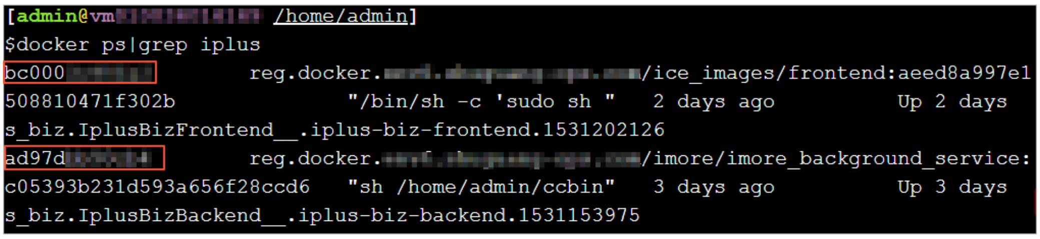


```
[admin@vm[redacted] /home/admin]
$
```

The left-side navigation pane on the **TerminalService** page displays the virtual machine selected by you (**vmxxxxxxxxxxxx**).

4. In the left-side navigation pane on the **TerminalService** page, click **vmxxxxxxxxxxxx**, and the command-line tool appears on the right-side of the page.
5. Run the **docker ps|grep** *iplus* command to query the docker ID in the Graph Analytics cluster.

   Query the docker ID



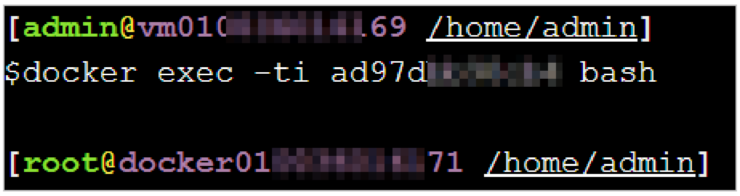
```
[admin@vm[redacted] /home/admin]
$docker ps|grep iplus
bc000[redacted]          reg.docker.[redacted]/ice_images/frontend:aeed8a997e1
508810471f302b            "/bin/sh -c 'sudo sh "   2 days ago          Up 2 days
s_biz.IplusBizFrontend__.iplus-biz-frontend.1531202126
ad97d[redacted]          reg.docker.[redacted]/imore/imore_background_service:
c05393b231d593a656f28ccd6   "sh /home/admin/ccbin"   3 days ago          Up 3 days
s_biz.IplusBizBackend__.iplus-biz-backend.1531153975
```

The query results of this sample display two docker IDs, which indicates that the **IplusBizBackend#** service is running on two containers.

6. Run the **docker exec -ti** *dockerID* **bash** command to log on to the docker container.

   Enter the docker ID of the container you need to log on to in *dockerID*.

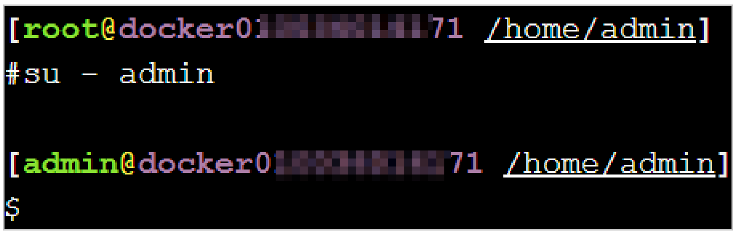
   Log on to the docker container



```
[admin@vm010[redacted]69 /home/admin]
$docker exec -ti ad97d[redacted] bash

[root@docker01[redacted]71 /home/admin]
```

7. The root account is used by default. You can use the **su - admin** command to switch to the admin account.

   Switch to the admin account



```
[root@docker0[redacted]71 /home/admin]
#su - admin

[admin@docker0[redacted]71 /home/admin]
$
```

11.7.2. Operations and maintenance

11.7.2.1. Operations and maintenance based on BigData Manager

11.7.2.1.1. O&M overview

This topic describes the features of I+ O&M and how to access the I+ O&M page.

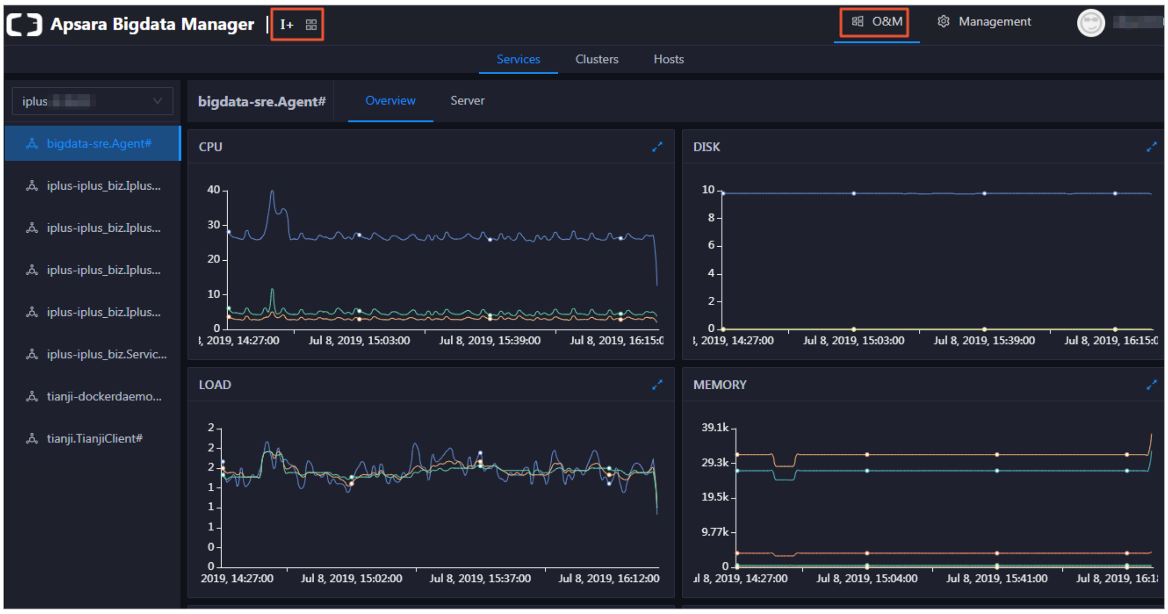
Modules

I+ O&M includes service O&M, cluster O&M, and host O&M. The following table describes them in detail.

Module	Feature	Description
Services	Service overview	Displays the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for each service in a cluster.
	Server	Displays the host list of each service in a cluster so that you can understand the service deployment on hosts.
Clusters	Cluster overview	Displays the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for a cluster.
	Cluster health	Displays all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.
Hosts	Host overview	Displays the overall running and health check information about a host. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.
	Host health	Displays the checkers of the selected host, including the checker details, check results, check history, and schemes to clear alerts (if any). In addition, you can log on to the host and perform manual checks on the host.

Entry

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner, and then click **I+** .
3. On the page that appears, click **O&M** in the top navigation bar. The **Services** page appears.



The **O&M** page includes three modules: **Services**, **Clusters**, and **Hosts**.

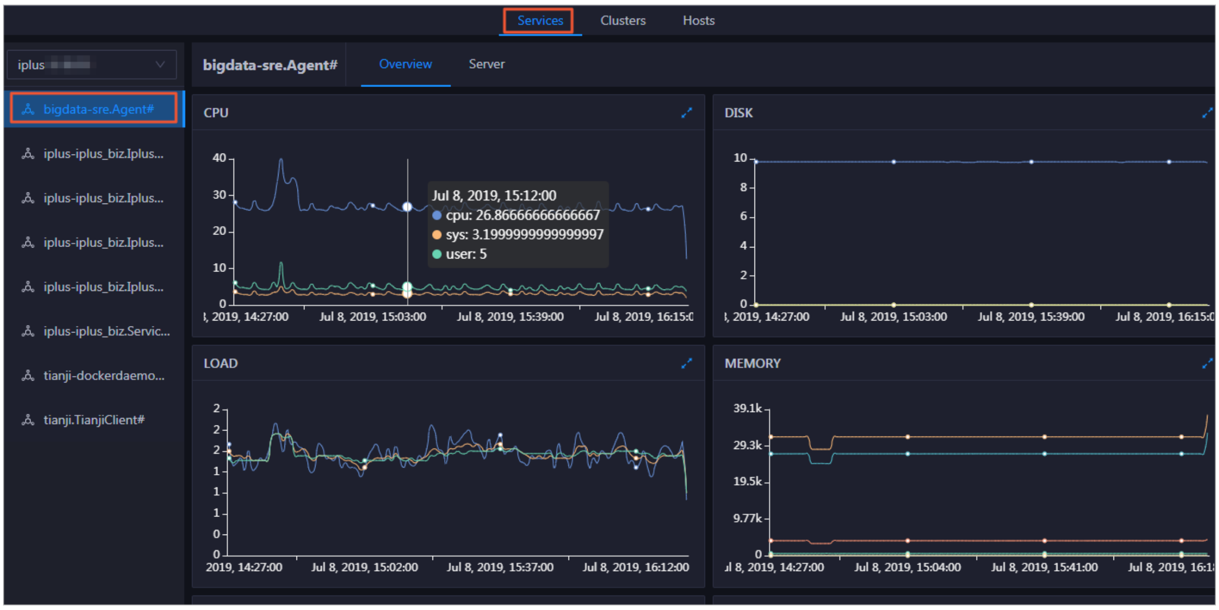
11.7.2.1.2. Service O&M

11.7.2.1.2.1. Service overview

The service overview page lists all I+ services in a cluster. You can view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for each service.

Entry

On the **Services** page, search for a cluster in the search box above the left-side service list, select a service in the service list, and then click the **Overview** tab. The **Overview** page for the service appears.



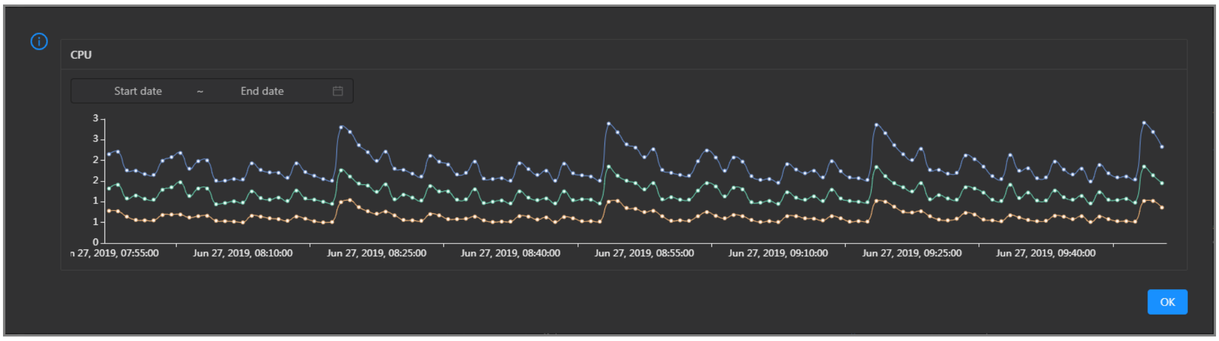
On the **Overview** page, you can view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the selected service.

CPU

This chart displays the trend lines of the total CPU usage (cpu), CPU usage for executing code in kernel space (sys), and CPU usage for executing code in user space (user) for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

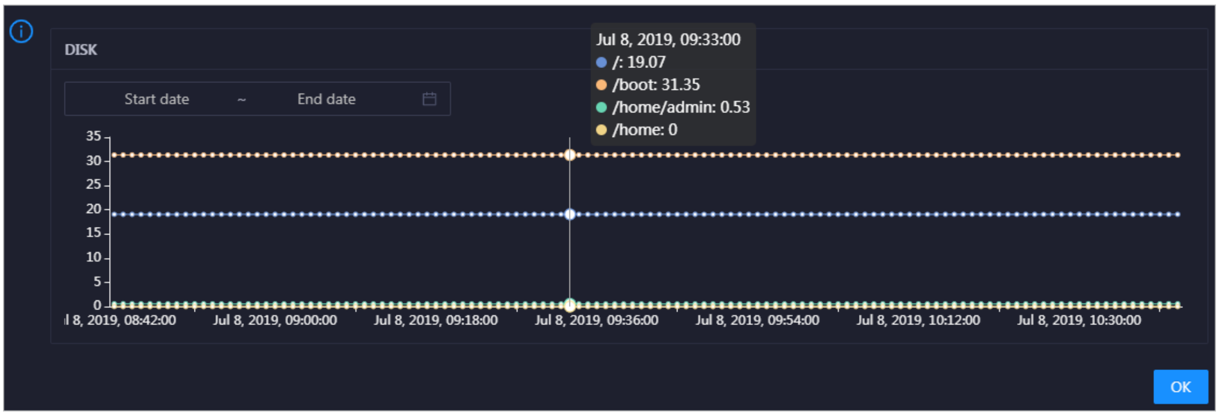
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU usage of the service in the specified period.



DISK

This chart displays the trend lines of the storage space usage on the */*, */boot*, */home/admin*, and */home* directories for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

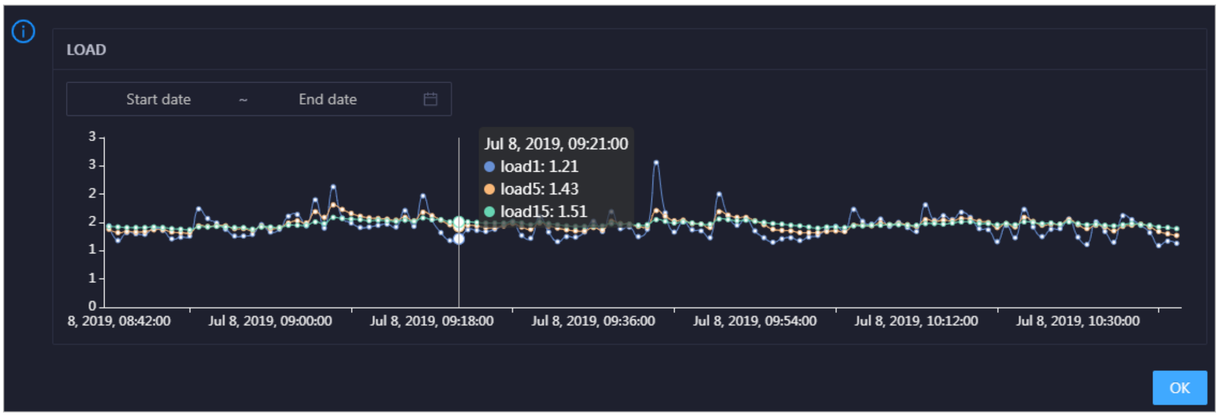


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage space usage of the service in the specified period.

LOAD

This chart displays the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

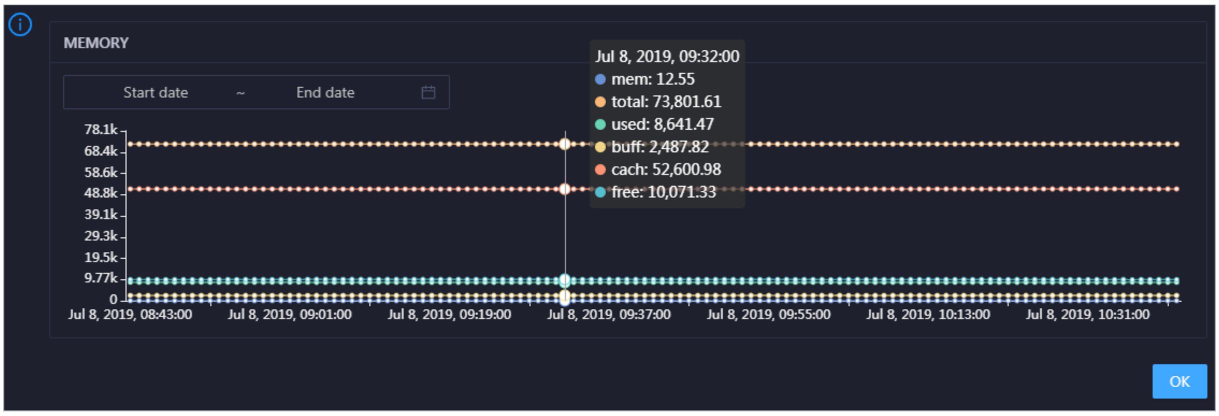


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the selected service in the specified period.

MEMORY

This chart displays the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

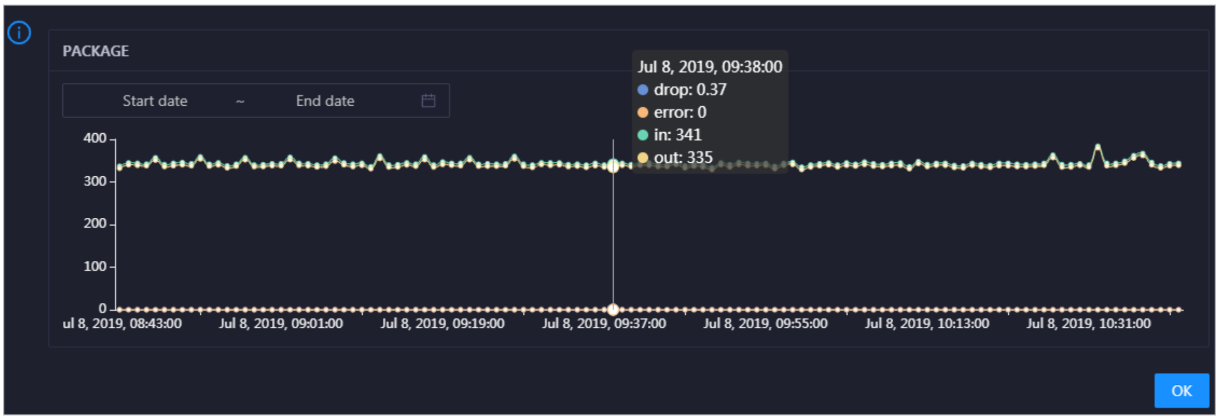


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the selected service in the specified period.

PACKAGE

This chart displays the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the selected service over time in different colors. These trend lines reflect the data transmission status of the service.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

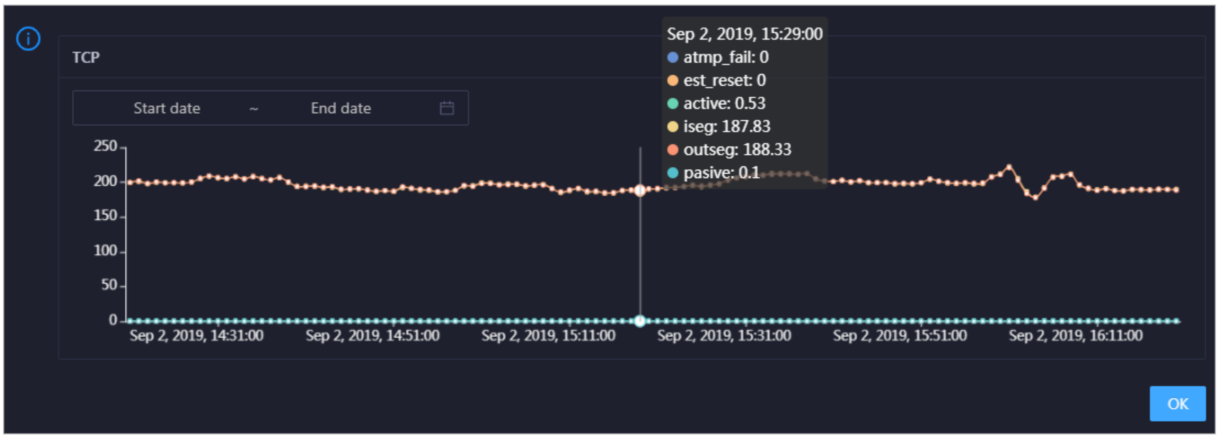


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the selected service in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the selected service over time in different colors. These trend lines reflect the TCP connection status of the service.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

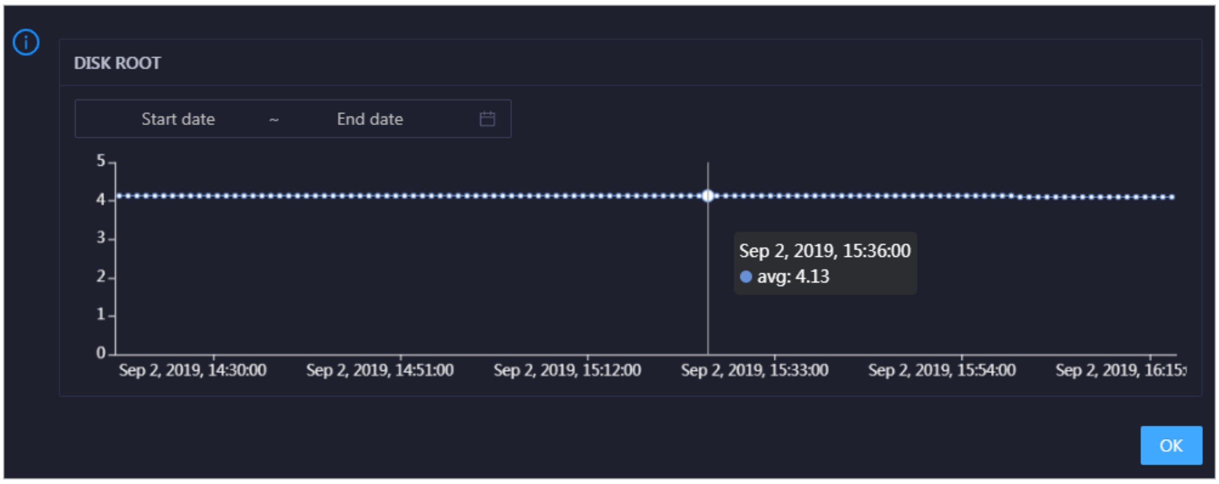


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the selected service in the specified period.

DISK ROOT

This chart displays the trend line of the average root disk usage (avg) for the selected service over time.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

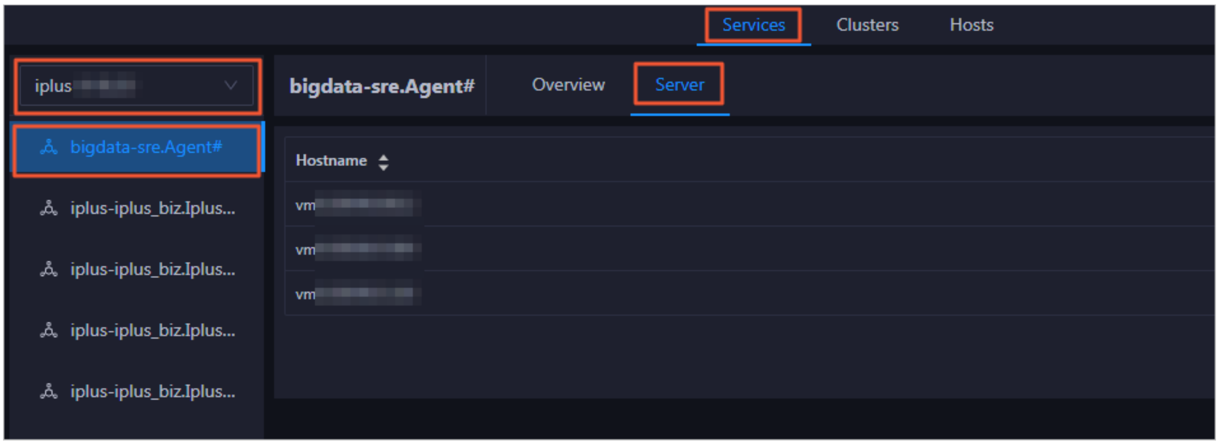


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the selected service in the specified period.

11.7.2.1.2.2. Service hosts

Apsara Big Data Manager allows you to view the hosts of each I+ service so that you can understand the service deployment on hosts.

On the **Services** page, search for a cluster in the search box above the left-side service list, select a service in the service list, and then click the **Server** tab. The **Server** page for the service appears.



Hostname
vm[redacted]
vm[redacted]
vm[redacted]

On the **Server** page, you can view the hosts where the selected service is run.

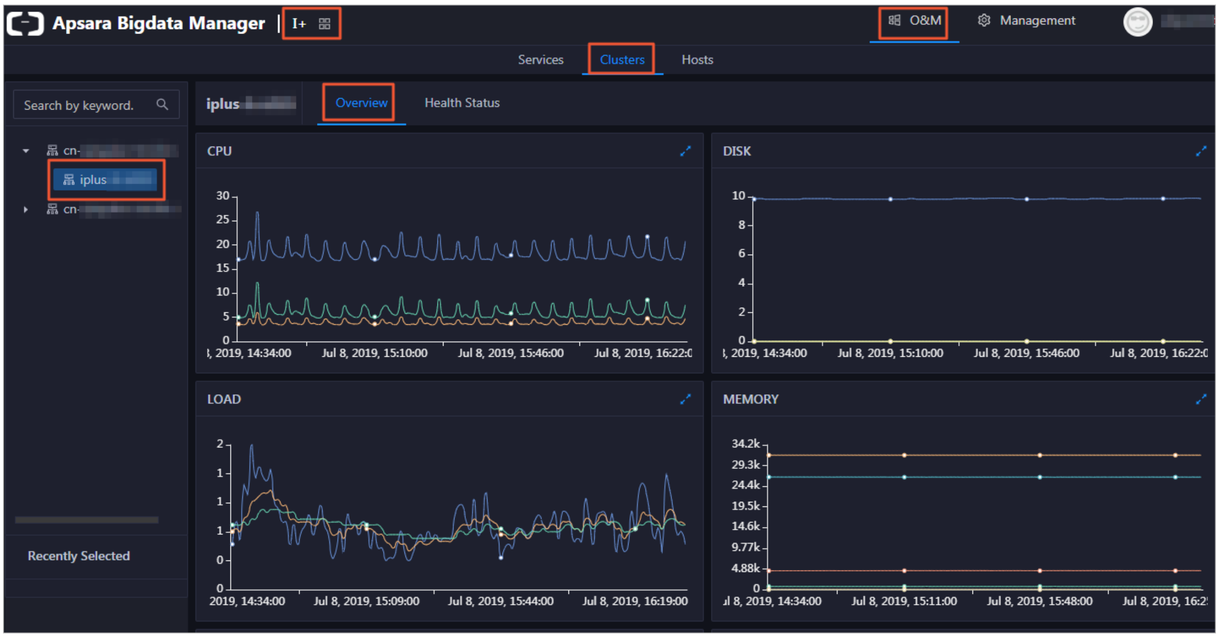
11.7.2.1.3. Cluster O&M

11.7.2.1.3.1. Cluster overview

The cluster overview page displays the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for a cluster.

Entry

On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Overview** tab. The **Overview** page for the cluster appears.

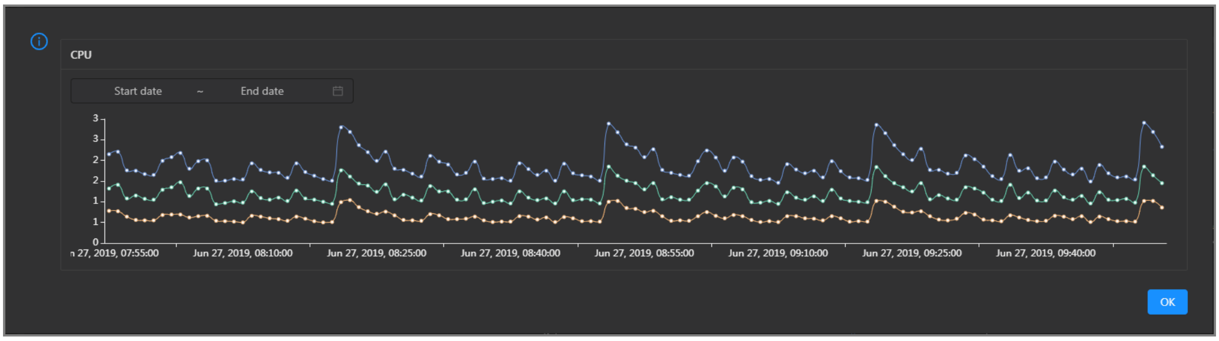


CPU

This chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

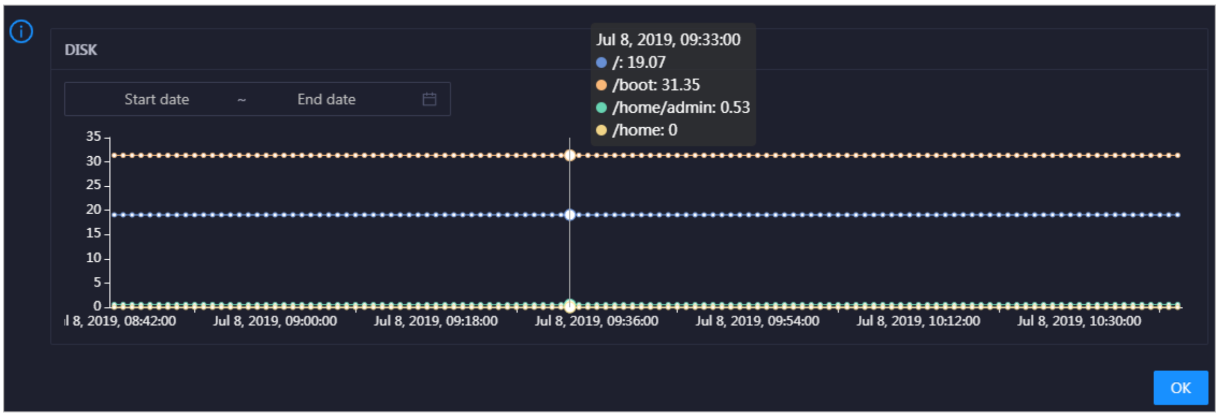
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the cluster in the specified period.



DISK

This chart shows the trend lines of the storage usage on the */*, */boot*, */home/admin*, and */home* directories for the cluster over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

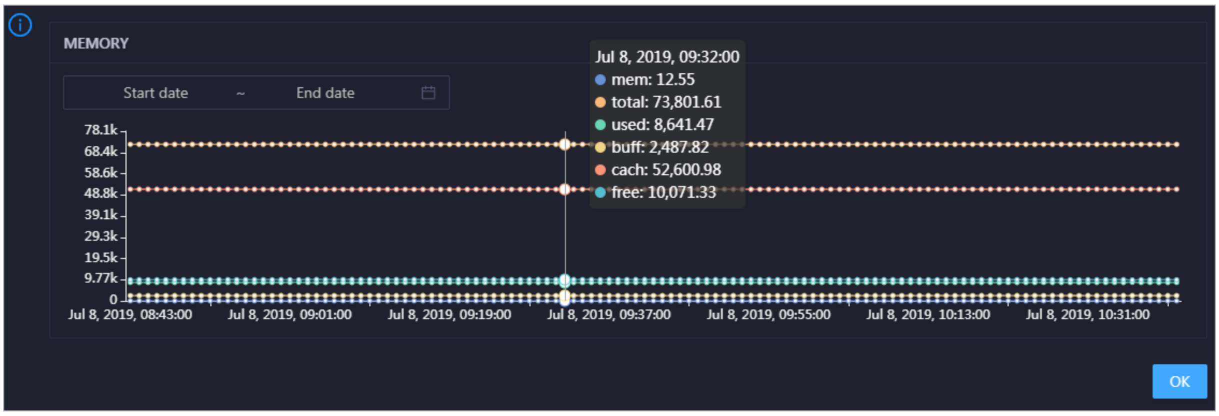


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

MEMORY

This chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

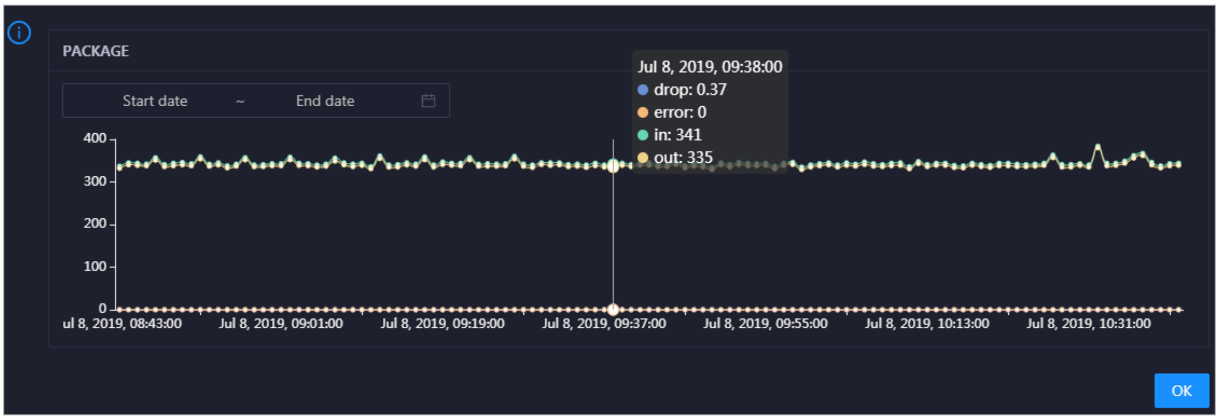


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the cluster in the specified period.

PACKAGE

This chart shows the trend lines of the numbers of dropped packets (drop), error packets (error), received packets (in), and sent packets (out) for the cluster in different colors. These trend lines reflect the data transmission status of the cluster.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

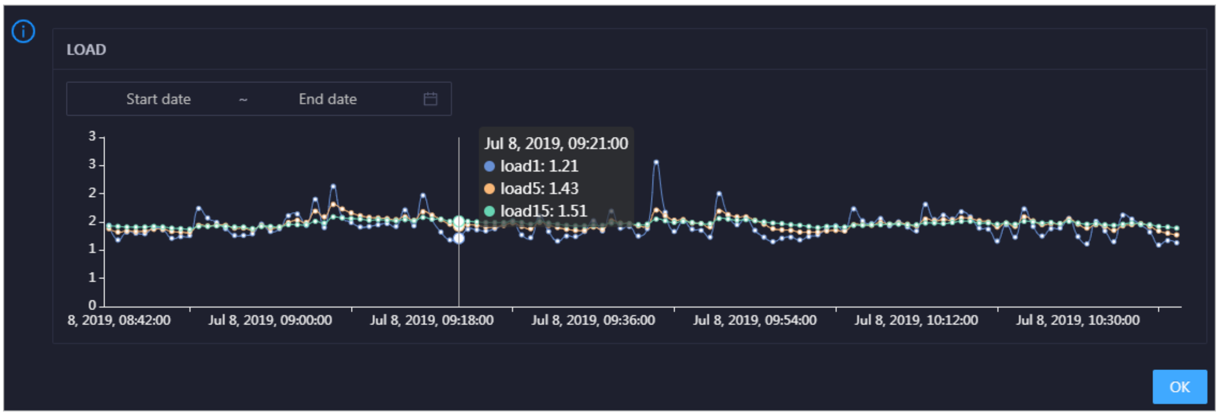


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the cluster in the specified period.

LOAD

This chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



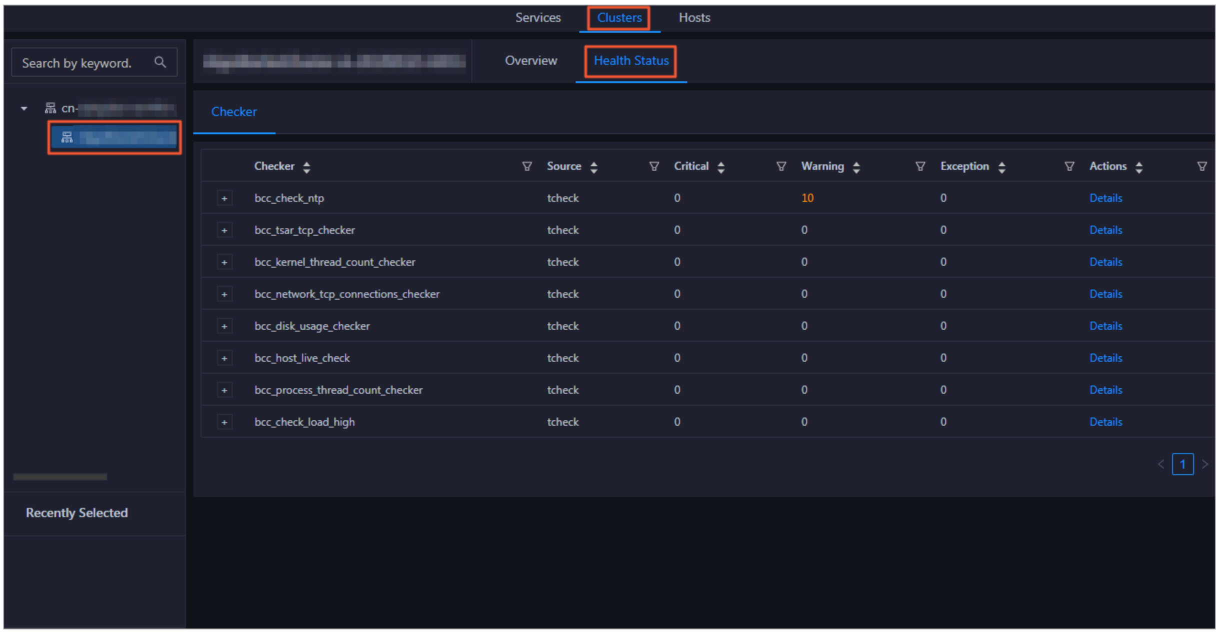
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the cluster in the specified period.

11.7.2.1.3.2. Cluster health

On the Health Status page, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Entry

On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Health Status** tab. The Health Status page for the cluster appears.

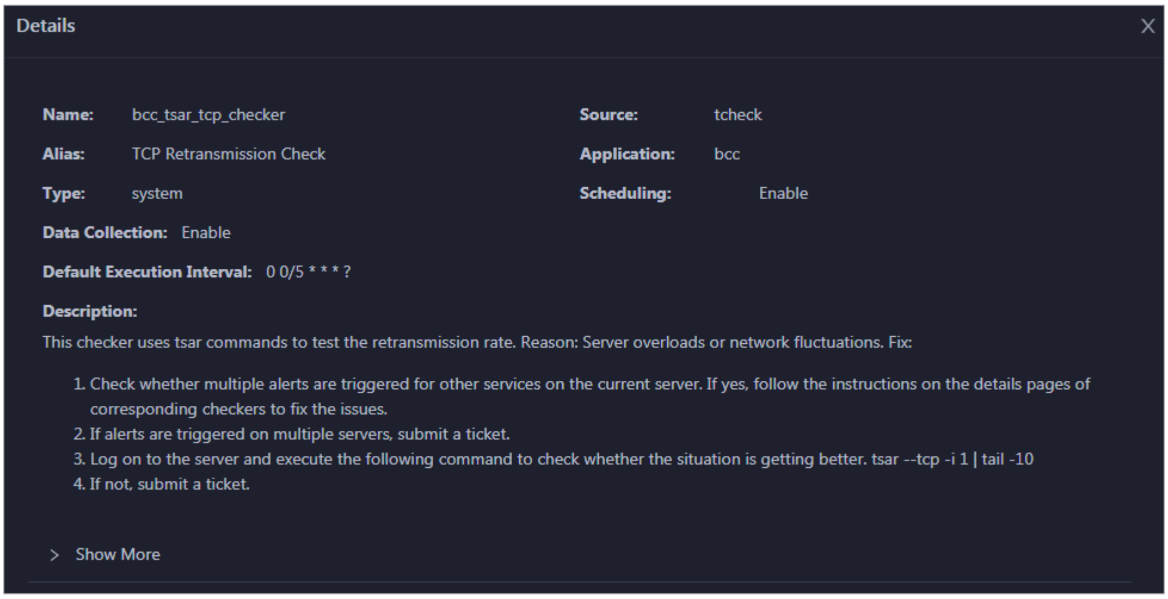


	Checker	Source	Critical	Warning	Exception	Actions
+	bcc_check_ntp	tcheck	0	10	0	Details
+	bcc_tsar_tcp_checker	tcheck	0	0	0	Details
+	bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
+	bcc_network_tcp_connections_checker	tcheck	0	0	0	Details
+	bcc_disk_usage_checker	tcheck	0	0	0	Details
+	bcc_host_live_check	tcheck	0	0	0	Details
+	bcc_process_thread_count_checker	tcheck	0	0	0	Details
+	bcc_check_load_high	tcheck	0	0	0	Details

On the **Health Status** tab, you can view all checkers for the cluster and the check results for the hosts in the cluster. The following alerts may be reported on a host: **CRITICAL**, **WARNING**, and **EXCEPTION**. The alerts are represented in different colors. You must handle the alerts in a timely manner, especially the **CRITICAL** and **WARNING** alerts.

View checker details

1. On the Health Status tab, click **Details** in the Actions column of a checker. On the Details page, view checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

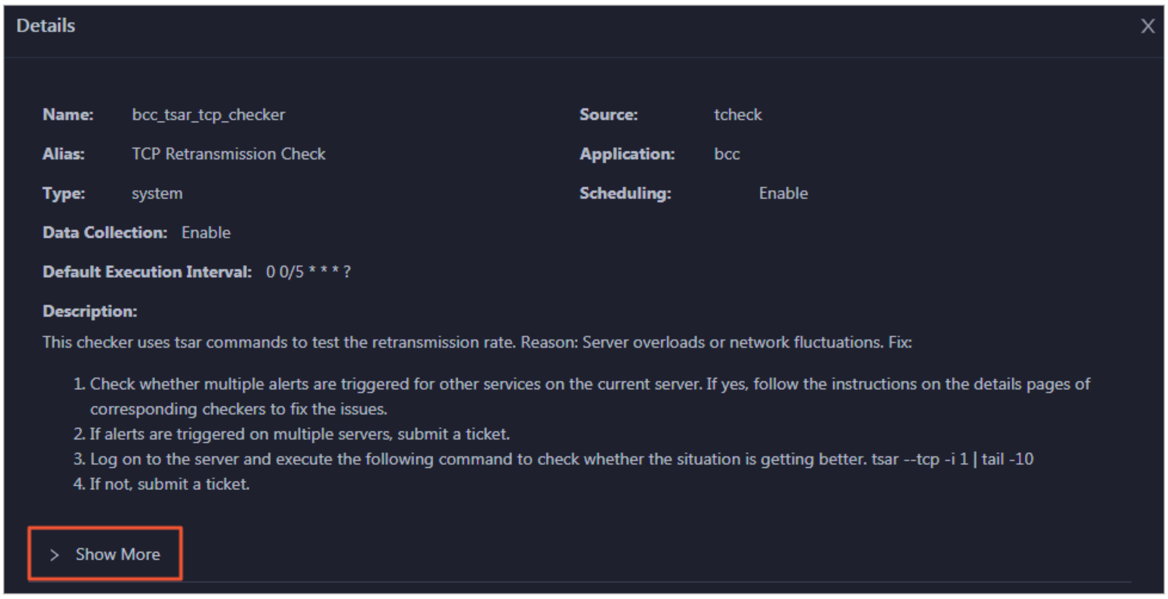
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include **Name**, **Source**, **Alias**, **Application**, **Type**, **Scheduling**, **Data Collection**, **Default Execution Interval**, and **Description**. The schemes to clear alerts are provided in the description.

2. Click **Show More** to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

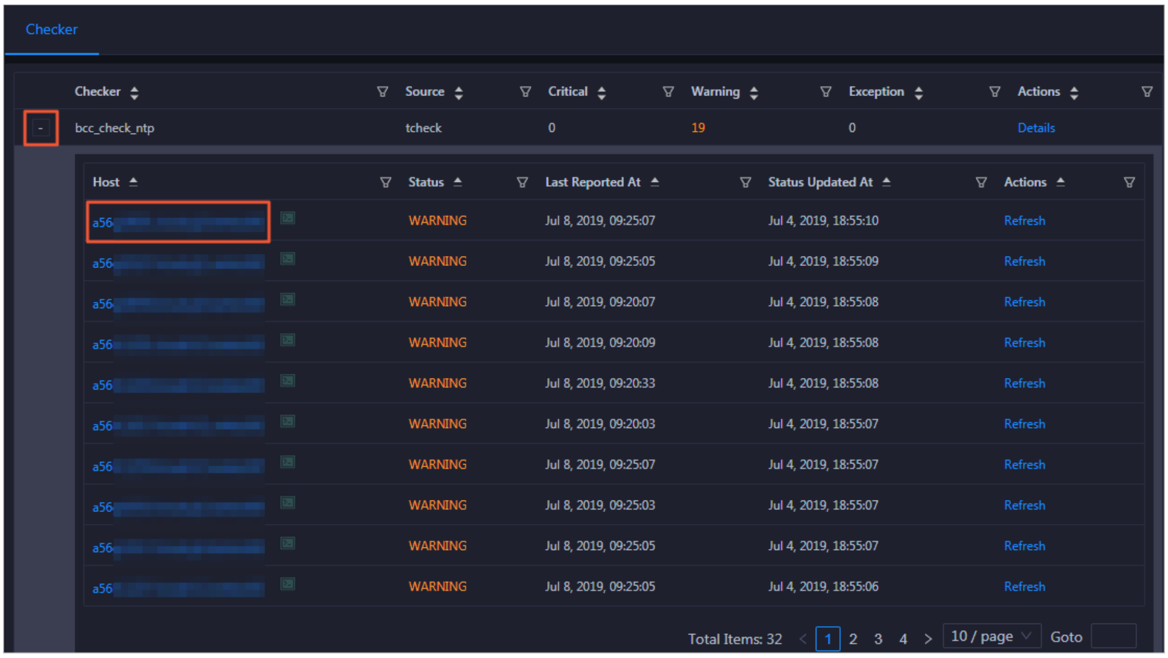
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about **Script**, **Target (TianJi)**, **Default Threshold**, and **Mount Point**.

View the hosts for which alerts are reported and causes for the alerts

You can view the check history and check results of a checker on a host.

1. On the Health Status tab, click **+** to expand a checker for which alerts are reported. You can view all hosts where the checker is run.



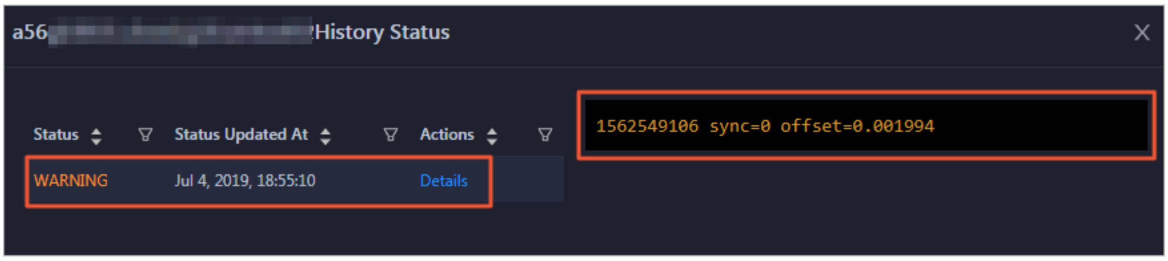
Checker

Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:06	Refresh

Total Items: 32 < 1 2 3 4 > 10 / page Goto

2. Click a hostname. In the panel that appears, click **Details** in the Actions column of a check result to view the cause of the alert.



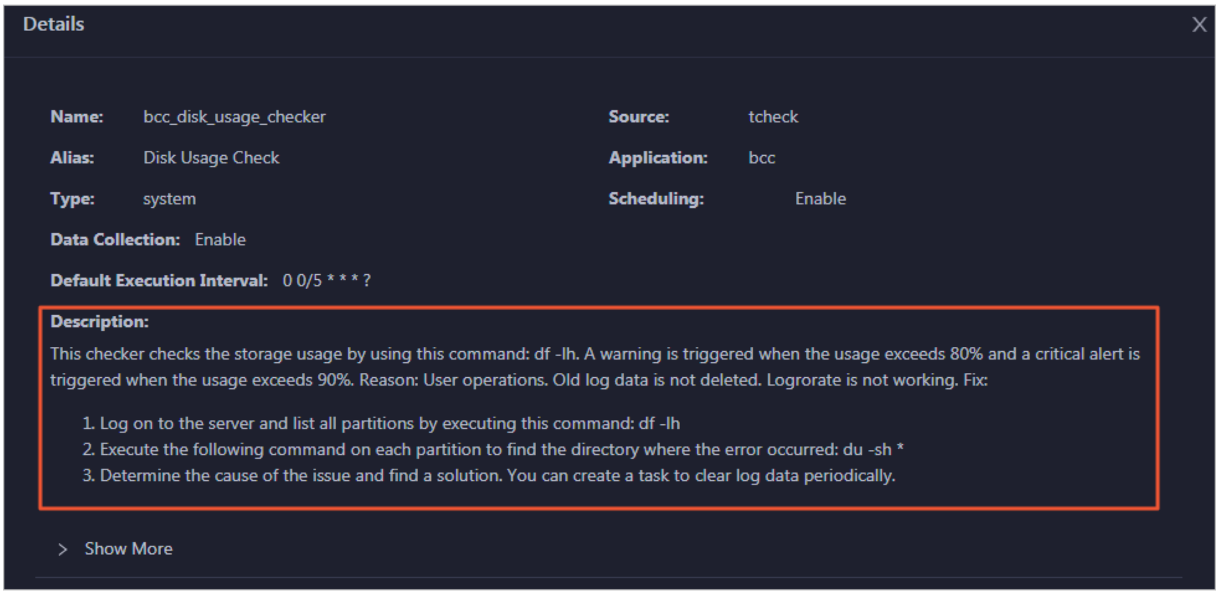
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status tab, click **Details** in the Actions column of a checker for which alerts are reported. On the Details page, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

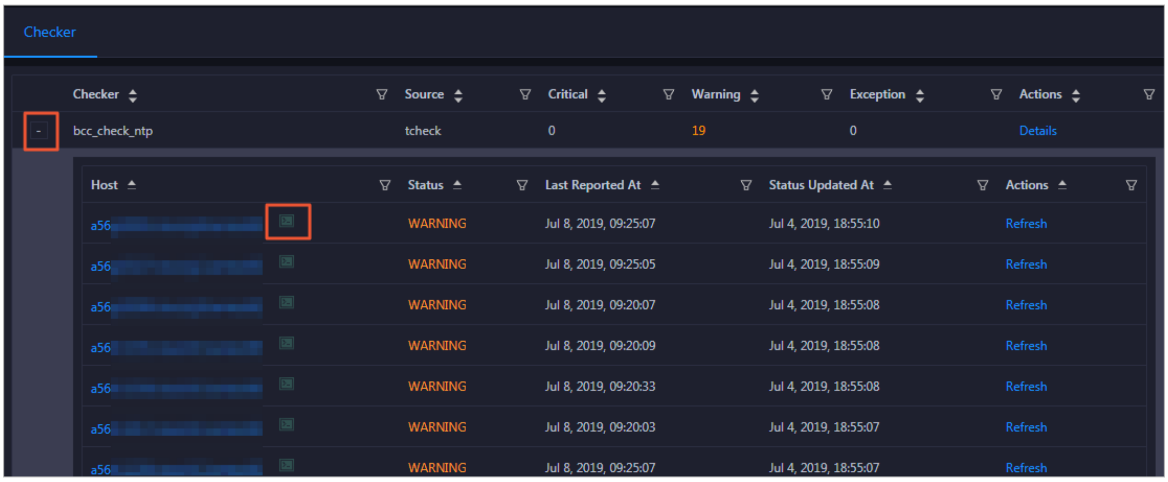
1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

> Show More

Log on to a host

You may need to log on to a host to handle alerts or other issues that occurred on the host.

1. On the Health Status tab, click **+** to expand a checker for which alerts are reported.

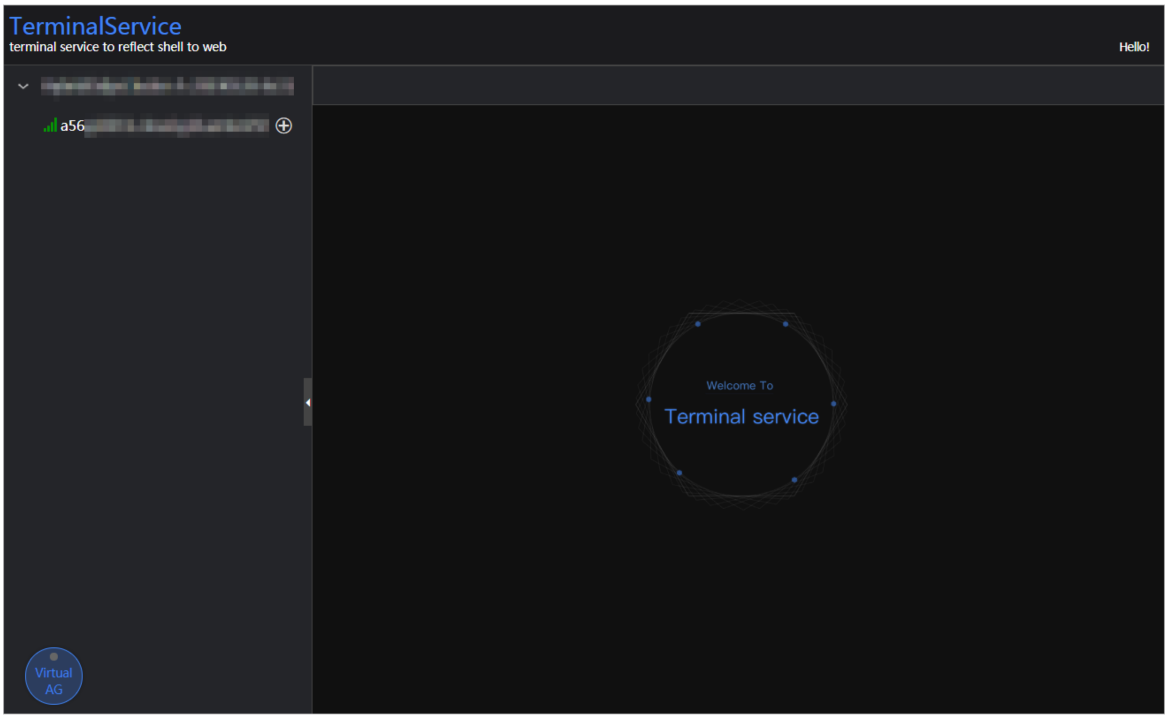


Checker

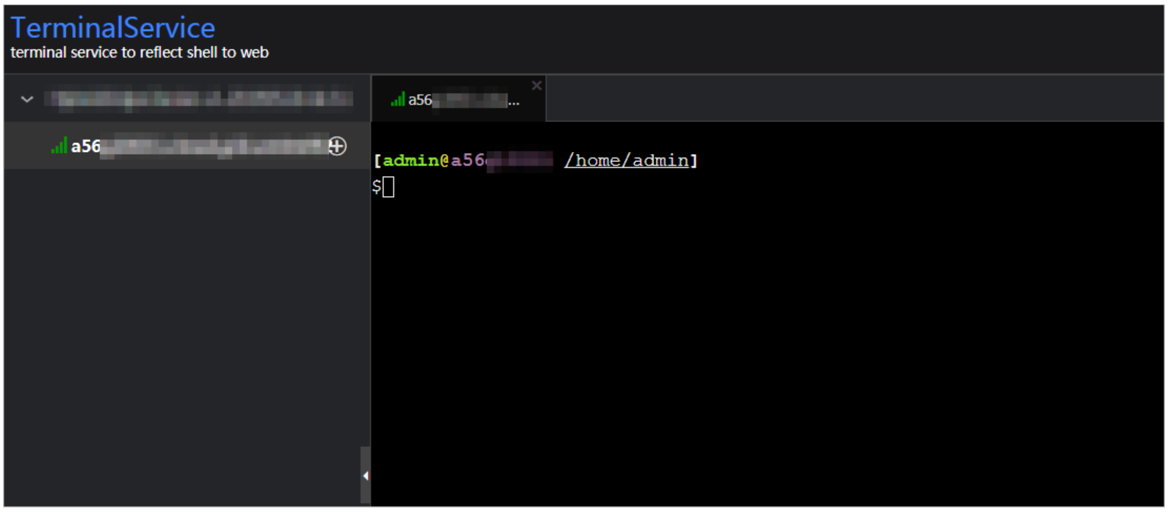
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host		Status	Last Reported At	Status Updated At	Actions
a56[redacted]		WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]		WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]		WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]		WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]		WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]		WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]		WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

2. Click the **Login in** icon of a host. The **TerminalService** page appears.



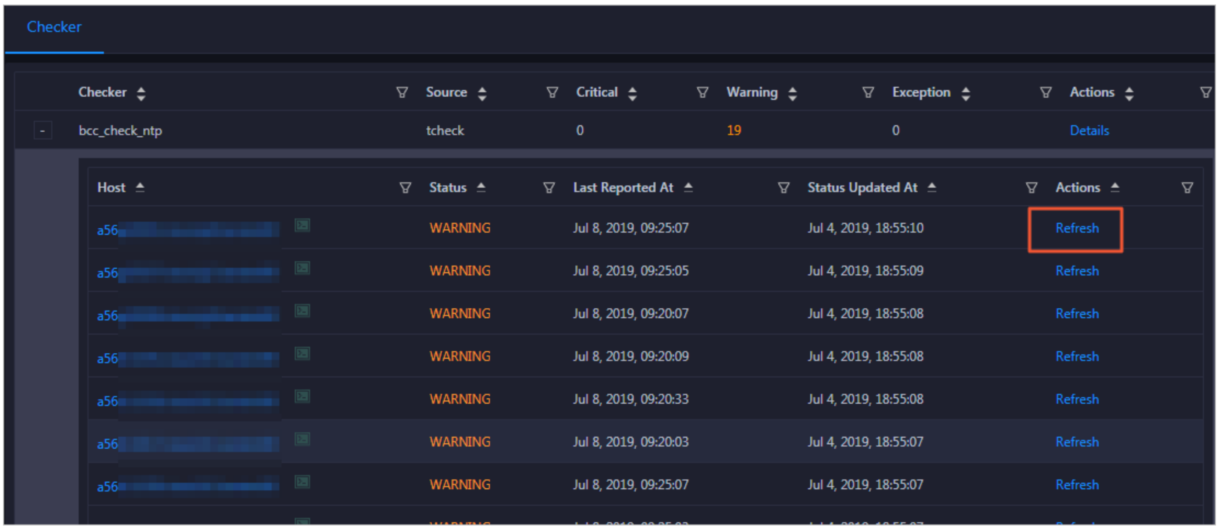
3. On the **TerminalService** page, click the hostname in the left-side navigation pane to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. This way, you can check whether the alert is cleared.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

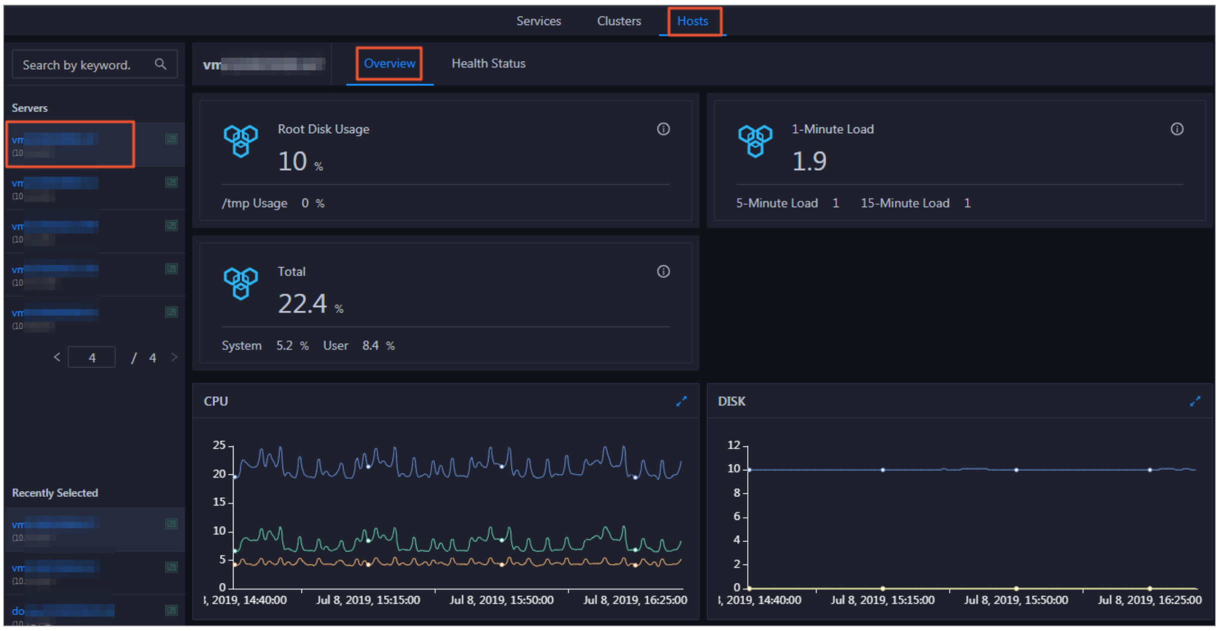
11.7.2.1.4. Host O&M

11.7.2.1.4.1. Host overview

The host overview page displays the overall running information about a host in an I+ cluster. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.

Entry

On the **Hosts** page, select a host in the left-side navigation pane. The **Overview** page for the host appears.



Root Disk Usage 10 %
/tmp Usage 0 %

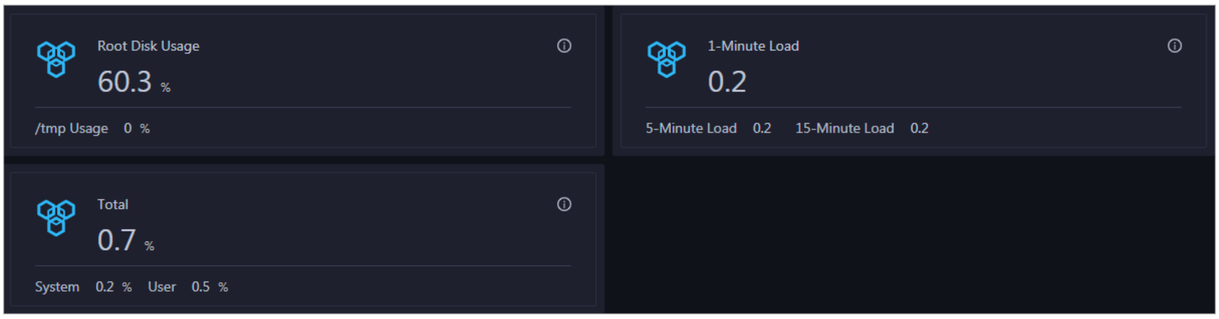
1-Minute Load 1.9
5-Minute Load 1 15-Minute Load 1

Total 22.4 %
System 5.2 % User 8.4 %

On the **Overview** page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.

Root Disk Usage, Total, and 1-Minute Load

These sections display the root disk usage, total usage, and 1-minute load for the selected host. The Root Disk Usage section provides the usage of the */tmp* directory. The Total section provides the system usage and user usage. The 1-Minute Load section provides the 1-minute, 5-minute, and 15-minute load averages.



Root Disk Usage 60.3 %
/tmp Usage 0 %

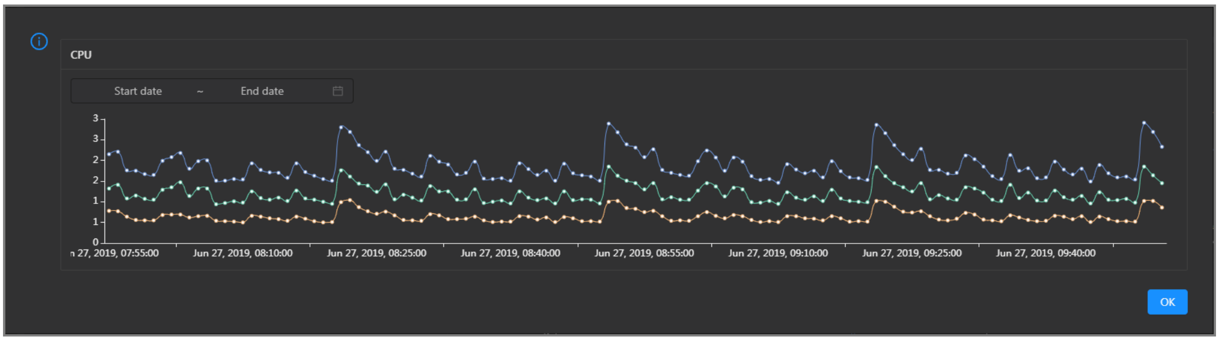
1-Minute Load 0.2
5-Minute Load 0.2 15-Minute Load 0.2

Total 0.7 %
System 0.2 % User 0.5 %

CPU

The CPU chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) of the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

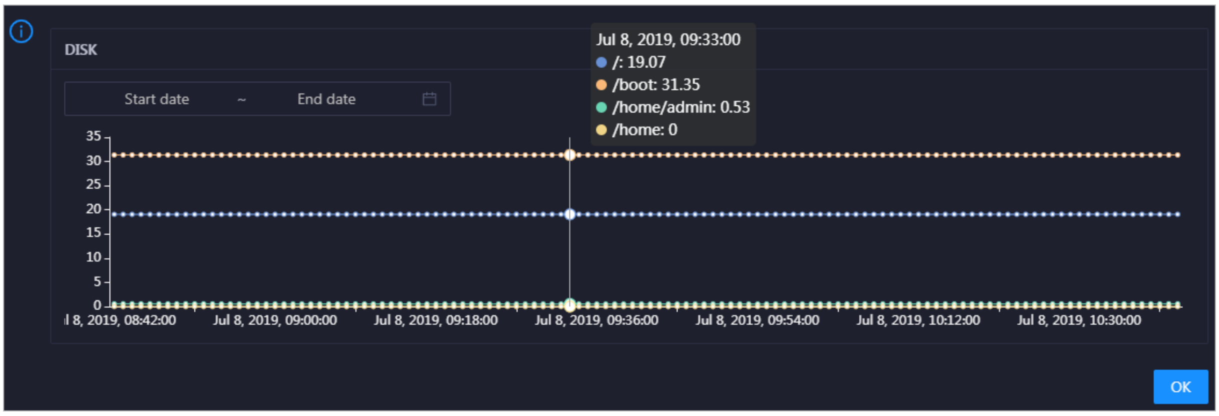


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the host in the specified period.

DISK

The DISK chart shows the trend lines of the storage usage in the */*, */boot*, */home/admin*, and */home* directories for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

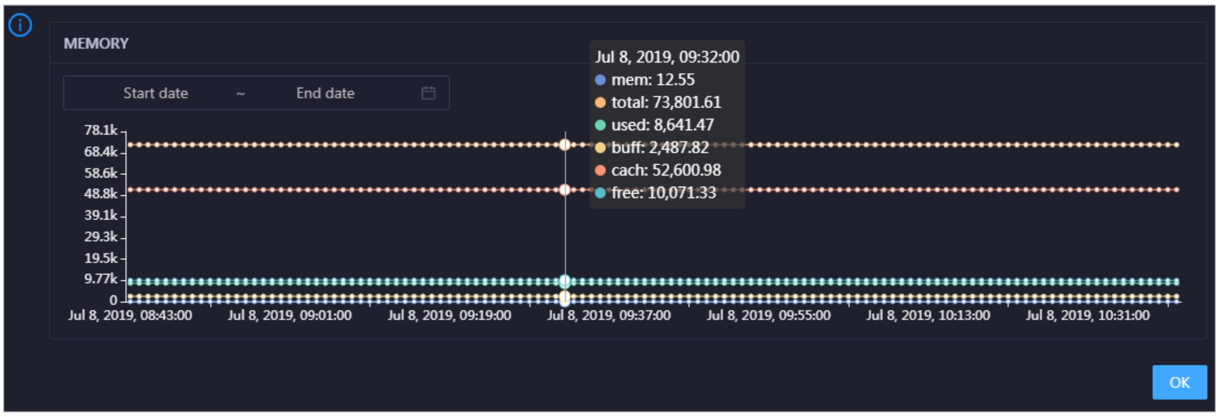


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the host in the specified period.

MEMORY

The MEMORY chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

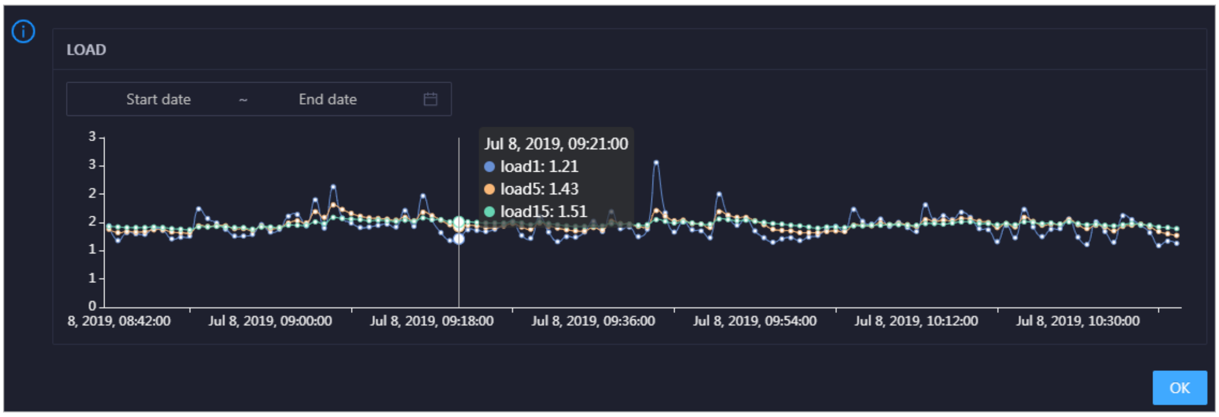


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the host in the specified period.

LOAD

The LOAD chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

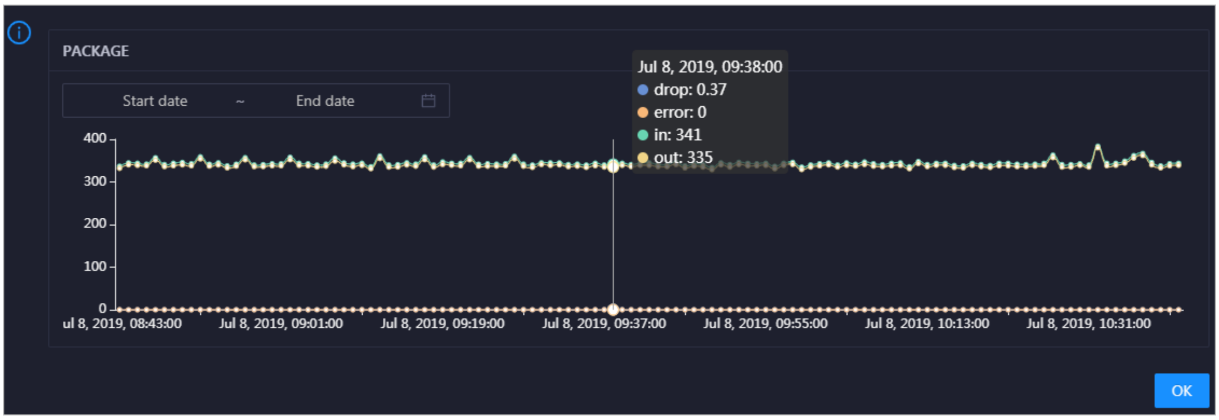


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the host in the specified period.

PACKAGE

The PACKAGE chart shows the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the host over time in different colors. These trend lines reflect the data transmission status of the host.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

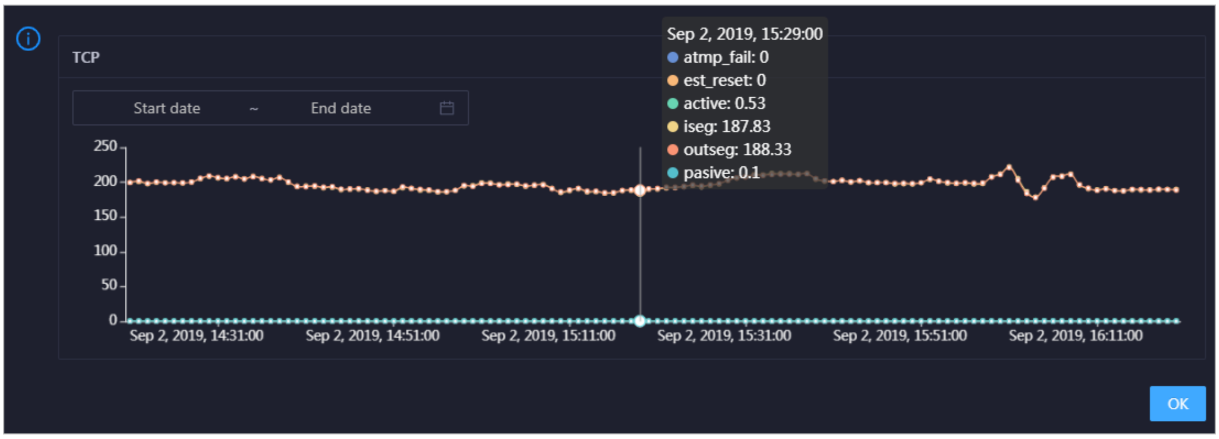


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the host in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the host over time in different colors. These trend lines reflect the TCP connection status of the host.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

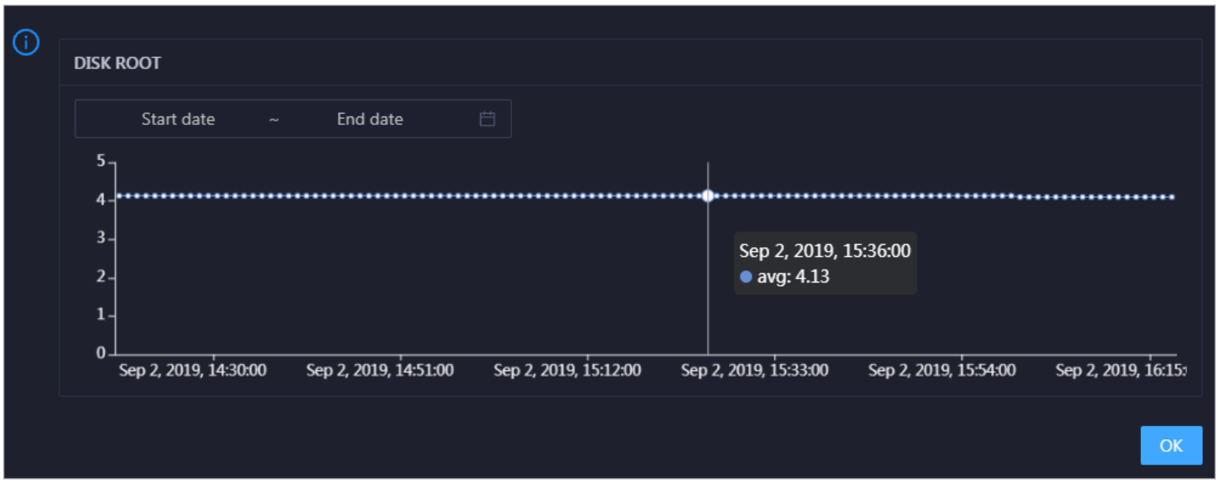


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the host in the specified period.

DISK ROOT

This chart displays the trend line of the average usage of the root disk (/) for the host over time.

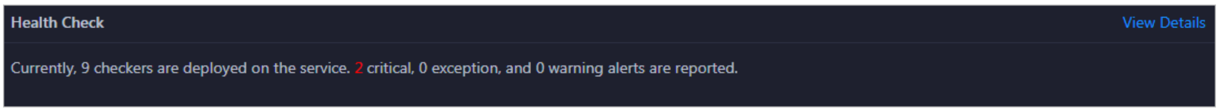
Click ⤢ in the upper-right corner of the chart to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the host in the specified period.

Health Check

This section displays the number of checkers deployed for the host and the respective number of Critical, Warning, and Exception alerts.



Health Check

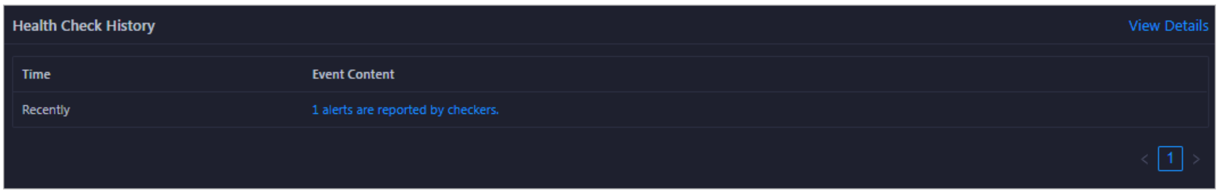
View Details

Currently, 9 checkers are deployed on the service. 2 critical, 0 exception, and 0 warning alerts are reported.

Click **View Details** to go to the Host health page. On this page, you can view the health check details.

Health Check History

This section displays a record of the health checks performed on the host.



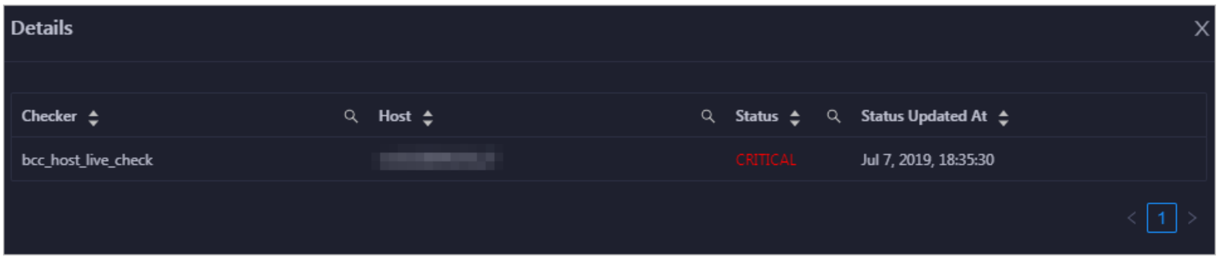
Health Check History

View Details

Time	Event Content
Recently	1 alerts are reported by checkers.

Click **View Details** to go to the Host health page. On this page, you can view the health check details.

You can click the event content of a check to view the exception items.



Details

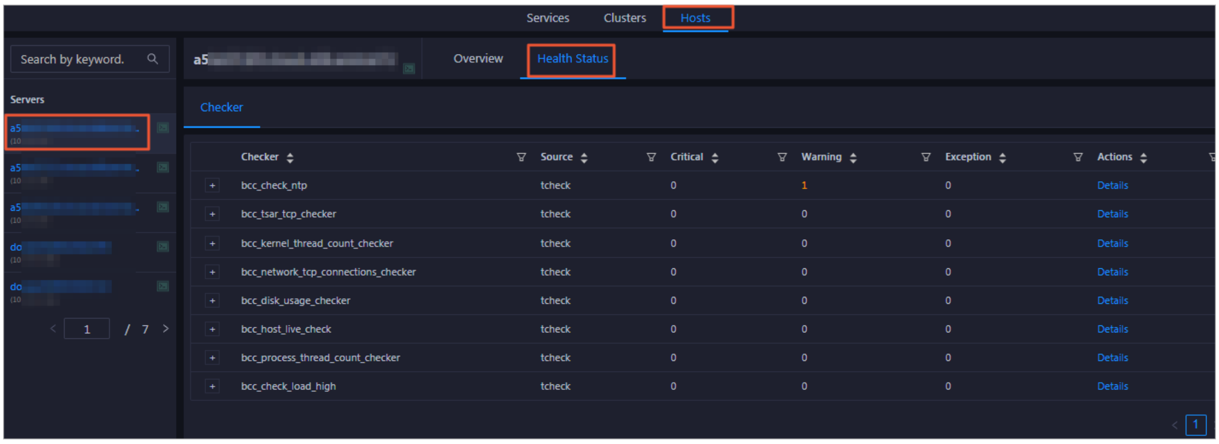
Checker	Host	Status	Status Updated At
bcc_host_live_check	[redacted]	CRITICAL	Jul 7, 2019, 18:35:30

11.7.2.1.4.2. Host health

On the Health Status page, you can view the checkers of the selected host, including the checker details, check results, and schemes to clear alerts (if any). In addition, you can log on to the host and perform manual checks on the host.

Entry

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Health Status** tab. The **Health Status** page for the host appears.

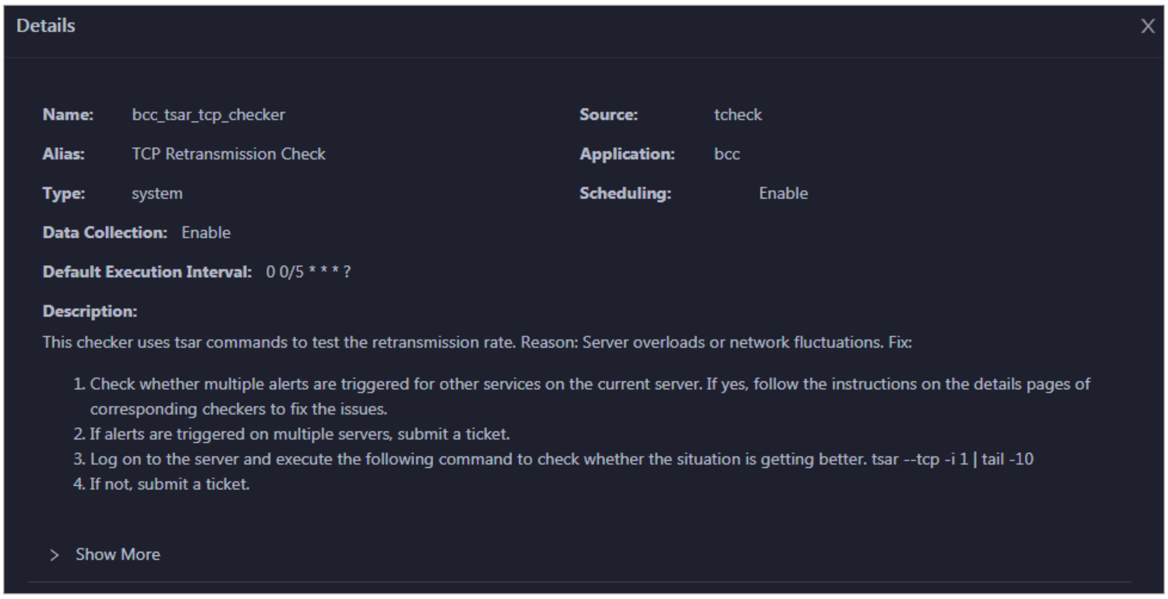


Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	1	0	Details
bcc_tsar_tcp_checker	tcheck	0	0	0	Details
bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
bcc_network_tcp_connections_checker	tcheck	0	0	0	Details
bcc_disk_usage_checker	tcheck	0	0	0	Details
bcc_host_live_check	tcheck	0	0	0	Details
bcc_process_thread_count_checker	tcheck	0	0	0	Details
bcc_check_load_high	tcheck	0	0	0	Details

On the **Health Status** page, you can view all checkers and the check results for the host. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

View checker details

1. On the Health Status page, click **Details** in the Actions column of a checker. In the dialog box that appears, view the checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

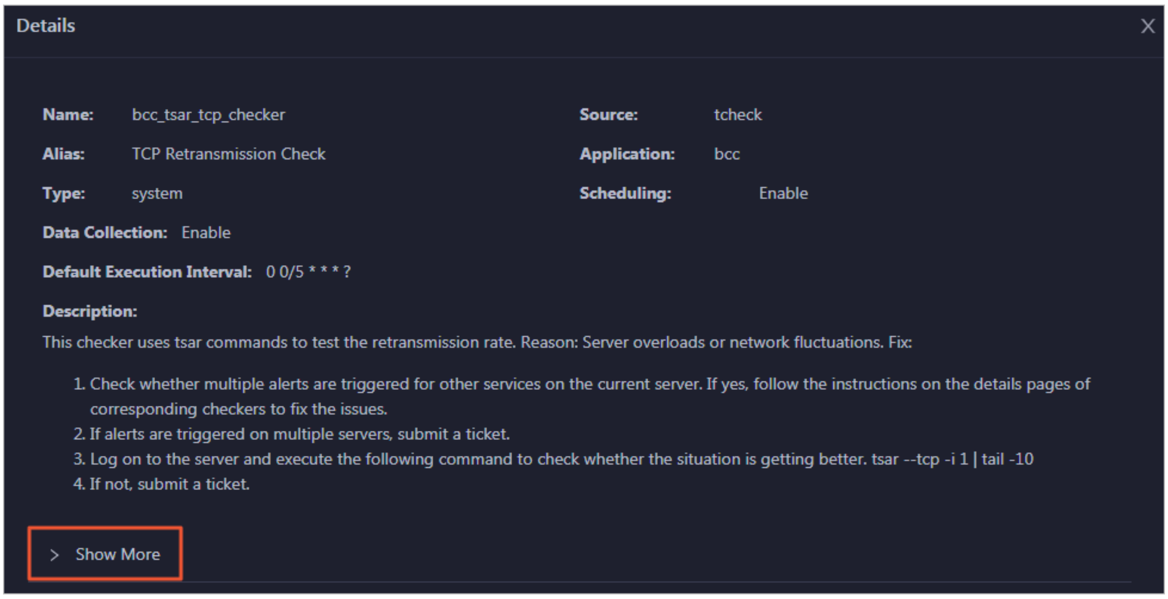
This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

> Show More

The checker details include the name, source, alias, application, type, default execution interval, and description of the checker, whether scheduling is enabled, and whether data collection is enabled. The schemes to clear alerts are provided in the description.

2. Click **Show More** at the bottom to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Alias: TCP Retransmission Check

Type: system

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Source: tcheck

Application: bcc

Scheduling: Enable

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

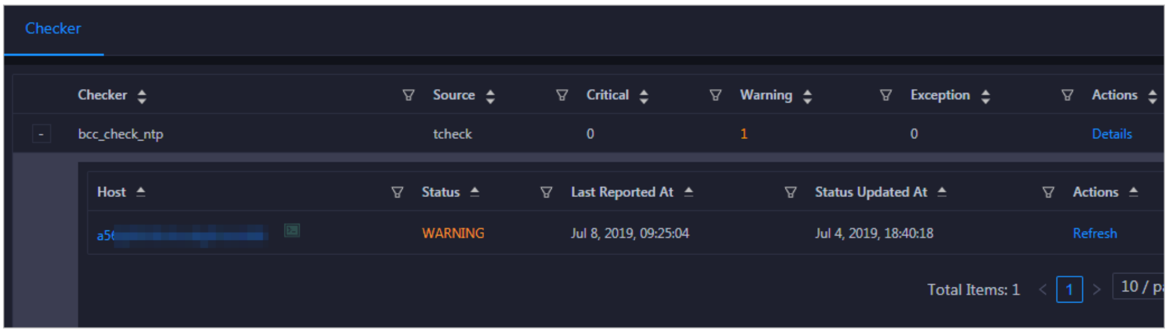
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about the execution script, execution target, default threshold, and mount point for data collection.

View alert causes

You can view the check history and check results of a checker.

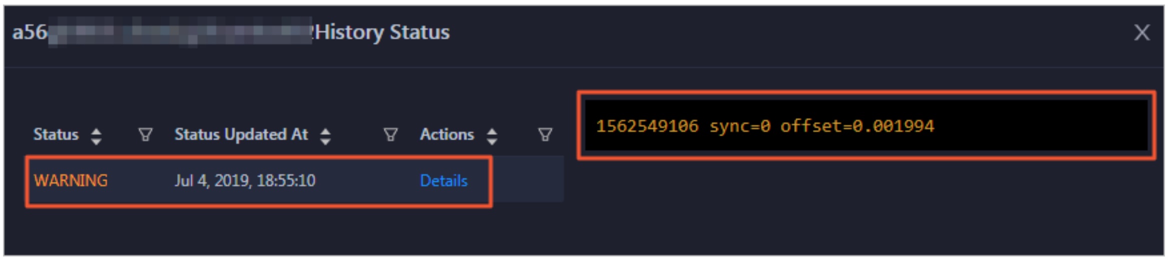
1. On the Health Status page, click **+** to expand a checker with alerts.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

2. Click the hostname. In the dialog box that appears, click **Details** in the Actions column of a check result to view the alert causes.



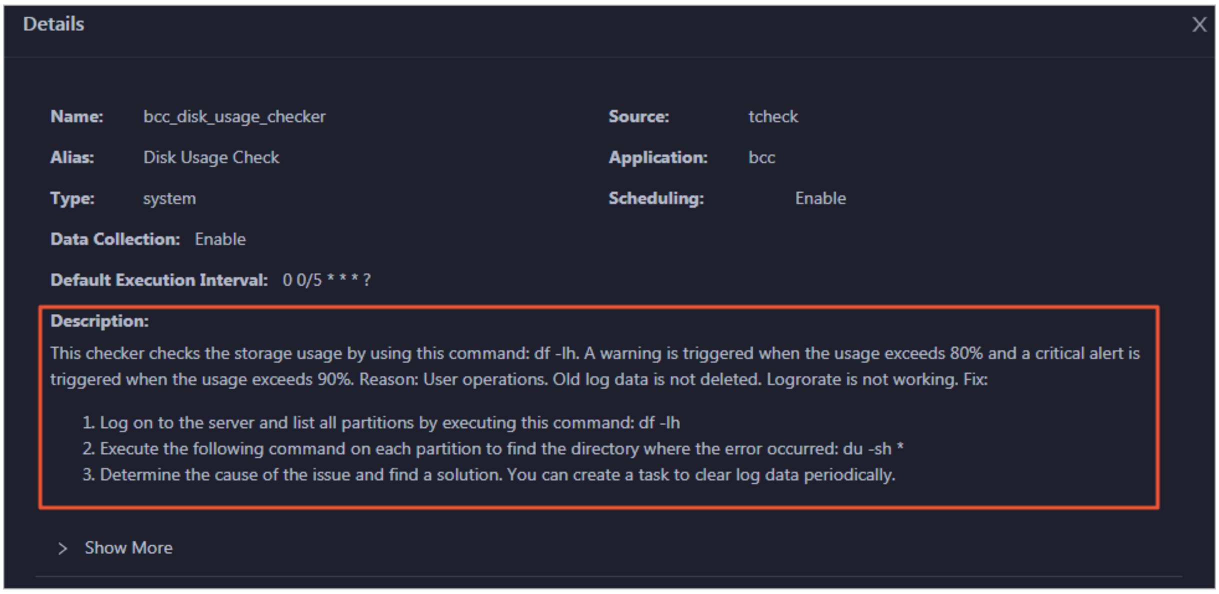
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status page, click **Details** in the Actions column of a checker with alerts. In the dialog box that appears, view the schemes to clear alerts.



Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

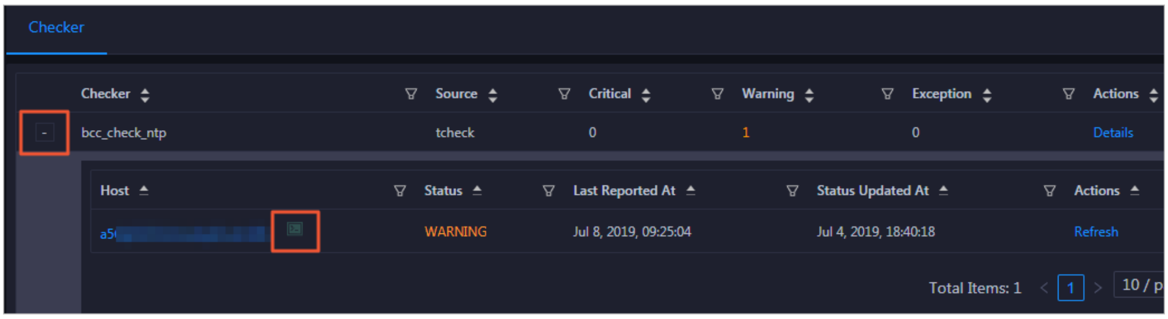
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

To log on to a host to clear alerts or perform other operations, follow these steps:

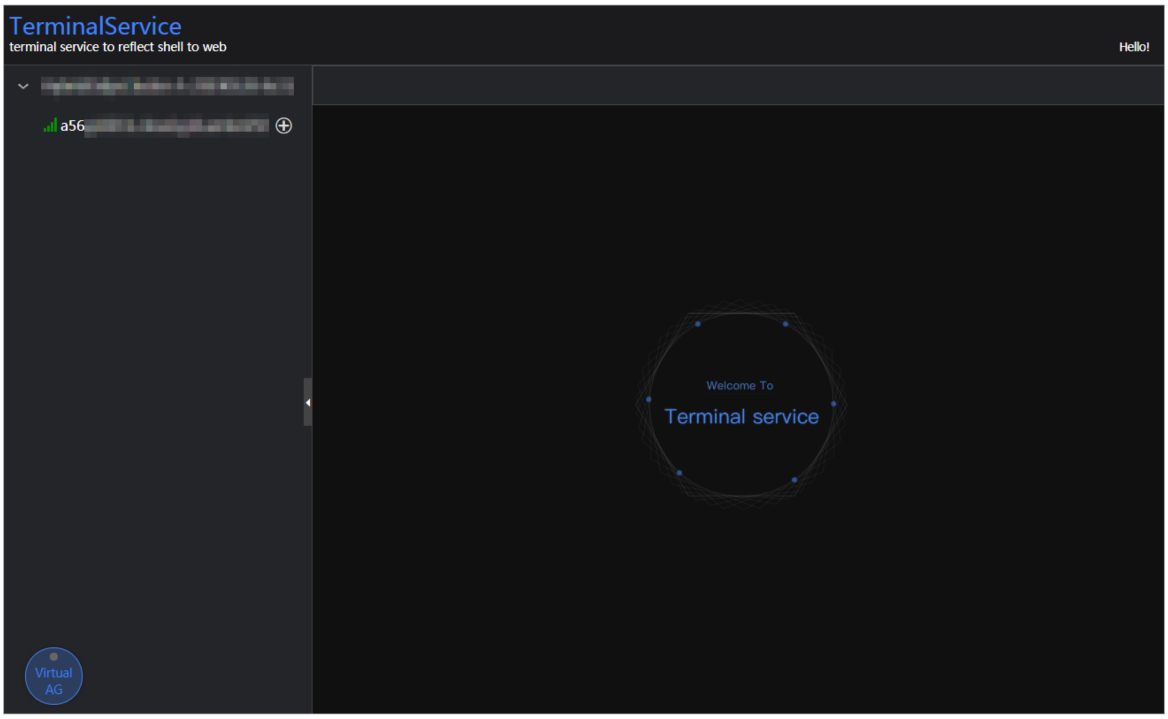
1. On the Health Status page, click **+** to expand a checker with alerts.



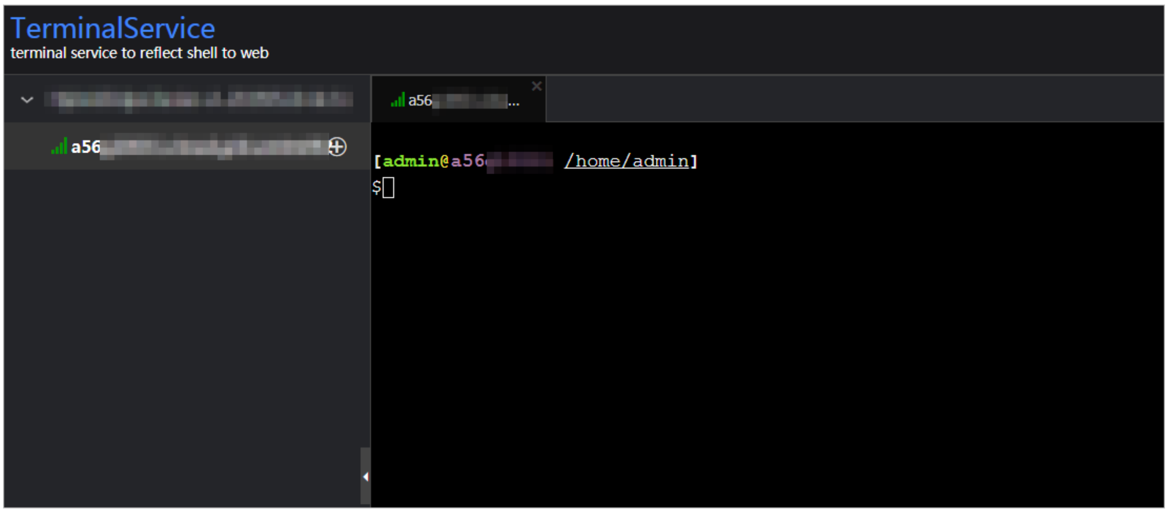
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

2. Click the **Log On** icon of a host. The **TerminalService** page appears.



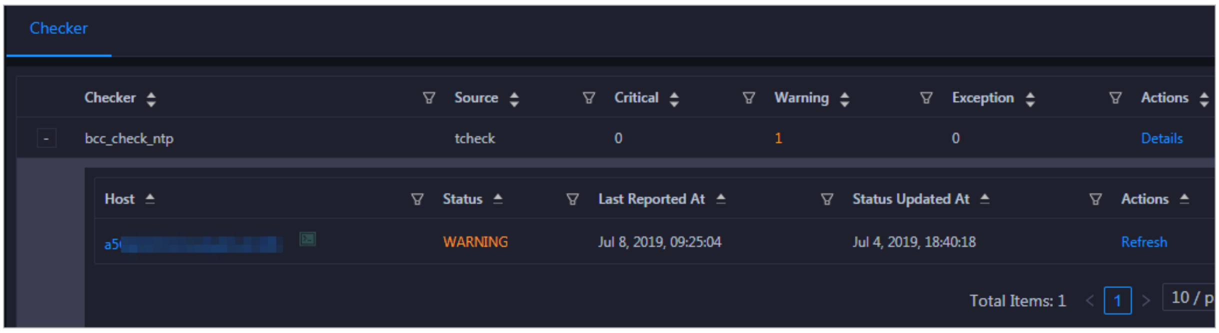
3. On the **TerminalService** page, click the hostname on the left to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. In this way, you can check whether the alert is cleared.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

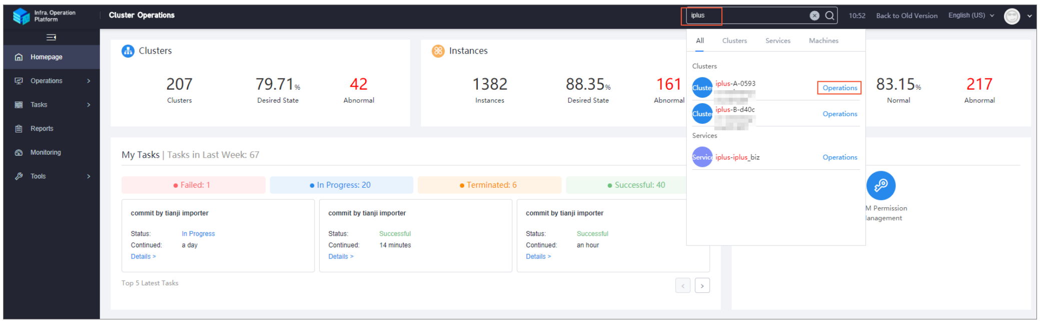
Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

11.7.2.2. O&M on Apsara Infrastructure Management Framework

1. Log on to Apsara Infrastructure Management Framework.
2. Enter *iplus* in the search box to search for the iplus cluster, as shown in Search for the iplus cluster.

   Search for the iplus cluster



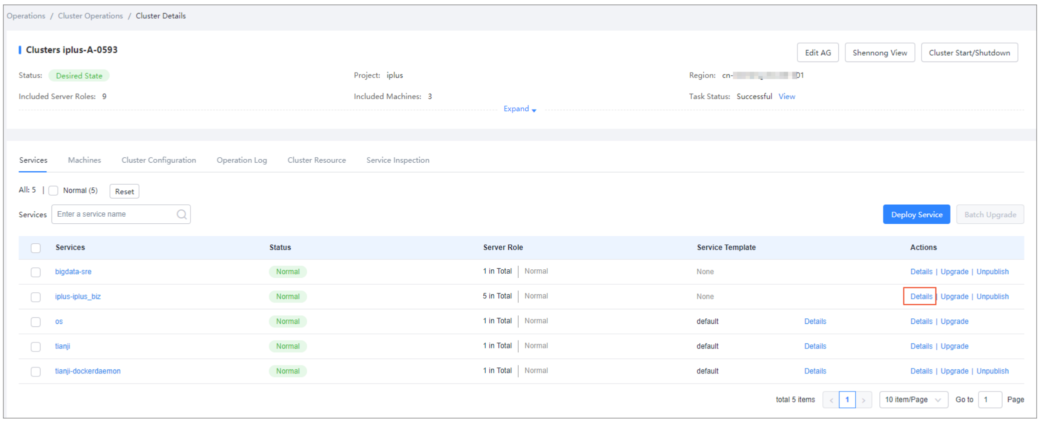
commit by tianji importer
Status: In Progress
Continued: a day
Details >

commit by tianji importer
Status: Successful
Continued: 14 minutes
Details >

commit by tianji importer
Status: Successful
Continued: an hour
Details >

3. Click **O&M** on the right of the cluster name to redirect to the **Cluster Details** page, as shown in Cluster Details page.

   Cluster Details page



Clusters iplus-A-0593

Status: Desired State
Project: iplus
Region: cn-[redacted]01
Included Server Roles: 9
Included Machines: 3
Task Status: Successful View

All: 5 | □ Normal (5)

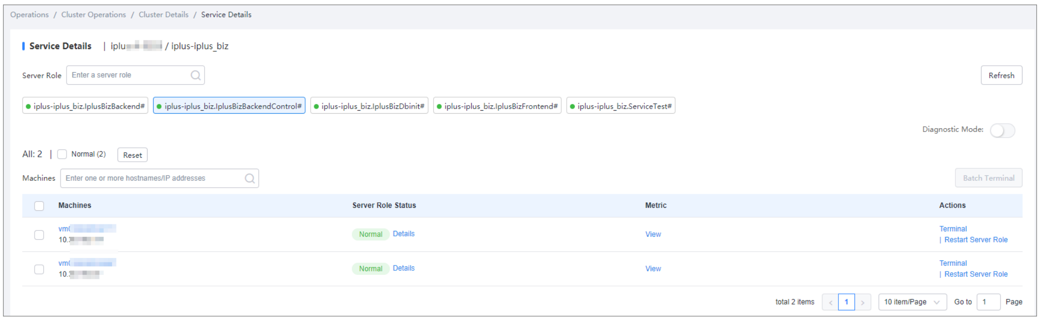
Services: Enter a service name

□	Services	Status	Server Role		Service Template		Actions
□	bigdata-sre	Normal	1 in Total	Normal	None		Details | Upgrade | Unpublish
□	iplus-iplus_biz	Normal	5 in Total	Normal	None		Details | Upgrade | Unpublish
□	os	Normal	1 in Total	Normal	default	Details	Details | Upgrade
□	tianji	Normal	1 in Total	Normal	default	Details	Details | Upgrade
□	tianji-dockerdaemon	Normal	1 in Total	Normal	default	Details	Details | Upgrade | Unpublish

total 5 items < 1 > 10 item/Page Go to 1 Page

4. On the **Services** tab, find the **iplus-iplus_biz** service and click **Details** in the Actions column to view the details, as shown in Service Details page.

   Service Details page


Operations / Cluster Operations / Cluster Details / Service Details
Refresh
Diagnostic Mode:
Reset
Batch Terminal

Service Details | iplu[redacted] / iplus-iplus_biz

Server Role: Enter a server role

● iplus-iplus_biz.IplusBizBackend# ● iplus-iplus_biz.IplusBizBackendControl# ● iplus-iplus_biz.IplusBizDbinit# ● iplus-iplus_biz.IplusBizFrontend# ● iplus-iplus_biz.ServiceTest#

All: 2 | □ Normal (2)

Machines: Enter one or more hostnames/IP addresses

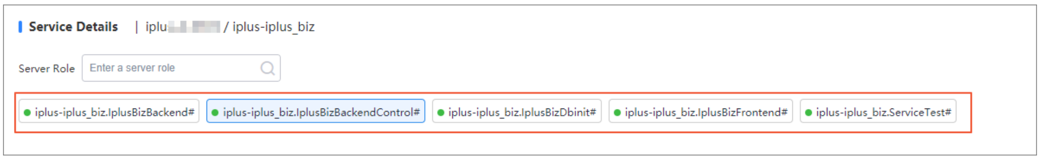
□	Machines	Server Role Status	Metric	Actions
□	vm[redacted] 10.[redacted]	Normal Details	View	Terminal | Restart Server Role
□	vm[redacted] 10.[redacted]	Normal Details	View	Terminal | Restart Server Role

total 2 items < 1 > 10 item/Page Go to 1 Page

You can restart any role in the server role list, as shown in Server role list. Typically, you only need to restart the **IplusBizBackendControl#** and **IplusBizBackend#** roles.

> Notice
>
> You must restart the **IplusBizBackendControl#** and **IplusBizBackend#** roles in the following sequence:
>
> - Restart **IplusBizBackendControl#** first, and then **IplusBizBackend#**.
> - You must follow this sequence to restart the two roles within 10 minutes.
>
> Other roles can be restarted without strict sequence.

Server role list



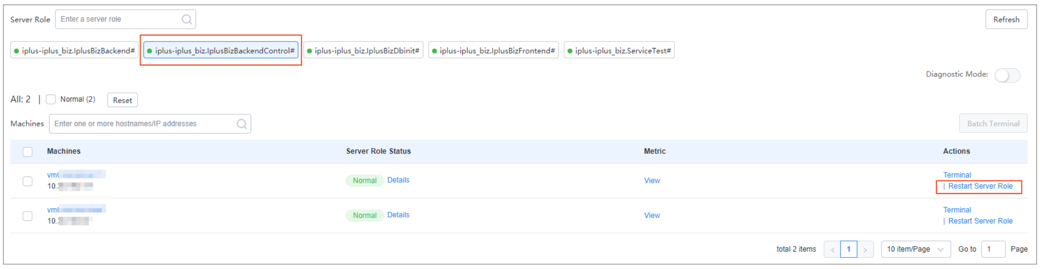
Service Details | iplu[redacted] / iplus-iplus_biz

Server Role: Enter a server role

● iplus-iplus_biz.IplusBizBackend# | ● iplus-iplus_biz.IplusBizBackendControl# | ● iplus-iplus_biz.IplusBizDbinit# | ● iplus-iplus_biz.IplusBizFrontend# | ● iplus-iplus_biz.ServiceTest#

5. Click the role you want to restart. In the Machines list, click **Restart** in the **Actions** column of all machines listed for this role, as shown in Restart a server role.

Restart a server role



Server Role: Enter a server role

● iplus-iplus_biz.IplusBizBackend# | ● iplus-iplus_biz.IplusBizBackendControl# | ● iplus-iplus_biz.IplusBizDbinit# | ● iplus-iplus_biz.IplusBizFrontend# | ● iplus-iplus_biz.ServiceTest#

Diagnostic Mode: ○

All: 2 | □ Normal (2) Reset

Machines: Enter one or more hostnames/IP addresses

□	Machines	Server Role Status	Metric	Actions
□	vm[redacted] 10.[redacted]	Normal Details	View	Terminal | Restart Server Role
□	vm[redacted] 10.[redacted]	Normal Details	View	Terminal | Restart Server Role

total 2 items < 1 > 10 item/Page Go to 1 Page

11.7.2.3. Operations and maintenance based on the Graph Analytics container

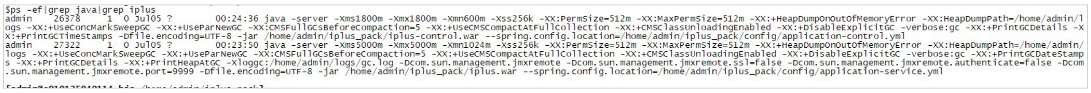
11.7.2.3.1. View instances

By viewing and examining instances, you can know the running status of instances and fix the problematic instances, for example, perform a switchover or clear logs.

View Java running instances

Log on to the Graph Analytics container, and run the `ps -ef|grep java|grep iplus` command. If the progress shown in View Java running instances exists, Administration Console is in the normal status.

View Java running instances



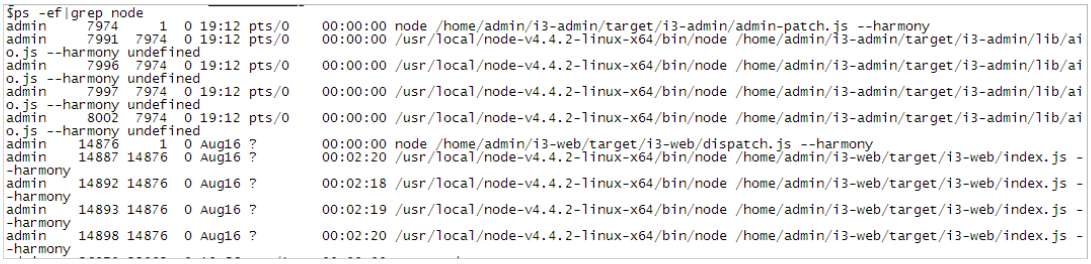
```
$ps -ef|grep java|grep iplus
admin    26378     1  0 Jul05 ?        00:24:36 java -server -Xms1800m -Xmx1800m -Xmn600m -Xss256k -XX:PermSize=512m -XX:MaxPermSize=512m -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/home/admin/l
ogs -XX:+UseConcMarkSweepGC -XX:+UseParNewGC -XX:CMSFullGCsBeforeCompaction=5 -XX:+UseCMSCompactAtFullCollection -XX:+CMSClassUnloadingEnabled -XX:+DisableExplicitGC -verbose:gc -XX:+PrintGCDetails -X
X:+PrintGCTimeStamps -Dfile.encoding=UTF-8 -jar /home/admin/iplus_pack/iplus-control.war --spring.config.location=/home/admin/iplus_pack/config/application-control.yml
admin    27322     1  0 Jul05 ?        00:23:50 java -server -Xms5000m -Xmx5000m -Xmn1024m -Xss256k -XX:PermSize=512m -XX:MaxPermSize=512m -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/home/admin/
logs -XX:+UseConcMarkSweepGC -XX:+UseParNewGC -XX:CMSFullGCsBeforeCompaction=5 -XX:+UseCMSCompactAtFullCollection -XX:+CMSClassUnloadingEnabled -XX:+DisableExplicitGC -verbose:gc -XX:+PrintGCDateStamp
s -XX:+PrintGCDetails -XX:+PrintHeapAtGC -Xloggc:/home/admin/logs/gc.log -Dcom.sun.management.jmxremote -Dcom.sun.management.jmxremote.ssl=false -Dcom.sun.management.jmxremote.authenticate=false -Dcom
.sun.management.jmxremote.port=9999 -Dfile.encoding=UTF-8 -jar /home/admin/iplus_pack/iplus.war --spring.config.location=/home/admin/iplus_pack/config/application-service.yml
```

View node instances

Log on to the Graph Analytics application server, and run the `ps –ef|grep node` command. If the process shown in View node instances exists, the node service of Graph Analytics is normal.

View node instances

View node instances



```
$ps -ef|grep node
admin     7974     1  0 19:12 pts/0    00:00:00 node /home/admin/i3-admin/target/i3-admin/admin-patch.js --harmony
admin     7991  7974  0 19:12 pts/0    00:00:00 /usr/local/node-v4.4.2-linux-x64/bin/node /home/admin/i3-admin/target/i3-admin/lib/ai
o.js --harmony undefined
admin     7996  7974  0 19:12 pts/0    00:00:00 /usr/local/node-v4.4.2-linux-x64/bin/node /home/admin/i3-admin/target/i3-admin/lib/ai
o.js --harmony undefined
admin     7997  7974  0 19:12 pts/0    00:00:00 /usr/local/node-v4.4.2-linux-x64/bin/node /home/admin/i3-admin/target/i3-admin/lib/ai
o.js --harmony undefined
admin     8002  7974  0 19:12 pts/0    00:00:00 /usr/local/node-v4.4.2-linux-x64/bin/node /home/admin/i3-admin/target/i3-admin/lib/ai
o.js --harmony undefined
admin    14876     1  0 Aug16 ?        00:00:00 node /home/admin/i3-web/target/i3-web/dispatch.js --harmony
admin    14887 14876  0 Aug16 ?        00:02:20 /usr/local/node-v4.4.2-linux-x64/bin/node /home/admin/i3-web/target/i3-web/index.js -
-harmony
admin    14892 14876  0 Aug16 ?        00:02:18 /usr/local/node-v4.4.2-linux-x64/bin/node /home/admin/i3-web/target/i3-web/index.js -
-harmony
admin    14893 14876  0 Aug16 ?        00:02:19 /usr/local/node-v4.4.2-linux-x64/bin/node /home/admin/i3-web/target/i3-web/index.js -
-harmony
admin    14898 14876  0 Aug16 ?        00:02:20 /usr/local/node-v4.4.2-linux-x64/bin/node /home/admin/i3-web/target/i3-web/index.js -
-harmony
```

In the preceding information, i3-web indicates that Analytics Workbench is in a normal status, and i3-admin indicates that Administration Console is in a normal status. If Administration Console is not released, the i3-admin process may not exist.

11.7.2.3.2. Log files

Graph Analytics application log:

The log files of Graph Analytics are stored in the `/home/admin/logs` directory.

A 100-GB data disk is mounted to the `/home/admin/logs` directory. Log files will increase with the execution time, which requires automatic cleanup. Two cleanup policies are available:

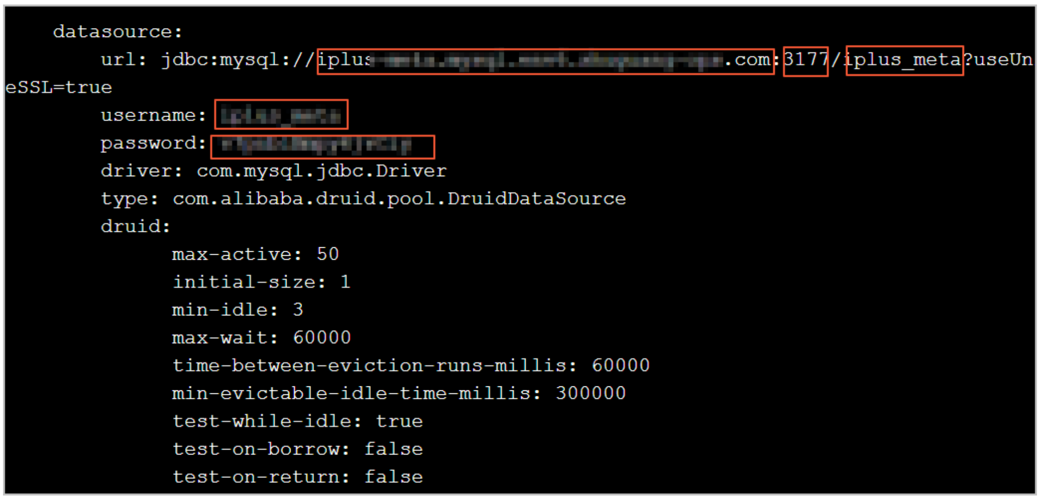
- Policy one: Time-based cleanup. The disk automatically deletes the log files that were created two weeks ago.
- Policy two: Cleanup based on the log size in the directory. If the log files occupy more than 80% of the total data disk space, the disk automatically deletes the earliest log files.

11.7.2.3.3. Database logs

Database logs record the execution information of i3-related programs, mainly the SQL statements. This information includes the execution time, whether the statements have been executed successfully, and whether an exception has occurred.

1. Log on to the Graph Analytics container.
2. Run the **cat** */home/admin/iplus_pack/config/application-service.yml* command to view the database information in *application-service.yml*.

   View database information



```
    datasource:
        url: jdbc:mysql://iplus[redacted].com:3177/iplus_meta?useUn
eSSL=true
        username: [redacted]
        password: [redacted]
        driver: com.mysql.jdbc.Driver
        type: com.alibaba.druid.pool.DruidDataSource
        druid:
              max-active: 50
              initial-size: 1
              min-idle: 3
              max-wait: 60000
              time-between-eviction-runs-millis: 60000
              min-evictable-idle-time-millis: 300000
              test-while-idle: true
              test-on-borrow: false
              test-on-return: false
```

3. Run the **mysql -h${db_host} -P${db_port} -u${db_user} -p${db_password} -D${db_name}**

command to log on to the database.

4. Query the latest SQL statement executed by Graph Analytics and the time track.

```
SELECT * from i3eye_time_trace WHERE main_time_trace_id in (
SELECT max(main_time_trace_id) from i3eye_time_trace);
```

5. View the SQL statements executed within the last hour.

```
select * from i3eye_time_trace where name like 'com.alibaba.iplus.common.dal.manual%' and (gmt_cr
eate < now() and gmt_create > date_sub(now(), interval 1 hour) );
```

6. View the SQL statements that have errors within the last hour.

```
select * from i3eye_time_trace where complete = 0 and name like 'com.alibaba.iplus.common.dal.manu
al%' and (gmt_create < now() and gmt_create > date_sub(now(), interval 1 hour) );
```

11.7.2.3.4. Stop the service

Use admin Log on to the Graph Analytics container, run the start script, and run the following ps commands to view processes:

- View Java process: `ps –ef|grep java`
- View node process: `ps –ef|grep node`

You can stop a service by killing the corresponding thread.

11.7.2.3.5. Restart the service

Use admin Log on to the Graph Analytics container and run the startup script:

- Directly start iplus, i3-web, and i3-admin: `iplus-deploy.sh start`
- Start iplus only: `iplus-deploy.sh start_iplus`
- Start i3web only: `iplus-deploy.sh start_i3web`
- Start i3admin only: `iplus-deploy.sh start_i3admin`

11.7.3. Security maintenance

11.7.3.1. Network security maintenance

Network security maintenance handles the device security and the network security.

Device security

- Check network devices, and enable security management protocols and configurations of the devices.
- Check for new versions of the network device software and update to a more secure version in a timely manner.
- For more information about the security maintenance methods, see the product documentation of each device.

Network security

Select the intrusion detection system (IDS) or intrusion prevention system (IPS) based on the network situations to detect public and internal network traffic and protect the network against attacks and unusual activities.

11.7.3.2. Account password maintenance

Account passwords include the Graph Analytics system password and the device password.

To ensure account security, you must change the system and device passwords periodically, and use passwords with high complexity.

11.7.4. Troubleshooting

11.7.4.1. Fault response mechanism

The IT administrator must establish a fault emergency response mechanism, so that the service can be recovered quickly after a fault or security accident occurs.

11.7.4.2. Troubleshooting methods

After a system fault is detected during routine maintenance, the IT administrator can read the Operations and Maintenance part of this documentation for reference.

If the fault cannot be fixed, collect the fault information, including the system information and fault symptoms, contact Alibaba Cloud technical support engineers, and troubleshoot the fault under the guidance of the engineers.

After the fault is fixed, the IT administrator must analyze the causes, review the troubleshooting process, and make improvements.

11.7.4.3. Common failure troubleshooting

Insufficient disk space

Possible cause: The log size in the Graph Analytics system is too large.

Solution: Monitoring logs are usually stored in the `/home/admin/logs` directory. You can delete earlier logs to free up space.

Machine maintenance or downtime

Possible cause: The hardware is damaged or the warranty of the machine is expired.

Solution: Reinstall Graph Analytics.

Suspicious processes

Possible cause: If the process fails to start automatically or is terminated unexpectedly, view the logs in `/home/admin/logs` to identify the cause.

Solution: Restart Graph Analytics.

11.7.4.4. Hardware troubleshooting

Disk failure

Disk failure

Solution: Graph Analytics supports cluster deployment. Therefore, you can directly end all Graph Analytics threads, replace the hard drive, and then start the threads again.

Failures requiring server shutdown, including memory, MPU, CPU, and power supply failures

Solution:

Repairs involving server shutdown:

- If you can access the system, you can follow the service stop procedure to disable the Graph Analytics service on the server.
- If you cannot access the system, you must force the server to shut down.

11.8. Machine Learning Platform for AI

11.8.1. Query server and application information

11.8.1.1. Apsara Stack Machine Learning Platform for AI

11.8.1.1.1. Query server information

Machine Learning Platform for AI is deployed based on Apsara Infrastructure Management Framework. Its application information and database information can be found by accessing the corresponding Apsara Infrastructure Management Framework address. This topic describes how to query server information.

Procedure

1. Open Chrome and ensure that you can access internal services through the network.
2. Enter the username and password to log on to the homepage of Apsara Infrastructure Management Framework.

    > **Notice** To avoid logon failures, make sure that your network is connected and the hosts have been bound.

3. Click the C and search for **pai**. Hover over the dots next to PaiCluster-20170630-c34b, and choose **Dashboard** from the shortcut menu.
4. Query the server information for an application, such as the server where PaiDmscloud runs.
    i. Find the service instance and click **Details**. The instance detail page appears.
    ii. Find the role list and click **Details**. The role detail page appears.
    iii. The IP address of the server is displayed in the server information list. You can click **Terminal** to manage the server on the terminal management page.

11.8.1.1.2. Log on to a server

Machine Learning Platform for AI is deployed based on Apsara Infrastructure Management Framework. Its application information and database information can be found by accessing the corresponding Apsara Infrastructure Management Framework address. This topic describes how to log on to a server.

Context

Each module is deployed on two servers with the same application package and configuration. You can log on to the back-end server through the server IP address and perform operations.

Procedure

1. Ensure that the network is connected and the IP address of the jump server has been obtained.
2. Log on to the jump server.
3. Switch to the root account.
4. All applications are deployed by using a Docker container. You can run the following command to view the current container:

   ```
   sudo docker ps
   ```

5. Run the following command to go to the container:

   ```
   sudo docker exec –ti container_id /bin/bash
   ```

   The application log is stored in the */home/admin/logs/${app}* path.

11.8.1.1.3. Query configurations

Prerequisites

Log on to the server of an application and go to the application container to view the configuration of the application.

Procedure

1. View the application configuration in the */home/admin/{app}/target/exploded/BOOTINF/classes/application.yml* file.

   > **Note** In the preceding file path, {app} indicates the component name, such as pai-dms.

2. View the application log in the */home/admin/pai-dms/* path.

   The pai-dms.log, err_pai-dms.log, java.log, and access.log files store the application log, error log, framework log, and access log, respectively.

3. Log on to a database.

   i. Query the database information of modules from the Dashboard cluster information of Apsara Infrastructure Management Framework. Find the corresponding **result** column and click **More** from the shortcut menu to obtain db_host, db_port, db_name, db_password, and db_user of the application.

   ii. Run the following command to connect to the database through a MySQL client:

   ```
   mysql –h$db_host –P$db_port –u$db_user –p$ db_password –D$ db_name
   ```

11.8.1.1.4. Restart an application service

The application structures and directories of the PaiCap, PaiDmscloud, and PaiJcs modules are almost the same. You can restart an application service in either of the following ways:

- Log on to the container and run the following command to restart the service:

  ```
  sudo -u admin /home/admin/pai-dms/bin/appclt.sh restart
  ```

- Run the following command on the server to restart the container:

  ```
  sudo docker restart $container_id
  ```

Run the following command to check whether the service is restarted:

```
curl localhost/status.taobao
```

11.8.1.2. Online model service

11.8.1.2.1. Query online model service information

Check the online model service status

Online model services are deployed in the Kubernetes cluster. Log on to the master node in the Kubernetes cluster and run the following command to query the service deployment status:

```
kubectl get pod -n eas-system
```

If no errors occur, all pods in the STATUS column display *Running*.

If not, run the following command to perform troubleshooting:

```
kubectl describe pod ${pod_name} -n eas-system
```

View the online model service configurations

1. Log on to the homepage of Apsara Infrastructure Management Framework.
2. Click the **C** tab and search for **pai**. Hover over the dots next to the PAI cluster, and choose **Dashboard** from the shortcut menu.
3. Search for the *eas-sentinel* role and log on to the VM from the terminal.
4. Run the `docker ps |grep eas-sentinel` command to view the ID of the container for the sentinel.
5. Run the `docker logs ${sentinelcontainerid}` command to view the output log, which contains the configuration information of the online model service.

11.8.1.2.2. Log on to the online model service container

Prerequisites

Ensure that the network is connected and the IP address of the jump server has been obtained.

Procedure

1. Log on to the jump server.
2. Switch to the root account.
3. All applications are deployed with a container. Run the following command to log on to the current pod: `kubectl exec -ti ${pod_name} -n ${pod_namespace} – bash`

11.8.1.2.3. Restart a pod

Procedure

1. Log on to the master node in the Kubernetes cluster.
2. Run the `kubectl get` command to find the corresponding *pod name*.
3. Run the following command to restart the pod: `kubectl delete ${pod_name}`

11.8.1.3. GPU cluster and task information

11.8.1.3.1. Query GPU cluster information

Prerequisites

You must deploy the deep learning service before querying the GPU cluster information. Deep learning tasks are performed in the GPU cluster. You can log on to ApsaraAG of the GPU cluster to query the GPU cluster status.

Procedure

1. Log on to the homepage of Apsara Infrastructure Management Framework.
2. Click the C tab and search for *PAIGPU*. Move the pointer over the dots next to the deployed GPU cluster. Log on to the cluster O&M center.
3. Select *pai-deep_learning* from the Service drop-down list and *ApsaraAG#* from the Service Role drop-down list. Log on to the VM from the terminal.
4. Run the `r ttrl` command to view all GPU workers in the current GPU cluster.

   If the Other column displays `FUXI_GPU:200`, the worker has two GPUs. If the column displays `FUXI_GPU:800`, the worker has eight GPUs.

11.8.1.3.2. Query GPU task information

Procedure

1. Perform steps 1 through 3 in Query GPU cluster information and log on to ApsaraAG of the GPU cluster.
2. Run the `r al` command to view the running tasks.
3. Run the `r wwl WorkItemName` command to view the status of a task and the allocated resources. `WorkItemName`: specifies the values in the first column displayed by the `r al` command.
4. Run the `r cru` command to view the resources allocated to the current cluster, including CPU, memory, and FUXI_GPU resources.
5. > **Notice** Use caution when performing this step.

   Run the `r jstop WorkItemName` command to stop a Fuxi task. `WorkItemName`: specifies the values in the first column displayed by the `r al` command.

11.8.2. Maintenance and troubleshooting

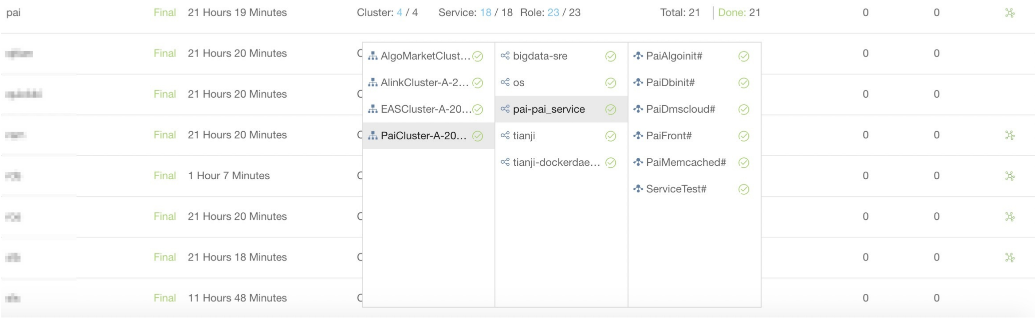
11.8.2.1. Machine Learning Platform for AI maintenance

11.8.2.1.1. Run ServiceTest

After ServiceTest is run, the automated test case is executed.

1. Log on to the homepage of Apsara Infrastructure Management Framework and choose **Tasks > Deployment Summary** from the top navigation bar. The **Deployment Summary** page appears.
2. On the **Deployment Summary** page, click **Deployment Details**. The Deployment Details page appears.
3. Move the pointer over the row in which the project name is PAI. Click **Details**, and click **ServiceTest#** to go to the server list page.
4. On the machine learning list page, click **Terminal** to access **TerminalService**.
5. Run the `sudo docker ps -a` command to find the ServiceTest instance of PAI, as shown in the following figure.

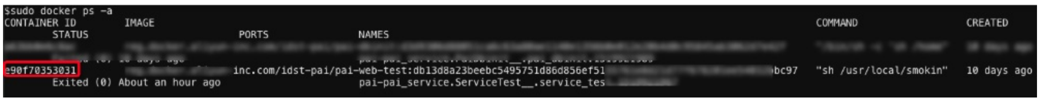
   ServiceTest instance

pai	Final	21 Hours 19 Minutes	Cluster: 4 / 4 Service: 18 / 18 Role: 23 / 23	Total: 21 Done: 21	0	0	
[redacted]	Final	21 Hours 20 Minutes	C		0	0	
[redacted]	Final	21 Hours 20 Minutes	C		0	0	
[redacted]	Final	21 Hours 20 Minutes	C		0	0	
[redacted]	Final	1 Hour 7 Minutes	C		0	0	
[redacted]	Final	21 Hours 20 Minutes	C		0	0	
[redacted]	Final	21 Hours 18 Minutes	C		0	0	
[redacted]	Final	11 Hours 48 Minutes	C		0	0	

6. Run the `sudo docker restart e90f70353031` command to restart the ServiceTest service, as shown in the following figure.

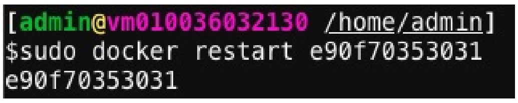
   Restart the ServiceTest service

   ```
   $sudo docker ps -a
   CONTAINER ID        IMAGE                                                                                                           COMMAND                  CREATED
           STATUS                  PORTS               NAMES
   [redacted]
   e90f70353031        [redacted] inc.com/idst-pai/pai-web-test:db13d8a23beebc5495751d86d856ef51[redacted]bc97   "sh /usr/local/smokin"   10 days ago
           Exited (0) About an hour ago                pai-pai_service.ServiceTest__.service_tes[redacted]
   ```

   The test case is executed when the service_test service is restarted. After the execution, you can view the log information.
7. Run the `sudo docker logs e90f70353031 --tail 1000` command to view the log. Only the last 1,000 rows are displayed.
8. After the test case is executed, the testing results for all algorithms are displayed, as shown in the following figure.

   Testing results

   ```
   [admin@vm010036032130 /home/admin]
   $sudo docker restart e90f70353031
   e90f70353031
   ```

   - PASS: The algorithm is running properly.

- SKIP or FAIL: The algorithm fails.

11.8.2.1.2. Common faults and solutions

11.8.2.1.2.1. Maintenance commands

nc, telent, curl, ping, mysql

`docker images` : shows all images on a server.

`docker ps` : shows the running images on a server.

`docker exec –ti containerID /bin/bash`

`docker log containerID` : shows the container log.

`curl http://localhost/status.taobao` : determines whether the SpringBoot service is started.

11.8.2.1.2.2. pai.xx.xx access failures

Procedure

1. Run the `ping pai.xx.xx` command to check whether the domain name has been translated to the corresponding VIP.

   If the domain name cannot be resolved properly, contact the on-site engineer to check the network configurations.

2. Run the `curl http://ip/status.taobao` command to check whether all service modules are running normally.

   If the status.taobao module fails the check, perform the following operations:

   i. Log on to the server to check whether the container is active.

   ii. Go to the container and run the following command to check whether the service process is active:

   ```
   ps –lef | grep java
   ```

   iii. View the */home/admin/{app}/logs/err_pai-dms.log* file to locate causes, such as dependent tenant service request timeout, dependent OCS timeout, and database connection exceptions.

   We recommend that you view the log after checking all items in the checklist to verify whether the malfunction was not caused by a component exception.

3. Verify whether ApsaraDB RDS is accessible.

   i. Run the following command to check whether the port is active:

   ```
   nc –v –z $rds_host $port
   ```

   ii. Run the following command to check whether the database is accessible:

   ```
   mysql –h$Host –P$Port –u$user –p$password
   ```

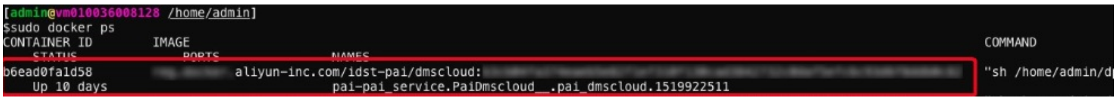
4. Verify whether the caching service is functioning properly.

   Run the following command to check whether port 11211 is active:

   ```
   nc –v –z $ocs_host 11211
   ```

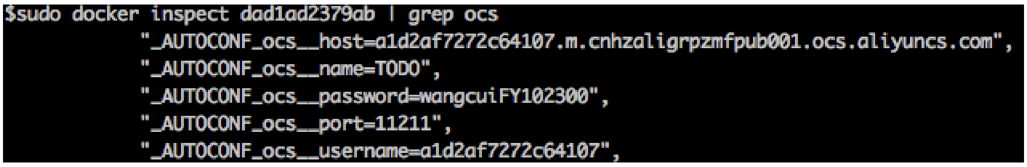
Search for ocs_host as follows:

i. Search for the dmscloud instance, as shown in the following figure.



```
[admin@vm010036008128 /home/admin]
$sudo docker ps
CONTAINER ID        IMAGE                                                                                   COMMAND
    STATUS              PORTS               NAMES
b6ead0fa1d58        [redacted]      aliyun-inc.com/idst-pai/dmscloud:[redacted]                           "sh /home/admin/d
    Up 10 days                              pai-pai_service.PaiDmscloud__.pai_dmscloud.1519922511
```

ii. Run the `sudo docker inspect b6ead0fa1d58 | grep ocs` command to view the ocs_host information, as shown in the following figure.



```
$sudo docker inspect dad1ad2379ab | grep ocs
                "_AUTOCONF_ocs__host=a1d2af7272c64107.m.cnhzaligrpzmfpub001.ocs.aliyuncs.com",
                "_AUTOCONF_ocs__name=TODO",
                "_AUTOCONF_ocs__password=wangcuiFY102300",
                "_AUTOCONF_ocs__port=11211",
                "_AUTOCONF_ocs__username=a1d2af7272c64107",
```

`host` is a list of servers on which OCS (caching service) is deployed. `port` indicates the port number.

Machine Learning Platform for AI in Apsara Stack typically uses the built-in memcached service as the dependent caching service. If port 11211 is inaccessible, log on to the server and run the following command to restart the memcached service:

```
docker restart containerid
```

11.8.2.1.2.3. Experiment failures

We recommend that you run a Machine Learning Platform for AI experiment in Google Chrome version 66 or later. Google Chrome is the only supported browser.

- Components cannot be dragged and dropped.

  Clear cookies and caches, and then retry. Check the version of Chrome. If the problem persists, it is due to a service failure. Log on to the container to view the log.

- An error message is displayed while an algorithm is running.

  If an error message is displayed, the task has been submitted to MaxCompute. Check the parameters and source data against the user guide and algorithm descriptions to locate the error.

11.8.2.1.2.4. Other failures

If a problem persists after you have checked all items by referring to pai.xx.xx access failures, troubleshoot the underlying dependency services, including MaxCompute and DataWorks (tenants and metadata).

- MaxCompute: Make sure that MaxCompute can pass the pai_console test.
- DataWorks: Make sure the configured domain name is accessible, and verify the application log.

If no errors are found, restart the service.

11.8.2.2. Online model service maintenance (must be activated separately)

Node maintenance

Online model service nodes are Kubernetes nodes. You can run the `kubectl get node` command to view all nodes in a cluster. A healthy node is in the Ready state. When a node is not in the Ready state, the one of the following errors may have occurred:

- Node failures

  There are many reasons that may cause a node to fail. Typically, a node fails when the kernel crashes or the disk does not have sufficient space. If the node can be restarted properly, it rejoins the cluster after it is restarted. If the node cannot be restarted properly, contact the corresponding ECS support personnel.

- Docker daemon exceptions

  A Docker daemon exception rarely occurs. Docker daemon exceptions are typically caused by storage issues. Run the `systemctl restart docker` command to restart the Docker daemon.

Online model service maintenance

- A service cannot be created or deleted.
  - If Error 500 is returned while an operation is called, the configurations of the eas-ui component are incorrect. Contact Apsara Stack delivery engineers.
  - If a creation or deletion operation is called but no response is returned in a timely manner, the jobworker of the service does not work properly. Check whether the KVStore for Redis service in the cluster is normal. If not, restart the pod for KVStore for Redis.

- The system fails to read the monitoring data.

  Check whether the influxdb-0 pod under *eas-system* is created properly. If the pod is not in the running state, an influxdb out of memory error has occurred. You can expand the influxdb-0 memory.

Service maintenance

- Service creation failures.

  The request is sent but the service creation result displays **Failed**. A model error has caused a crash. The system then fails to create the model. Check whether the model code contains any null pointers or has any other problems.

- The system fails to obtain the monitoring data.

  Check whether the influxdb-0 of each service is normal. The service cannot be created because a persistent volume cannot be created. Check whether the Apsara Stack environment has sufficient disk space. If influxdb-0 runs properly but you cannot obtain the monitoring data, restart the influxdb-0 pod.

11.8.2.3. GPU cluster maintenance (deep learning must be activated separately)

Node maintenance

A deep learning node is a server where a GPU cluster runs.

1. Perform steps 1 through 3 in Query GPU cluster information and log on to ApsaraAG of the GPU cluster.
2. Run the `r ttrl` command to view all nodes that support deep learning tasks.

- Node failures

  There are many reasons that may cause a node to fail. Typically, a node fails when the kernel crashes or the disk does not have sufficient space. If the node can be restarted properly, it rejoins the cluster after it is restarted. If the node cannot be restarted properly, contact the corresponding service support team.

- Docker daemon exceptions

  A Docker daemon exception rarely occurs. Docker daemon exceptions are typically caused by storage issues. Run the `systemctl restart docker` command to restart the Docker daemon.

Service maintenance

Failure to allocate resources to a task

Perform the following steps for troubleshooting:

1. Perform steps 1 through 3 in Query GPU cluster information and log on to ApsaraAG of the GPU cluster.
2. Run the `r quota` command to view the quota information of the GPU cluster.
3. Run the `r cru` command to view the resources allocated to each task in the current cluster.
4. Run the `r al` command to view all tasks submitted to the cluster.
5. Run the `r wwl WorkItemName` command to view the status of a specific task.
   - If only **ChildMaster** is displayed, no resources are allocated to the worker.
   - If **worker name** is displayed but no **hostname** is displayed, service resuming is pending or has failed. Log on to the server of the ChildMaster and locate the error. You can also contact the service support team.
6. Run the `r ttrl` command to check the value of **FUXI_GPU** in the **Other** column. If the value is 200, the worker has two GPUs. If the value is 800, the worker has eight GPUs.
7. Log on to a GPU worker in the worker list obtained in Step 3 over SSH. Run the `nvidia-smi` command to view the GPU status. If an exception occurs, contact the relevant service support personnel.

11.9. DataHub

11.9.1. Concepts and architecture

11.9.1.1. Terms

Project

A project is an organizational unit in DataHub and contains one or more topics. DataHub projects and MaxCompute projects are independent of each other. Projects that you create in MaxCompute cannot be used in DataHub.

Topic

The smallest unit for data subscription and publishing. You can use topics to distinguish different types of streaming data. For more information about projects and topics, see Limits in *Product Introduction*.

Topic lifecycle

The period that each record can be retained in the topic. Unit: day. Valid values: 1 to 7.

Shard

A shard in a topic. Shards ensure the concurrent data transmission of a topic. Each shard has a unique ID. A shard can be in different states. For more information about shard status, see the following table. Each active shard consumes server resources. We recommended that you create shards as needed.

Note Shard status

Status	Description
Activating	All shards in a topic are in the Activating state when the topic is created. You cannot perform read or write operations on shards because they are being activated.
Active	Read and write operations are allowed when a shard is in the Active state.
Deactivating	A shard is in the Deactivating state when it is being split or merged with another shard. You cannot perform read or write operations on the shard because it is being deactivated.
Deactivated	A shard is in the Deactivated state when the split or merge operation is complete. The shard is read-only when it is in the Deactivated state.

Hash key range

The range of hash key values for a shard, which is in the format of [Starting hash key,Ending hash key). The hashing mechanism ensures that all records with the same partition key are written to the same shard.

Shard merge

The operation that merges two adjacent shards. Two shards are considered adjacent if the hash key ranges for the two shards form a contiguous set with no gaps.

Shard split

The operation that splits one shard into two adjacent shards.

Record

A unit of data that is written into DataHub.

Record type

The data type of records in a topic. Tuple and blob are supported. A tuple is a sequence of immutable objects. A blob is a chunk of binary data stored as a single entity.

Note

- The following table describes the data types that are supported in a tuple topic. Tuple data types

Data type	Description	Valid values
Bigint	An 8-byte signed integer. Note Do not use the minimum value, which is -9223372036854775808, because this is a system reserved value.	-9223372036854775807 to 9223372036854775807
String	A string. Only UTF-8 encoding is supported.	A string whose size is no greater than 1 MB
Boolean	One of two possible values.	True and False, true and false, or 0 and 1
Double	A double-precision floating-point number. It is 8 bytes in length.	-1.0 10^{308} to 1.0 10^{308}
TimeStamp	A timestamp.	A timestamp that is accurate to microseconds

- In a blob topic, a chunk of binary data is stored as a record. Records written to DataHub are Base64 encoded.

Service roles

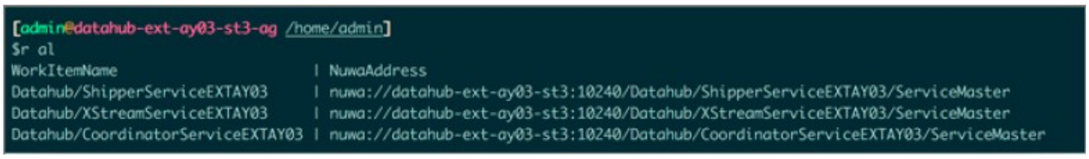
Available service roles in DataHub

Service	Service role	Description
DataHub	Xstream	Receives read and write requests from the frontend server and forwards the requests to Apsara Distributed File System.
	Shipper/Connector	Synchronizes data from DataHub to other Apsara Stack services, including MaxCompute, ApsaraDB RDS for MySQL, and Object Storage Service (OSS).
	Coordinator	Saves consumption offsets for applications. You can resume data consumption from a saved consumption offset.
	Frontend	Receives all the read and write requests.

Run the following command on the admin gateway of a cluster to query the services deployed on the cluster:

```
r al
```

Services deployed on the cluster

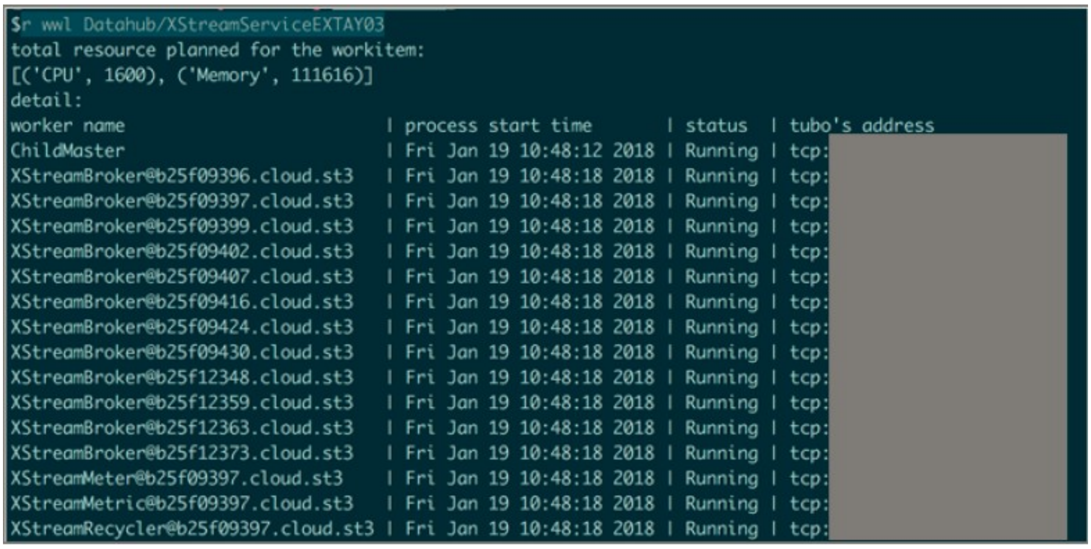


```
[admin@datahub-ext-ay03-st3-ag /home/admin]
$r al
WorkItemName                       | NuwaAddress
Datahub/ShipperServiceEXTAY03      | nuwa://datahub-ext-ay03-st3:10240/Datahub/ShipperServiceEXTAY03/ServiceMaster
Datahub/XStreamServiceEXTAY03      | nuwa://datahub-ext-ay03-st3:10240/Datahub/XStreamServiceEXTAY03/ServiceMaster
Datahub/CoordinatorServiceEXTAY03 | nuwa://datahub-ext-ay03-st3:10240/Datahub/CoordinatorServiceEXTAY03/ServiceMaster
```

Run the following command on the admin gateway of the cluster to query the service role and the hosts where the service is running:

```
r wwl $WorkItemName
```

Service role and hosts where the service is running



```
$r wwl Datahub/XStreamServiceEXTAY03
total resource planned for the workitem:
[('CPU', 1600), ('Memory', 111616)]
detail:
worker name                          | process start time       | status  | tubo's address
ChildMaster                          | Fri Jan 19 10:48:12 2018 | Running | tcp:
XStreamBroker@b25f09396.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f09397.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f09399.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f09402.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f09407.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f09416.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f09424.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f09430.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f12348.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f12359.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f12363.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamBroker@b25f12373.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamMeter@b25f09397.cloud.st3     | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamMetric@b25f09397.cloud.st3    | Fri Jan 19 10:48:18 2018 | Running | tcp:
XStreamRecycler@b25f09397.cloud.st3 | Fri Jan 19 10:48:18 2018 | Running | tcp:
```

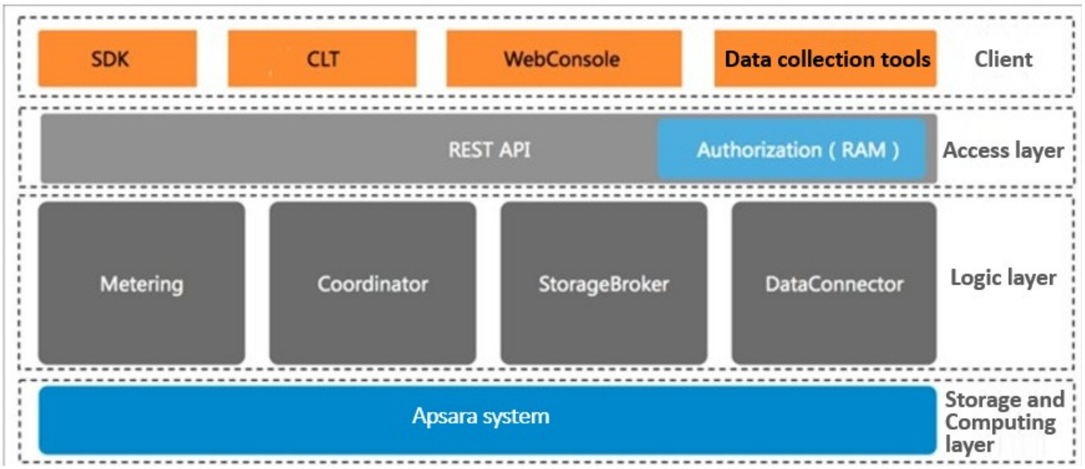
[redacted]

11.9.1.2. Architecture

11.9.1.2.1. Architecture

Architecture shows the architecture of DataHub.

Architecture



The architecture of DataHub consists of four layers: **clients**, **access layer**, **logic layer**, and **storage and scheduling layer**.

Clients

DataHub supports the following types of clients:

- SDKs: DataHub provides SDKs in a variety of languages such as C++, Java, Python, Ruby, and Go.
- Command-line tools (CLTs): You can run commands in Windows, Linux, or Mac operating systems to manage projects and topics.
- Console: In the console, you can manage projects and topics, create subscriptions, view the shard status, monitor topic performance, and manage DataConnectors.
- Data collection tools: You can use Logstash, Fluentd, and Oracle GoldenGate (OGG) to collect data to DataHub.

Access layer

You can access DataHub by using HTTP and HTTPS. DataHub supports Resource Access Management (RAM) authorization and horizontal scaling of topic performance.

Logic layer

The logic layer handles the key features of DataHub, including project and topic management, data read and write, offset-based data consumption, traffic statistics, and data synchronization. Based on these key features, the logic layer is composed of the following modules: StorageBroker, Metering, Coordinator, and DataConnector.

- StorageBroker: provides data reads and writes in DataHub. This module adopts the log file storage model of Apsara Distributed File System, halving the read/write volume compared with the conventional write-ahead logging (WAL) model. This module stores three copies of data to ensure that no data is lost if a server fault occurs, and supports disaster recovery between data centers. It supports real-time data caching to ensure efficient consumption of real-time data and supports an independent read cache of historical data to enable concurrent consumption of historical data.
- Metering: supports shard-level billing based on the consumption period.
- Coordinator: supports offset-based data consumption and horizontal scaling of the processing capacity. It supports up to 150,000 QPS on a single node.
- DataConnector: supports automatic data synchronization from DataHub to other Apsara Stack services, including MaxCompute, OSS, AnalyticDB, ApsaraDB RDS for MySQL, Tablestore, and Elasticsearch.

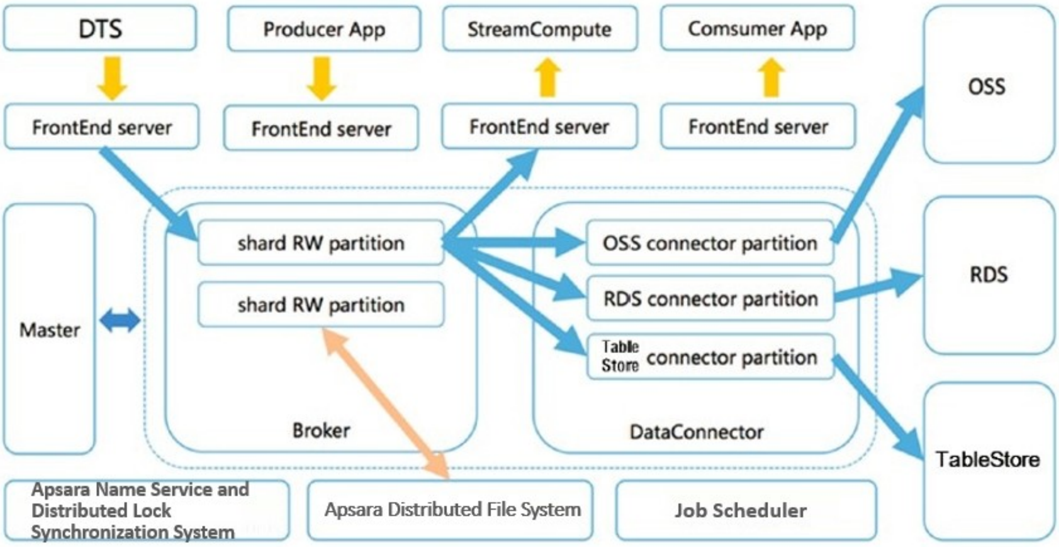
Storage and scheduling layer

- Storage: Based on the log file storage model of Apsara Distributed File System, DataHub supports append operations and solid state drive (SSD) storage. Data in each shard is stored in a separate file based on the timestamp of the data.
- Scheduling: Based on Job Scheduler, DataHub assigns shards to nodes based on the traffic on each shard. This ensures that the shards do not occupy the CPU or memory of Job Scheduler. The number of partitions on a single node has no upper limit. DataHub supports failovers within milliseconds and hot upgrades.

11.9.1.2.2. Technical architecture

Technical architecture of DataHub shows the technical architecture of DataHub.

Technical architecture of DataHub



The figure shows the process from data ingestion to consumption.

1. A shard is the smallest unit of data management in DataHub, and is a first-in, first-out (FIFO) collection of records.
2. Data in each shard is stored in a set of log files in Apsara Distributed File System.
3. The master distributes each shard to a StorageBroker. Each StorageBroker is responsible for the read and write operations on multiple shards.
4. The frontend server finds a StorageBroker based on the project, topic, and shard information specified in the request and forwards the request to the StorageBroker.
5. DataConnectors read data from the StorageBroker and forward the data to other Apsara Stack services.

Data collection

You can write data to DataHub from applications developed by using SDKs and data collection tools such as Logstash, Fluentd, and OGG. You can also write data by using Data Transmission Service (DTS) and Realtime Compute.

Frontend server

Frontend servers constitute the access layer and support horizontal scaling. You can call RESTful API operations to access DataHub. RAM authorization is supported.

Master

The master handles metadata management and shard scheduling. It supports create, read, update, and delete operations on projects and topics. The master also supports split and merge operations on shards.

StorageBroker

StorageBrokers handle read and write operations on each shard including data indexing, caching, and file organization and management.

DataConnector

DataConnectors forward data in DataHub to other Apsara Stack services. DataConnectors provide different features for various destination services. These features include automatically creating partitions in MaxCompute and converting data streams into files stored in OSS.

11.9.2. Commands and tools

11.9.2.1. Common commands for the Apsara system

DataHub is built based on the Apsara system. Both DataHub and the Apsara system including Job Scheduler, Apsara Distributed File System, and Apsara Name Service and Distributed Lock Synchronization System are hosted by Apsara Infrastructure Management Framework.

- Run the following command to view the server roles that are installed on the server:

```
tj_show
```

- Run the following command to view all server roles:

```
tj_show –l
```

- Run the following command to retrieve a list of servers that the pangu_chunkserver server role is installed on:

```
tj_show -r pangu.PanguChunkserver# //The hostnames of the servers are returned.
tj_show -r pangu.PanguChunkserver# -ip //The IP addresses of the servers are returned.
```

- Run the following command to retrieve a list of servers that the FrontEnd server role is installed on:

```
tj_show –r datahub-frontend.Frontend#
```

- Run the following command to retrieve a list of servers that the WebConsole server role is installed on:

```
tj_show –r datahub-webconsole.WebConsole#
```

11.9.2.2. Common commands for Apsara Distributed File System

Commands for Apsara Distributed File System start with pu or puadmin. To view the complete description of a command, enter the command followed by **--help** and press enter.

- Run the following command similar to the ls command used in Linux to retrieve the file content in a specific directory:

```
pu ls
```

- Run the following command to upload local files to Apsara Distributed File System:

```
pu put
```

- Run the following command to retrieve metadata:

```
pu meta
```

- Run the following command to retrieve details about all masters in Apsara Distributed File System:

```
puadmin gems
```

- Run the following command to retrieve details about all chunk servers:

```
puadmin lscs
```

- Run the following command to view version information:

```
puadmin --buildinfo
```

- Before maintaining a chunk server, remove the chunk server from the cluster. Perform the following operations:
  i. Run the following command to retrieve the current status of a chunk server:

  ```
  pyadmin cs -stat tcp://x.x.x.x:10260
  ```

  ii. Run the following command to remove the chunk server from the cluster by setting its status to shutdown:

  ```
  pyadmin cs -stat tcp://x.x.x.x:10260 --set=shutdown
  ```

  iii. After the maintenance is completed, run the following command to add the chunk server back to the cluster:

  ```
  pyadmin cs -stat tcp://x.x.x.x:10260 --set=normal
  ```

11.9.2.3. Common commands for Job Scheduler

The commands for Job Scheduler start with `r`, which is encapsulation of rpc.sh.

```
alias r='sh /apsara/deploy/rpc_wrapper/rpc.sh'
```

- Run the following command to retrieve all services and service jobs:

```
r al
```

> ⓘ **Note** Typically, service jobs are deployed on the DataHub cluster. The list returned has many entries.

- Run the following command to retrieve the status of a service:

```
r wwl $servicename
```

- Run the following command to terminate a service:

```
r sstop $servicename
```

- Run the following command to start a service:

```
r sstart $servicename
```

- Run the following command to retrieve a list of all resources in the cluster:

```
r ttrl
```

- Run the following command to retrieve a list of idle resources in the cluster:

  ```
  r tfrl
  ```

  You can run other commands for scheduling purposes as needed.

11.9.2.4. Xstream

You can run commands on a service terminal by using Xstream for maintenance purposes. To access the target service terminal, perform the following operations:

> ? **Note** To use Xstream, you must log on as the administrator.

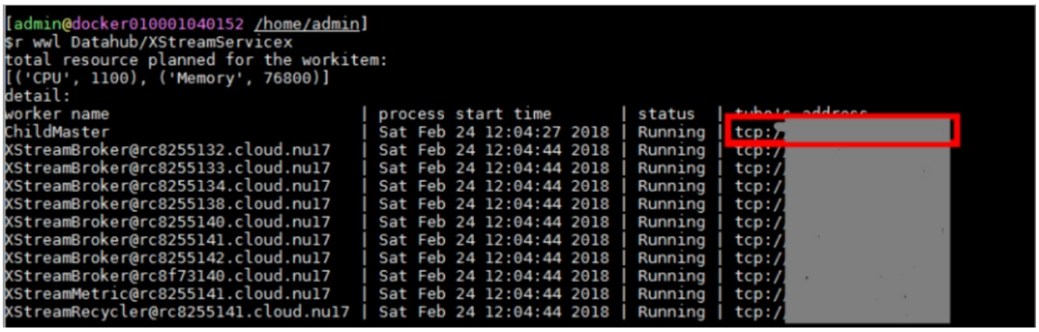
1. Log on to the Apsara Infrastructure Management Framework console. In the left-side navigation pane, choose **Operations > Cluster Operations**. On the Cluster Operations page, enter datahub in the **Clusters** search box in the upper-right corner.
2. Click the name of the cluster in the search result. The **Services** tab on the Cluster Details page appears. In the **Service** search box, enter **datahub-webconsole**. Click datahub-webconsole in the search result.
3. The server role **datahub-webconsole.WebConsole#** appears. Click **Terminal** in the Actions column of the host to go to the TerminalService page.

On the TerminalService page, you can use Xstream to run commands for maintenance purposes.

1. Run the following command and find the IP address of ChildMaster. Log on to the host where ChildMaster is running by using Secure Shell (SSH).

   ```
   r wwl Datahub/XStreamServicex
   ```

   Find the IP address of ChildMaster

   ```
   [admin@docker010001040152 /home/admin]
   $r wwl Datahub/XStreamServicex
   total resource planned for the workitem:
   [('CPU', 1100), ('Memory', 76800)]
   detail:
   worker name                          | process start time       | status  | tubo's address
   ChildMaster                          | Sat Feb 24 12:04:27 2018 | Running | tcp:/[redacted]
   XStreamBroker@rc8255132.cloud.nu17   | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   XStreamBroker@rc8255133.cloud.nu17   | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   XStreamBroker@rc8255134.cloud.nu17   | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   XStreamBroker@rc8255138.cloud.nu17   | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   XStreamBroker@rc8255140.cloud.nu17   | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   XStreamBroker@rc8255141.cloud.nu17   | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   XStreamBroker@rc8255142.cloud.nu17   | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   XStreamBroker@rc8f73140.cloud.nu17   | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   XStreamMetric@rc8255141.cloud.nu17   | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   XStreamRecycler@rc8255141.cloud.nu17 | Sat Feb 24 12:04:44 2018 | Running | tcp:/
   ```

2. Run the following command to go to the specified directory:

   ```
   cd /apsara/tubo/TempRoot/Datahub/XStreamServicex/tool
   ```

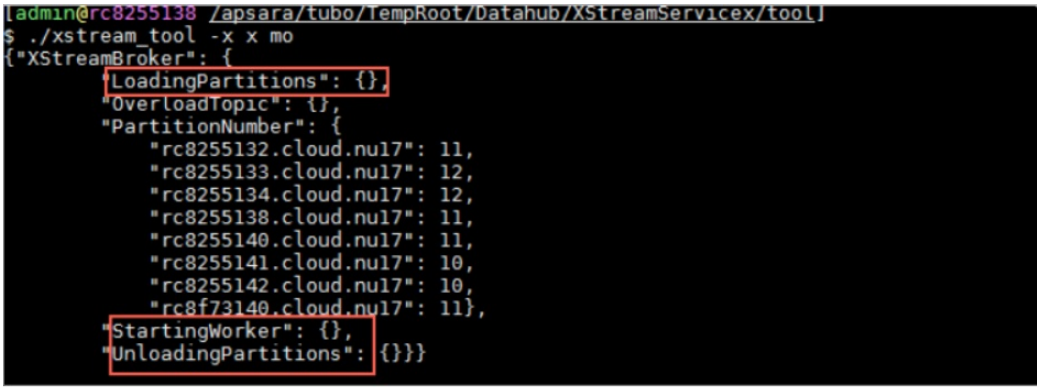
3. Run the following command to configure environment variables:

   ```
   export LD_LIBRARY_PATH=/apsara/lib64/:../lib/
   ```

4. Run the following command to view resources:

   ```
   ./xstream_tool -x x mo
   ```

   View resources



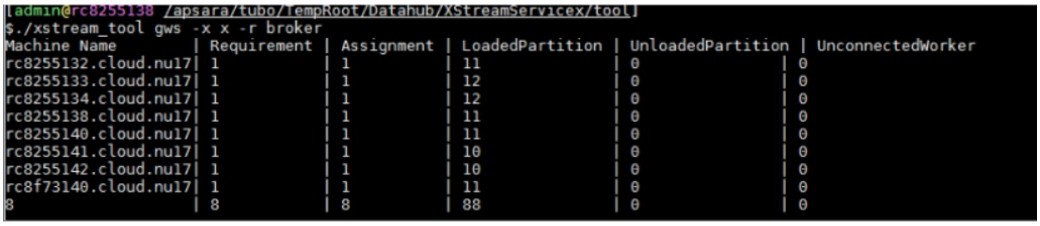
```
[admin@rc8255138 /apsara/tubo/TempRoot/Datahub/XStreamServicex/tool]
$ ./xstream_tool -x x mo
{"XStreamBroker": {
        "LoadingPartitions": {},
        "OverloadTopic": {},
        "PartitionNumber": {
            "rc8255132.cloud.nu17": 11,
            "rc8255133.cloud.nu17": 12,
            "rc8255134.cloud.nu17": 12,
            "rc8255138.cloud.nu17": 11,
            "rc8255140.cloud.nu17": 11,
            "rc8255141.cloud.nu17": 10,
            "rc8255142.cloud.nu17": 10,
            "rc8f73140.cloud.nu17": 11},
        "StartingWorker": {},
        "UnloadingPartitions": {}}}
```

If **LoadingPartitions**, **UnloadingPartitions**, and **StartingWorker** are returned with values, run the command again. If these parameters are repeatedly returned with values, an error may occur when the shards are being activated or deactivated.

5. Run the following command to check the status of all StorageBrokers:

```
./xstream_tool gws -x x -r broker
```

Check the status of all StorageBrokers



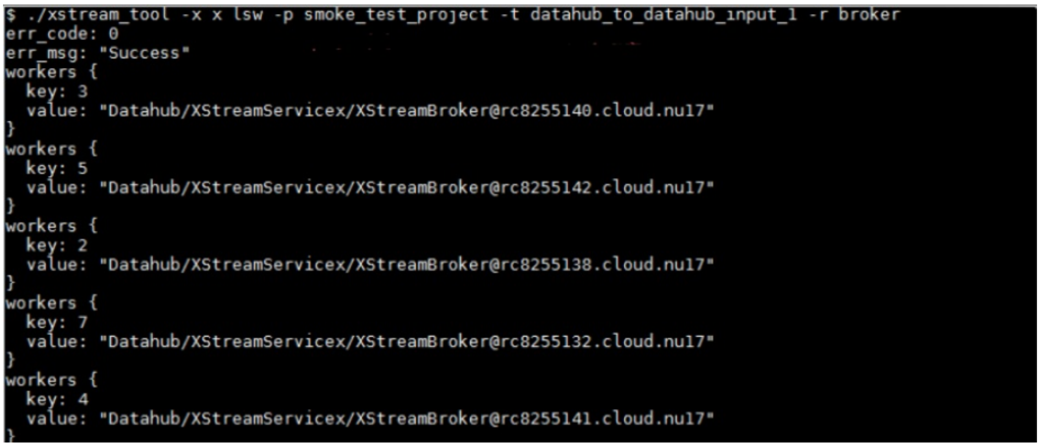
```
[admin@rc8255138 /apsara/tubo/TempRoot/Datahub/XStreamServicex/tool]
$./xstream_tool gws -x x -r broker
Machine Name         | Requirement | Assignment | LoadedPartition | UnloadedPartition | UnconnectedWorker
rc8255132.cloud.nu17| 1            | 1          | 11              | 0                 | 0
rc8255133.cloud.nu17| 1            | 1          | 12              | 0                 | 0
rc8255134.cloud.nu17| 1            | 1          | 12              | 0                 | 0
rc8255138.cloud.nu17| 1            | 1          | 11              | 0                 | 0
rc8255140.cloud.nu17| 1            | 1          | 11              | 0                 | 0
rc8255141.cloud.nu17| 1            | 1          | 10              | 0                 | 0
rc8255142.cloud.nu17| 1            | 1          | 10              | 0                 | 0
rc8f73140.cloud.nu17| 1            | 1          | 11              | 0                 | 0
8                    | 8            | 8          | 88              | 0                 | 0
```

When 0 is returned for **UnloadedPartition** and **UnconnectedWorker**, the StorageBrokers are functioning properly.

6. Run the following command to check the status of all shards in the topic:

```
./xstream_tool -x x lsw -p $project -t $topic -r broker
```

Check the status of all shards in the topic



```
$ ./xstream_tool -x x lsw -p smoke_test_project -t datahub_to_datahub_input_1 -r broker
err_code: 0
err_msg: "Success"
workers {
  key: 3
  value: "Datahub/XStreamServicex/XStreamBroker@rc8255140.cloud.nu17"
}
workers {
  key: 5
  value: "Datahub/XStreamServicex/XStreamBroker@rc8255142.cloud.nu17"
}
workers {
  key: 2
  value: "Datahub/XStreamServicex/XStreamBroker@rc8255138.cloud.nu17"
}
workers {
  key: 7
  value: "Datahub/XStreamServicex/XStreamBroker@rc8255132.cloud.nu17"
}
workers {
  key: 4
  value: "Datahub/XStreamServicex/XStreamBroker@rc8255141.cloud.nu17"
}
```

From the command output, you can find the anomalous shards.

> **Note** We recommend that you do not run other commands by using Xstream except for those described in the preceding example. If you need to run other commands, contact an operations engineer.

11.9.2.5. DataHub console

In the DataHub console, you can obtain performance statistics to facilitate O&M.

For more information about how to log on to the DataHub console, see Log on to the DataHub console in *User Guide*.

To check the performance statistics in the DataHub console, perform the following steps:

1. Log on to the DataHub console. In the left-side navigation pane, click **Project Manager**. On the Project List page, find the target project that you want to view performance statistics and click **View** in the Operate column. The project details page appears.
2. On the project details page, find the target topic and click **View** in the Operate column.
3. On the topic details page that appears, click the **Metric Statistics** tab to view the charts that display the performance statistics of the selected topic.

11.9.2.6. Apsara Big Data Manager

Apsara Big Data Manager provides O&M on big data services from the perspective of business, services, clusters, and hosts. You can upgrade big data services, customize alert configurations, and view the O&M history in the Apsara Big Data Manager console.

Apsara Big Data Manager allows onsite Apsara Stack engineers to manage big data services. For example, they can view resource usage, check and handle alerts, and modify configurations.

For information about how to log on to the Apsara Big Data Manager console and the O&M operations of DataHub, see the relevant topics in *DataHub O&M*.

11.9.3. Routine maintenance

11.9.3.1. Restore data after a power outage

Prerequisites

None.

Procedure

1. DataHub stores data in Apsara Distributed File System. A power outage may cause data loss. After a power outage, run the following command in the DataHub console to check whether the data stored in Apsara Distributed File System has been lost:

```
puadmin fs -abnchunk|grep NONE|awk '{print $1}'|awk -F"_" '{print $1}'|while read line;do puadmin who is $line;done|grep FileId|awk '{print $4}' |sort|uniq >/home/admin/lostfile
-- Ignore directories that start with /deleted/ and send all other directories to an operations engineer to check the lost data.
```

2. Restore data based on file types.
   - If DataHub files have been lost, notify your users that they must re-create the corresponding

topics.

- If metadata has been lost, re-install the corresponding package or initialize the Docker container.

3. After the data is restored, wait until the tianji cluster is at desired state. For assistance, contact an operations engineer.

11.9.3.2. Shut down anomalous chunkserver hosts

Prerequisites

None.

Procedure

1. Configure the action and action status for the anomalous chunkserver hosts.

   i. Log on to the ops1 host and set action to rma and action status to pending for the anomalous chunkserver host. In this example, the name of the anomalous chunkserver host is m1.

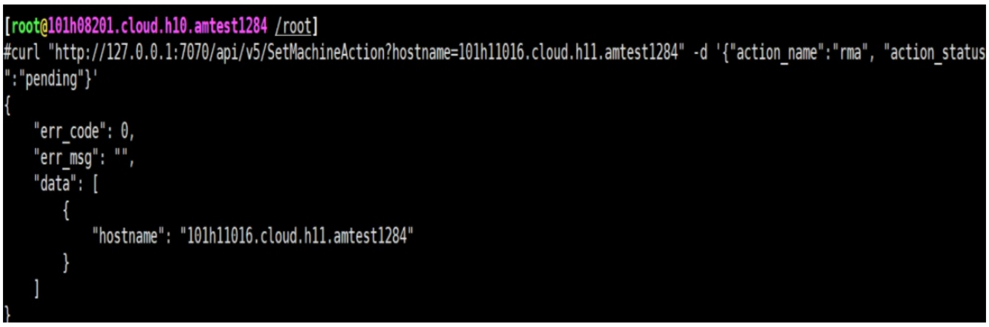
   Run the following command to configure the action and action status for the anomalous chunkserver host:

   ```
   curl "http://127.0.0.1:7070/api/v5/SetMachineAction?hostname=m1" -d '{"action_name":"rma", "a
   ction_status":"pending"}'
   ```

   The following response is returned:

   ```
   {
     "err_code": 0,
     "err_msg": "",
     "data": [
       {
         "hostname": "m1"
       }
     ]
   }
   ```

   Set action to rma and action status to pending for the anomalous chunkserver host



```
[root@101h08201.cloud.h10.amtest1284 /root]
#curl "http://127.0.0.1:7070/api/v5/SetMachineAction?hostname=101h11016.cloud.h11.amtest1284" -d '{"action_name":"rma", "action_status
":"pending"}'
{
    "err_code": 0,
    "err_msg": "",
    "data": [
        {
            "hostname": "101h11016.cloud.h11.amtest1284"
        }
    ]
}
```

> ⓘ **Note** Replace the IP address and hostname in the sample code with those of your anomalous chunkserver host.

ii. Run the following command to configure audit logs:

```
curl "http://127.0.0.1:7070/api/v5/AddAuditLog?object=/m/m1&category=action" -d '{"category":"action", "from":"tianji.HealingService#", "object":"/m/m1", "content": "{\n  \"action\" : \"/action/rma\",\n  \"description\" : \"/monitor/rma=error, mtime: 1513488046851649\",\n  \"status\" : \"pending\"\n}\n" }'
```

Note

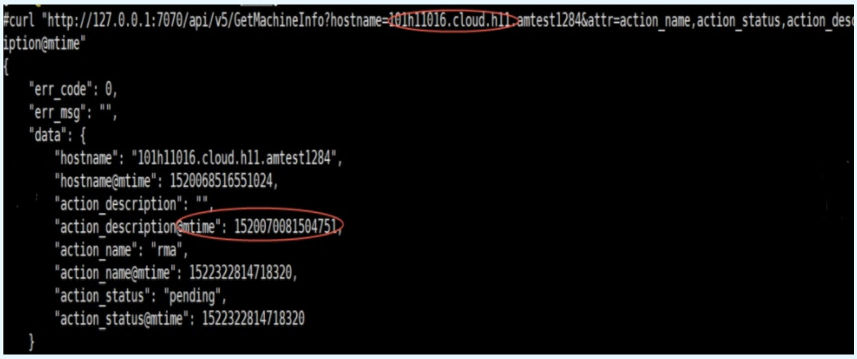
- Replace the IP address and hostname in the sample code with those of your anomalous chunkserver host.
- Replace the value of the mtime parameter in the sample code with the current time.
- Run the following command to query mtime. The sample code is for your reference only.

  ```
  curl "http://127.0.0.1:7070/api/v5/GetMachineInfo?hostname=m1&attr=action_name,action_status,action_description@mtime"
  ```

  The following response is returned:

  ```
  {
    "err_code": 0,
    "err_msg": "",
    "data": {
      "action_description": "",
      "action_description@mtime": 1516168642565661,
      "action_name": "rma",
      "action_name@mtime": 1516777552688111,
      "action_status": "pending",
      "action_status@mtime": 1516777552688111,
      "hostname": "m1",
      "hostname@mtime": 1516120875605211
    }
  }
  ```

  Query mtime

  ```
  #curl "http://127.0.0.1:7070/api/v5/GetMachineInfo?hostname=101h11016.cloud.h11.amtest1284&attr=action_name,action_status,action_desc
  iption@mtime"
  {
      "err_code": 0,
      "err_msg": "",
      "data": {
          "hostname": "101h11016.cloud.h11.amtest1284",
          "hostname@mtime": 1520068516551024,
          "action_description": "",
          "action_description@mtime": 1520070081504751,
          "action_name": "rma",
          "action_name@mtime": 1522322814718320,
          "action_status": "pending",
          "action_status@mtime": 1522322814718320
      }
  ```

2. Wait for approval.

i. Check the action status of the host.

   Run the following command to check the action status of the host:

   ```
   curl "http://127.0.0.1:7070/api/v5/GetMachineInfo?hostname=m1"
   ```

   The response is a long list. We recommend that you search for the host by the keyword **"action_status": "pending"**.

   After you verify that the action status is pending, you can approve the action in the Apsara Infrastructure Management Framework console.

ii. Check the action status of the server role. When the status is approved or done, you can shut down the host for maintenance.

   Run the following command to check the action status:

   ```
   curl http://127.0.0.1:7070/api/v5/GetMachineInfoPackage?hostname=m1&attr=sr.id,sr.action_name,sr.action_status
   ```

   The response is a long list. We recommend that you search for the host by the keyword **"action_status": "pending"**.

3. After the action of the host changes to rma and action status changes to approved or done, shut down the host. Restart the host after the maintenance is completed.
4. After the host is restarted, run the following command to configure the action status of the host:

   ```
   curl "http://127.0.0.1:7070/api/v5/SetMachineAction?hostname=m1&action_name=rma" -d '{"action_name":"rma","action_status":"done", "force":true}'
   ```

5. Check whether the cluster has reached the desired state.

11.9.3.3. Shut down a DataHub cluster

Prerequisites

None.

Procedure

1. Terminate DataHub services.

   i. Log on to the webconsole host of the target cluster and run the following commands as an administrator. Ensure that no data is returned.

   ```
   puadmin abnchunk fs -t none
   puadmin abnchunk fs -t onecopy
   puadmin abnchunk fs -t lessmin
   ```

   ii. On the webconsole host, run the following commands as an administrator to terminate all services run by chunkserver hosts in the Apsara system:

   ```
   r ttrl |grep disk |awk '{print $1}'  > tubo.list
   pssh -h tubo.list -i "/apsara/cloud/tool/tianji/apsarad stop"
   ```

iii. On the webconsole host, run the following command as an administrator to make sure that all services in the Apsara system have been terminated:

```
pssh -h tubo.list -i "/apsara/cloud/tool/tianji/apsarad status"
```

2. Shut down the cluster.
3. Restart DataHub services.

i. On the webconsole host, run the following command as an administrator to restart all services run by chunkserver hosts in the Apsara system:

```
r ttrl |grep disk |awk '{print $1}' > tubo.list
pssh -h tubo.list -i "/apsara/cloud/tool/tianji/apsarad start"
```

ii. On the webconsole host, run the following command as an administrator to make sure that all services in the Apsara system are functioning properly:

```
pssh -h tubo.list -i "/apsara/cloud/tool/tianji/apsarad status"
```

11.9.3.4. Replace a hard drive with a new one on the pangu_cs node

Prerequisite

Obtain the following information:

- The hostname or the IP address.
- The drive letters of the problematic drive. For example, /dev/sdk.
- The ID of the problematic drive. For example, if the path of the problematic drive in the Apsara Distributed File System is /apsarapangu/disk5, the drive ID is 5. You can also obtain the drive ID by running the following command: puadmin lscs -m

Procedure

1. Run the following command to check that the drive to be replaced is in DISK_ERROR status.

```
puadmin lscs -m
```

> **Note** If the hard drive is not in DISK_ERROR status, run the following command to change the status:
>
> ```
> puadmin cs -stat tcp://hostname or IP address:10260 -d drive ID  --set=ERROR
> ```

2. Run the following command to unmount the drive. In this example, the drive letters of the drive to be unmounted are /dev/sdk.

```
sudo umount /dev/sdk1
```

> **Note** Ignore this operation if the df command output shows that the drive is not mounted.

3. After the unmount operation is completed, replace the hard drive in hot swap mode.
4. Upload the **sudo repair_app_disk.sh** script to the server and execute the script to format the drive.
5. Run the following command to set the drive status in the Apsara Distributed File System to OK:

```
puadmin cs -stat tcp://hostname or  IP address:10260 -d drive ID  --set=OK
```

6. Restart the server. After the server is started up, it detects a new hard drive.

> **Note** Kill the processes running on the pangu_cs chunk server and restart the server. Restarting a chunk server does not affect the continuity of your business because DataHub adopts a distributed storage model.

7. Run the following command to check whether the drive status is DISK_OK.

```
puadmin lscs -m
```

You can log on to the server to confirm that the drive has the chunks sub-directory. For example, the chunks exists in the /apsarapangu/disk5/chunks/ directory and new chunks are written into the sub-directory.

11.9.4. DataHub O&M

11.9.4.1. Log on to the ABM console

This topic describes how to log on to the Apsara Big Data Manager (ABM) console.

Prerequisites

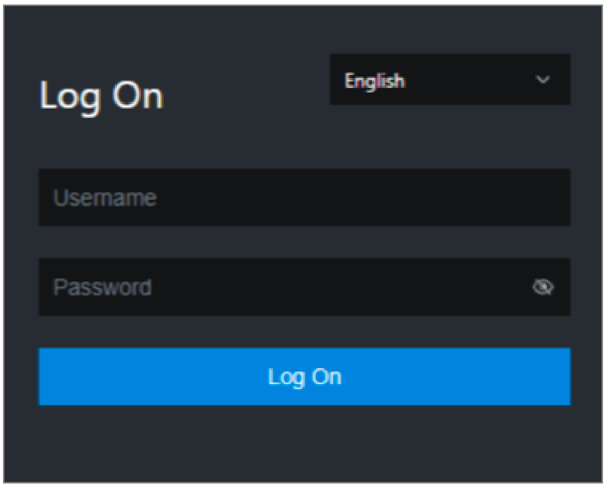
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.



> Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

> Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

For security reasons, your password must meet the following requirements:

- The password contains uppercase and lowercase letters.
- The password contains digits.
- The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
- The password must be 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Product Management > Products**.
7. In the **Big Data Services** section, choose **General-Purpose O&M > Apsara Big Data Manager**.

11.9.4.2. Common operations

The data tables and legends in the Apsara Big Data Manager (ABM) console facilitate operations. This topic uses MaxCompute as an example to describe the common operations.

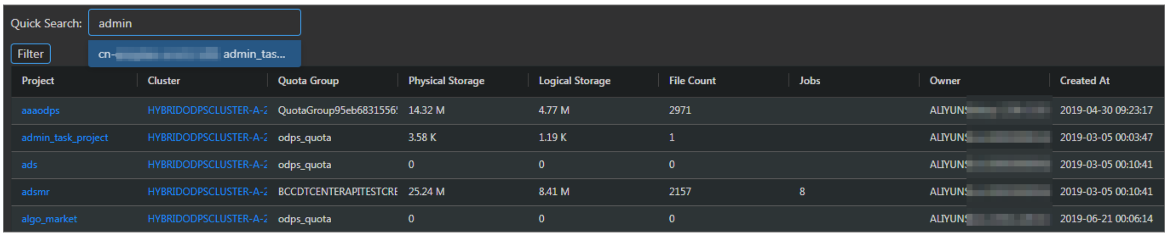
Search for a project quickly

You can quickly search for a project based on the project name.

1. On the **MaxCompute** page, click **O&M** in the upper-right corner, and then click the **Business** tab. The **Project List** page under **Projects** appears.
2. In the **Quick Search** field, enter the project name. Auto-suggestion is supported. Select the target

project from the drop-down list, or select the project by using the up and down arrow keys, and then press **Enter**.

> **Note** When a project is matched, the region of the project appears before the project name.



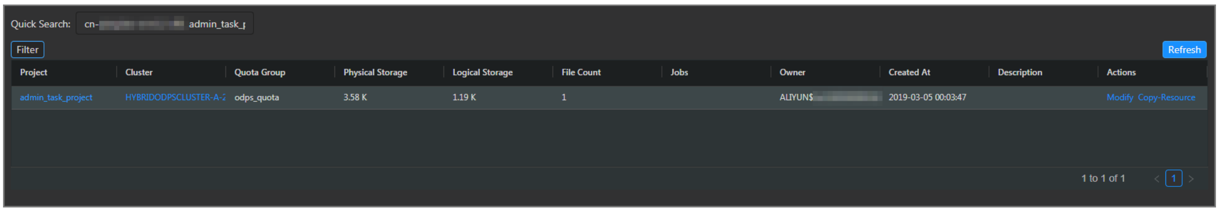
Quick Search: admin

Filter

cn-[redacted] admin_tas...

Project	Cluster	Quota Group	Physical Storage	Logical Storage	File Count	Jobs	Owner	Created At
aaaodps	HYBRIDODPSCLUSTER-A-2	QuotaGroup95eb6831556!	14.32 M	4.77 M	2971		ALIYUN$[redacted]	2019-04-30 09:23:17
admin_task_project	HYBRIDODPSCLUSTER-A-2	odps_quota	3.58 K	1.19 K	1		ALIYUN$[redacted]	2019-03-05 00:03:47
ads	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$[redacted]	2019-03-05 00:10:41
adsmr	HYBRIDODPSCLUSTER-A-2	BCCDTCENTERAPITESTCRE	25.24 M	8.41 M	2157	8	ALIYUN$[redacted]	2019-03-05 00:10:41
algo_market	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$[redacted]	2019-06-21 00:06:14

Example:



Quick Search: cn-[redacted] admin_task_p

Filter

Refresh

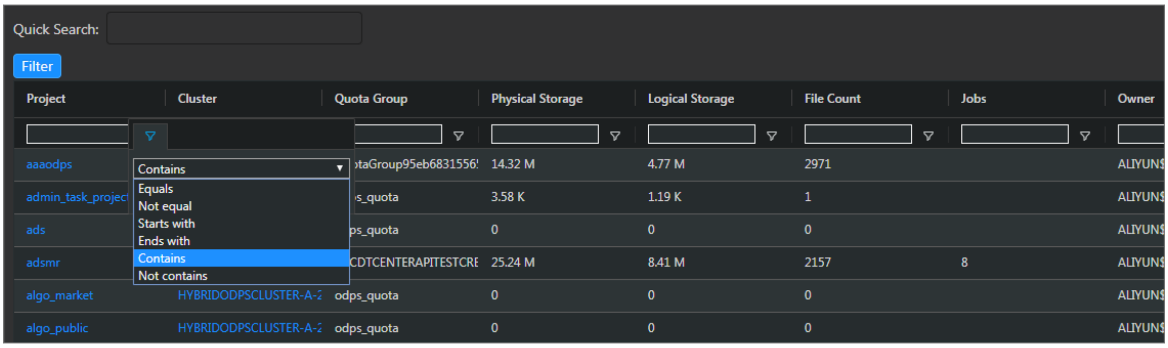
Project	Cluster	Quota Group	Physical Storage	Logical Storage	File Count	Jobs	Owner	Created At	Description	Actions
admin_task_project	HYBRIDODPSCLUSTER-A-2	odps_quota	3.58 K	1.19 K	1		ALIYUN$[redacted]	2019-03-05 00:03:47		Modify Copy-Resource

1 to 1 of 1

Filter projects

You can set filter conditions for multiple columns at the same time to quickly filter the projects you want.

1. On the **MaxCompute** page, click **O&M** in the upper-right corner, and then click the **Business** tab. The **Project List** page under **Projects** appears.
2. On the **Project List** page, click **Filter** in the upper-left corner of the list. A field for setting filter conditions appears for each column.
3. Click the icon next to each field for setting filter conditions and select the filtering method. The default method is **Contains**.



Quick Search:

Filter

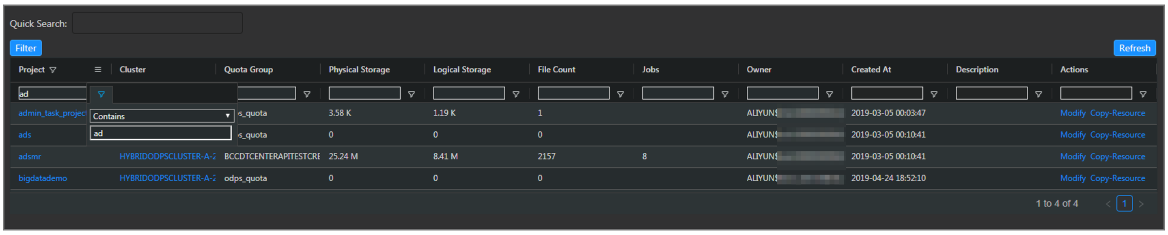
Project	Cluster	Quota Group	Physical Storage	Logical Storage	File Count	Jobs	Owner
aaaodps		ıtaGroup95eb6831556!	14.32 M	4.77 M	2971		ALIYUN$
admin_task_project		s_quota	3.58 K	1.19 K	1		ALIYUN$
ads		ps_quota	0	0	0		ALIYUN$
adsmr		CDTCENTERAPITESTCRE	25.24 M	8.41 M	2157	8	ALIYUN$
algo_market	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$
algo_public	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$

Optional filtering methods include:

- **Equals**
- **Not equal**
- **Starts with**
- **Ends with**
- **Contains**

  - ○ **Not contains**

4. After selecting the filtering method, enter the filter condition. The projects that meet the filter condition are automatically filtered.



Quick Search:

Filter

Refresh

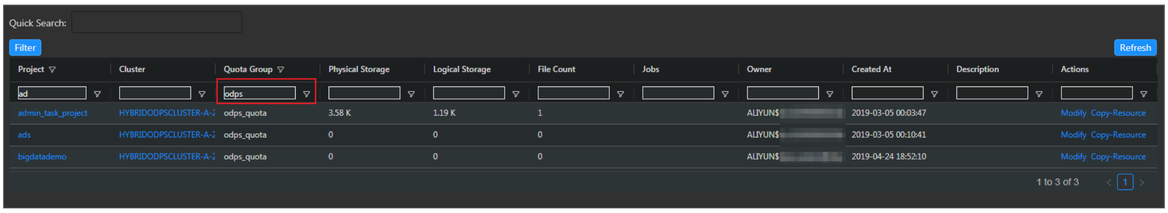
Project	Cluster	Quota Group	Physical Storage	Logical Storage	File Count	Jobs	Owner	Created At	Description	Actions
ad										
admin_task_project		s_quota	3.58 K	1.19 K	1		ALIYUN$[redacted]	2019-03-05 00:03:47		Modify Copy-Resource
ads		s_quota	0	0	0		ALIYUN$[redacted]	2019-03-05 00:10:41		Modify Copy-Resource
adsmr	HYBRIDODPSCLUSTER-A-2	BCCDTCENTERAPITESTCRE	25.24 M	8.41 M	2157	8	ALIYUN$[redacted]	2019-03-05 00:10:41		Modify Copy-Resource
bigdatademo	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$[redacted]	2019-04-24 18:52:10		Modify Copy-Resource

Contains

ad

1 to 4 of 4 < 1 >

5. If the filtering result is not accurate, you can continue performing this operation on other columns.



Quick Search:

Filter

Refresh

Project	Cluster	Quota Group	Physical Storage	Logical Storage	File Count	Jobs	Owner	Created At	Description	Actions
ad		odps								
admin_task_project	HYBRIDODPSCLUSTER-A-2	odps_quota	3.58 K	1.19 K	1		ALIYUN$[redacted]	2019-03-05 00:03:47		Modify Copy-Resource
ads	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$[redacted]	2019-03-05 00:10:41		Modify Copy-Resource
bigdatademo	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$[redacted]	2019-04-24 18:52:10		Modify Copy-Resource

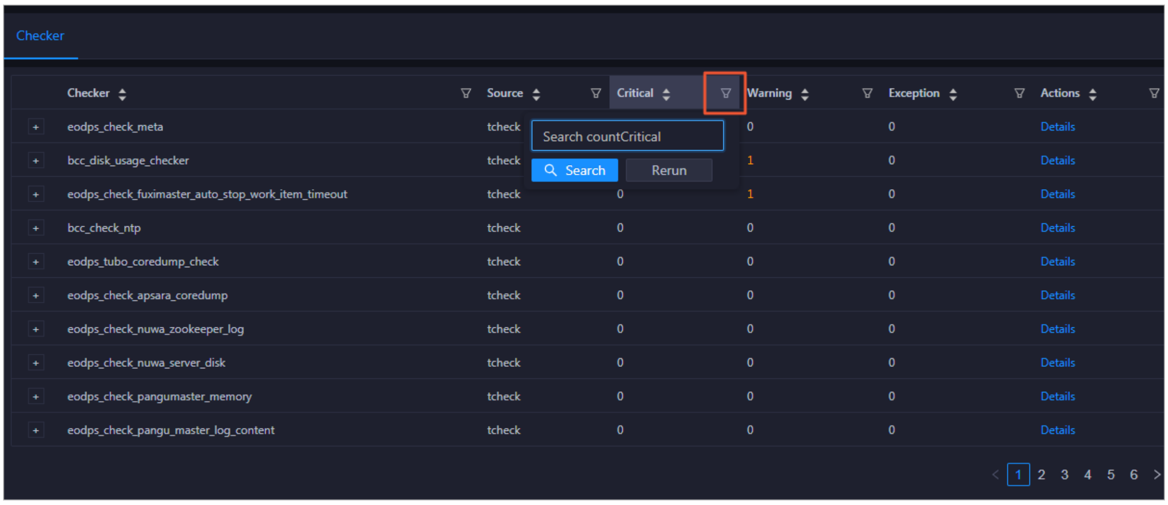
1 to 3 of 3 < 1 >

After you set the filter conditions for the projects, the **Filter** button is highlighted. If you need to cancel filtering, click the highlighted **Filter** button.

Search for items

You can search for items in a table by column, which is similar to filtering projects. For example, follow these steps to search for a checker:

1. On the **MaxCompute** page, click **O&M** in the upper-right corner, and then click the **Clusters** tab. On the Clusters page, click the **Health Status** tab.
2. In the checker list, click the **Filter** icon in a column, and enter a keyword in the search box.



Checker

	Checker	Source	Critical	Warning	Exception	Actions
+	eodps_check_meta	tcheck		0	0	Details
+	bcc_disk_usage_checker	tcheck		1	0	Details
+	eodps_check_fuximaster_auto_stop_work_item_timeout	tcheck	0	1	0	Details
+	bcc_check_ntp	tcheck	0	0	0	Details
+	eodps_tubo_coredump_check	tcheck	0	0	0	Details
+	eodps_check_apsara_coredump	tcheck	0	0	0	Details
+	eodps_check_nuwa_zookeeper_log	tcheck	0	0	0	Details
+	eodps_check_nuwa_server_disk	tcheck	0	0	0	Details
+	eodps_check_pangumaster_memory	tcheck	0	0	0	Details
+	eodps_check_pangu_master_log_content	tcheck	0	0	0	Details

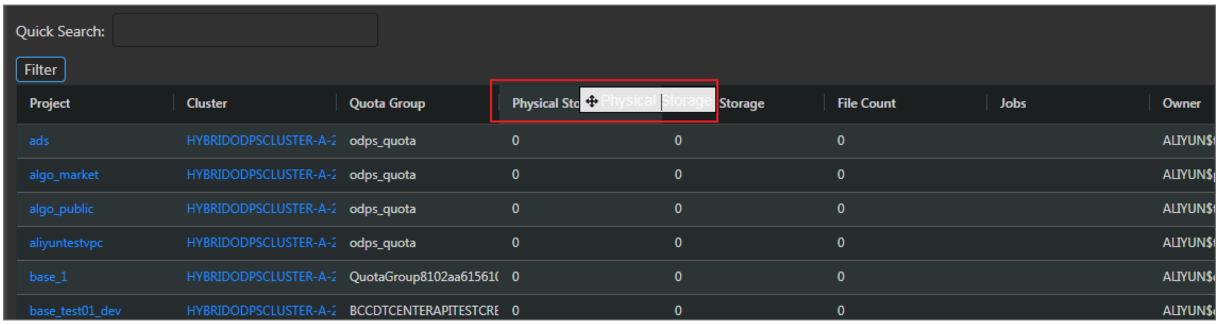
Search countCritical

3. Click **Search**. The checkers that meet the requirements appear.
4. If the search result is not accurate, you can continue performing this operation on other columns.

Customize a column

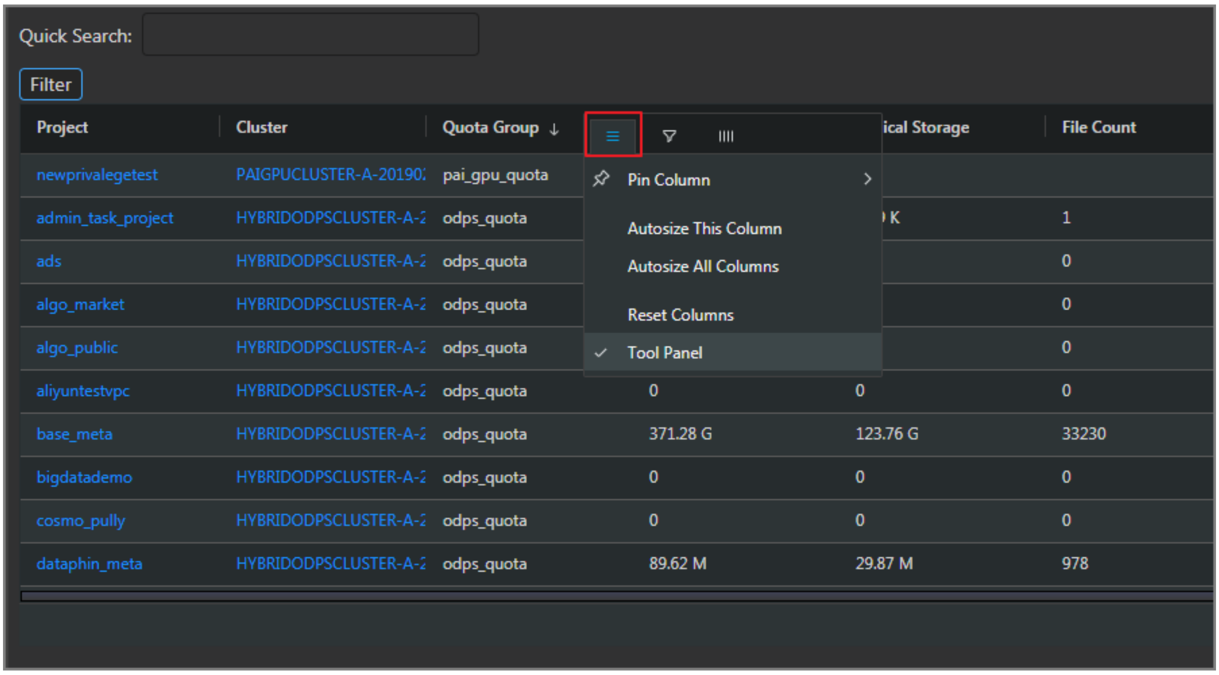
You can customize columns in the list. For example, you can set the column position or column width, and determine whether to display a column. You can also set filter conditions for columns.

On the **Project List** page, you can drag a column to change its position.



Project	Cluster	Quota Group	Physical Sto	Storage	File Count	Jobs	Owner
ads	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$
algo_market	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$
algo_public	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$
aliyuntestvpc	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$
base_1	HYBRIDODPSCLUSTER-A-2	QuotaGroup8102aa61561(	0	0	0		ALIYUN$
base_test01_dev	HYBRIDODPSCLUSTER-A-2	BCCDTCENTERAPITESTCRE	0	0	0		ALIYUN$

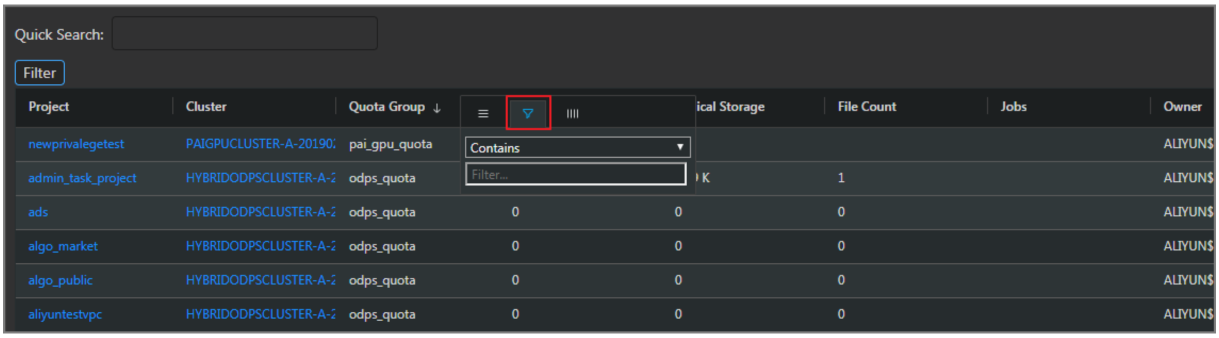
You can click ≡ in a column heading to customize the column.



Project	Cluster	Quota Group ↓		ical Storage	File Count
newprivalegetest	PAIGPUCLUSTER-A-20190:	pai_gpu_quota			
admin_task_project	HYBRIDODPSCLUSTER-A-2	odps_quota		K	1
ads	HYBRIDODPSCLUSTER-A-2	odps_quota			0
algo_market	HYBRIDODPSCLUSTER-A-2	odps_quota			0
algo_public	HYBRIDODPSCLUSTER-A-2	odps_quota			0
aliyuntestvpc	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
base_meta	HYBRIDODPSCLUSTER-A-2	odps_quota	371.28 G	123.76 G	33230
bigdatademo	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
cosmo_pully	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
dataphin_meta	HYBRIDODPSCLUSTER-A-2	odps_quota	89.62 M	29.87 M	978

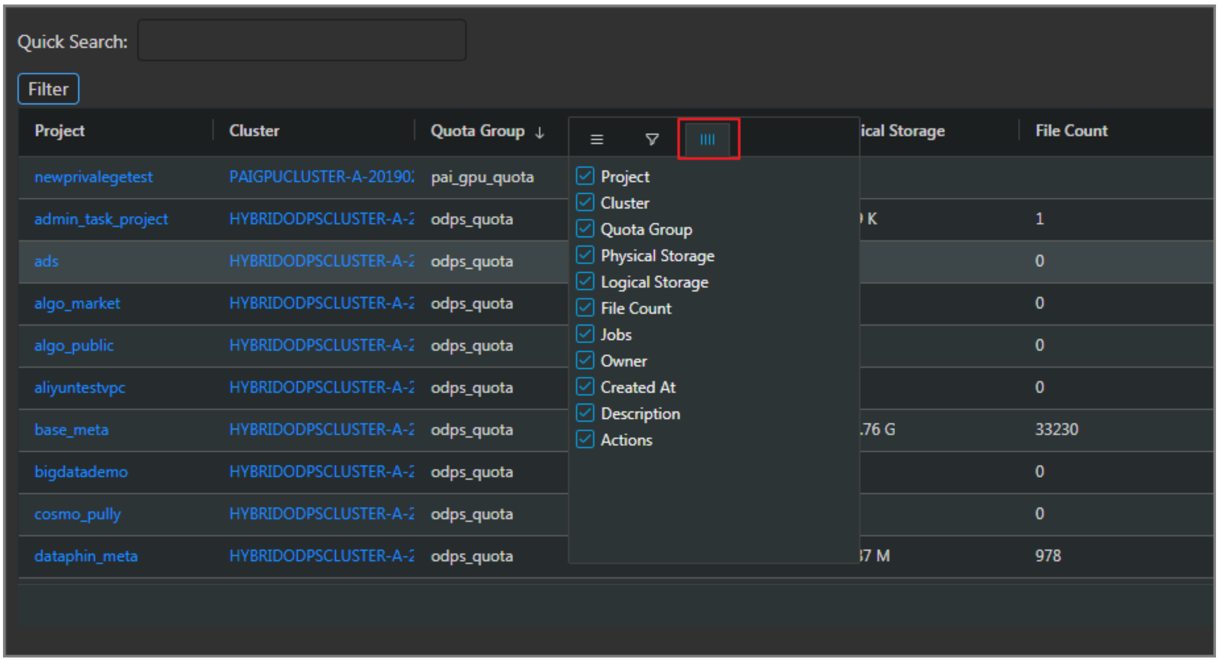
- **Pin Column**: allows you to fix a column to the rightmost or leftmost of the list. Unless being pinned, a column appears at the default position.
- **Autosize This Column**: allows you to adjust the width of a column automatically.
- **Autosize All Columns**: allows you to adjust the width of all columns automatically.
- **Reset Columns**: allows you to reset a column to its initial status.
- **Tool Panel**:

Click ▽ in a column heading and set a filter condition to filter projects based on the column.



Project	Cluster	Quota Group ↓		ical Storage	File Count	Jobs	Owner
newprivalegetest	PAIGPUCLUSTER-A-20190:	pai_gpu_quota					ALIYUN$
admin_task_project	HYBRIDODPSCLUSTER-A-2	odps_quota		K	1		ALIYUN$
ads	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$
algo_market	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$
algo_public	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$
aliyuntestvpc	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0		ALIYUN$

Click ▥ in a column heading and select the columns to be displayed.



Quick Search:

Filter

Project	Cluster	Quota Group ↓	ical Storage	File Count
newprivalegetest	PAIGPUCLUSTER-A-20190:	pai_gpu_quota		
admin_task_project	HYBRIDODPSCLUSTER-A-2	odps_quota	) K	1
ads	HYBRIDODPSCLUSTER-A-2	odps_quota		0
algo_market	HYBRIDODPSCLUSTER-A-2	odps_quota		0
algo_public	HYBRIDODPSCLUSTER-A-2	odps_quota		0
aliyuntestvpc	HYBRIDODPSCLUSTER-A-2	odps_quota		0
base_meta	HYBRIDODPSCLUSTER-A-2	odps_quota	.76 G	33230
bigdatademo	HYBRIDODPSCLUSTER-A-2	odps_quota		0
cosmo_pully	HYBRIDODPSCLUSTER-A-2	odps_quota		0
dataphin_meta	HYBRIDODPSCLUSTER-A-2	odps_quota	7 M	978

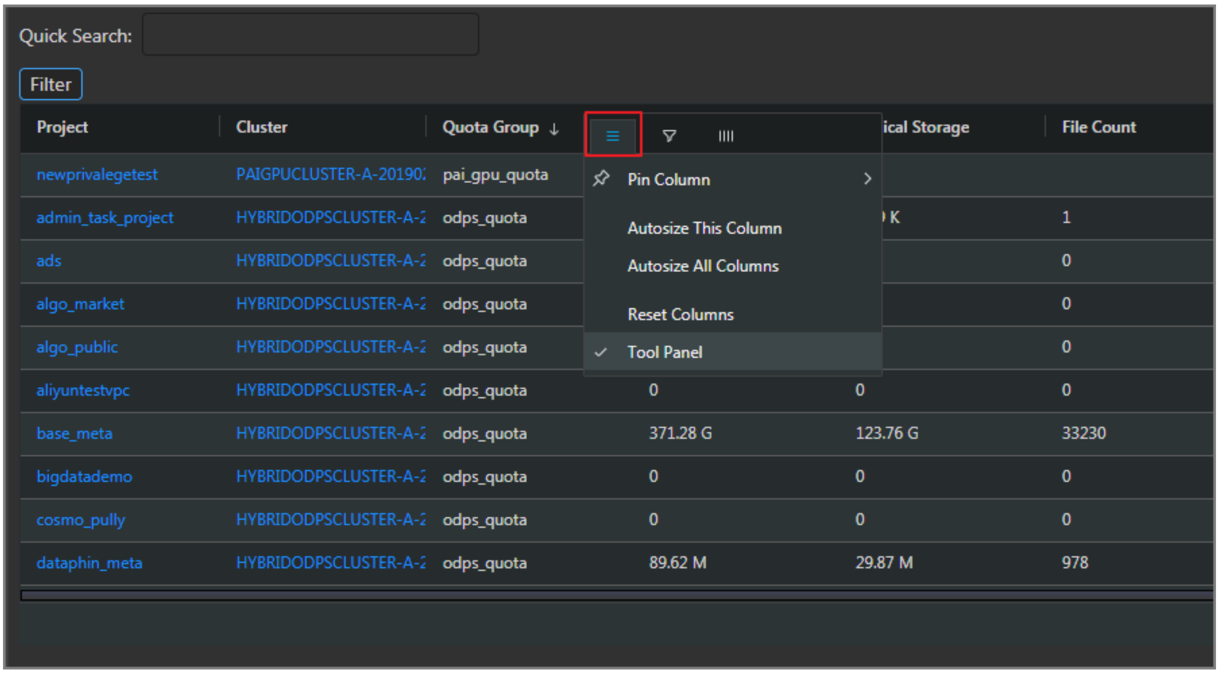
- ☑ Project
- ☑ Cluster
- ☑ Quota Group
- ☑ Physical Storage
- ☑ Logical Storage
- ☑ File Count
- ☑ Jobs
- ☑ Owner
- ☑ Created At
- ☑ Description
- ☑ Actions

If you select the check box of a column name, the column appears. Otherwise, the column is hidden.

Show the tool panel

After the tool panel appears, it is attached to the right of the list so that you can quickly set the columns to be displayed.

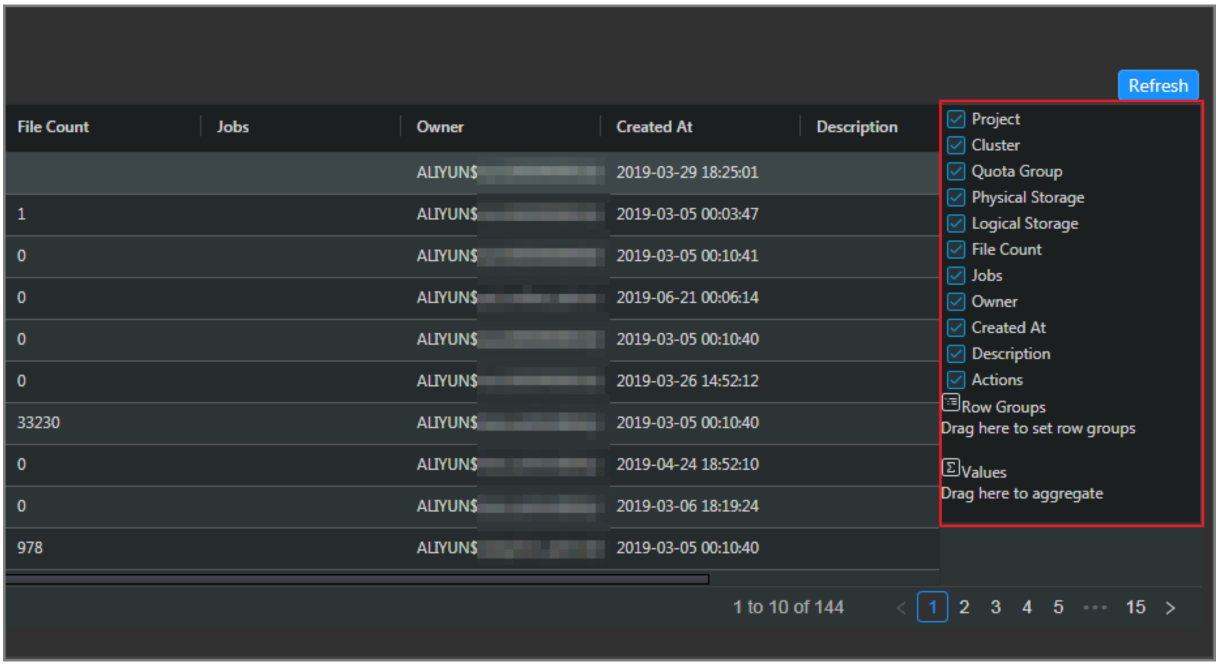
On the **Project List** page, click ☰ in a column heading and then select **Tool Panel**. The tool panel is then attached to the right of the list.



Quick Search:

Filter

Project	Cluster	Quota Group ↓		ical Storage	File Count
newprivalegetest	PAIGPUCLUSTER-A-20190:	pai_gpu_quota			
admin_task_project	HYBRIDODPSCLUSTER-A-2	odps_quota		) K	1
ads	HYBRIDODPSCLUSTER-A-2	odps_quota			0
algo_market	HYBRIDODPSCLUSTER-A-2	odps_quota			0
algo_public	HYBRIDODPSCLUSTER-A-2	odps_quota			0
aliyuntestvpc	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
base_meta	HYBRIDODPSCLUSTER-A-2	odps_quota	371.28 G	123.76 G	33230
bigdatademo	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
cosmo_pully	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
dataphin_meta	HYBRIDODPSCLUSTER-A-2	odps_quota	89.62 M	29.87 M	978



File Count	Jobs	Owner	Created At	Description
		ALIYUN$[redacted]	2019-03-29 18:25:01	
1		ALIYUN$[redacted]	2019-03-05 00:03:47	
0		ALIYUN$[redacted]	2019-03-05 00:10:41	
0		ALIYUN$[redacted]	2019-06-21 00:06:14	
0		ALIYUN$[redacted]	2019-03-05 00:10:40	
0		ALIYUN$[redacted]	2019-03-26 14:52:12	
33230		ALIYUN$[redacted]	2019-03-05 00:10:40	
0		ALIYUN$[redacted]	2019-04-24 18:52:10	
0		ALIYUN$[redacted]	2019-03-06 18:19:24	
978		ALIYUN$[redacted]	2019-03-05 00:10:40	

- ☑ Project
- ☑ Cluster
- ☑ Quota Group
- ☑ Physical Storage
- ☑ Logical Storage
- ☑ File Count
- ☑ Jobs
- ☑ Owner
- ☑ Created At
- ☑ Description
- ☑ Actions

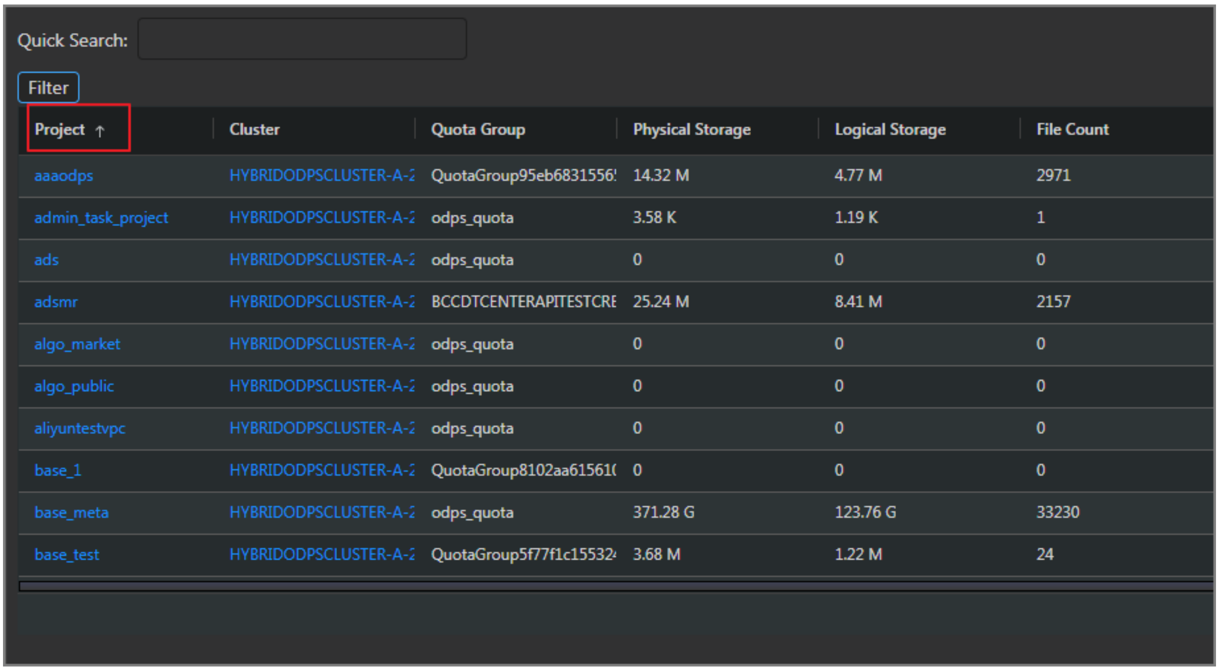
Row Groups
Drag here to set row groups

Σ Values
Drag here to aggregate

Sort projects based on a column

You can sort projects based on a column in ascending or descending order.

On the **Project List** page, click a column heading in the list. When you click the column heading for the first time, the projects are sorted based on the column in ascending order. When you click the column heading for the second time, the projects are sorted in descending order. When you click the column heading for the third time, the default sorting is restored.



Project ↑	Cluster	Quota Group	Physical Storage	Logical Storage	File Count
aaaodps	HYBRIDODPSCLUSTER-A-2	QuotaGroup95eb6831556	14.32 M	4.77 M	2971
admin_task_project	HYBRIDODPSCLUSTER-A-2	odps_quota	3.58 K	1.19 K	1
ads	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
adsmr	HYBRIDODPSCLUSTER-A-2	BCCDTCENTERAPITESTCRE	25.24 M	8.41 M	2157
algo_market	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
algo_public	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
aliyuntestvpc	HYBRIDODPSCLUSTER-A-2	odps_quota	0	0	0
base_1	HYBRIDODPSCLUSTER-A-2	QuotaGroup8102aa61561	0	0	0
base_meta	HYBRIDODPSCLUSTER-A-2	odps_quota	371.28 G	123.76 G	33230
base_test	HYBRIDODPSCLUSTER-A-2	QuotaGroup5f77f1c15532	3.68 M	1.22 M	24

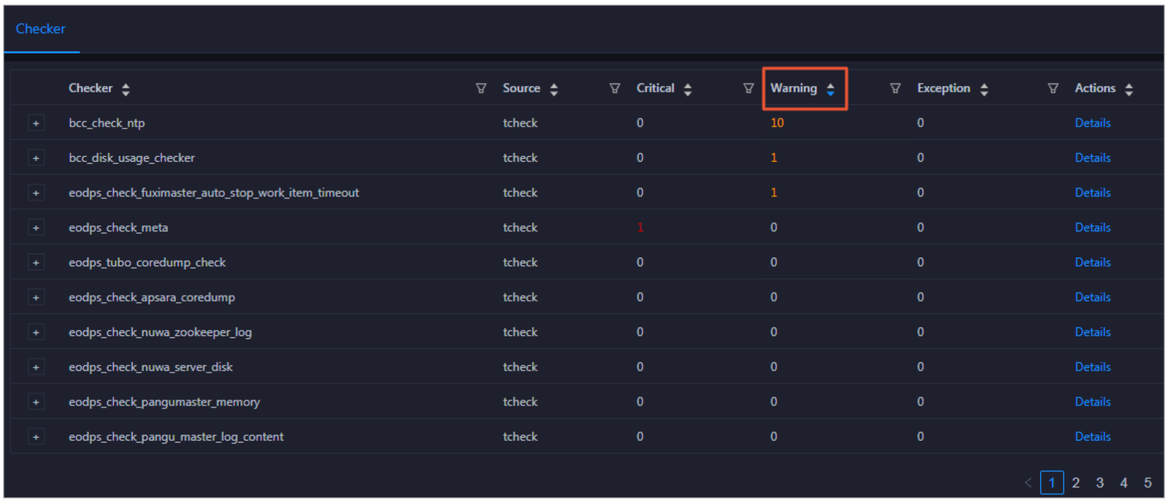
Sort items based on a column

You can sort items based on a column in ascending or descending order. The procedure and display method are different from those described in Sort projects based on a column.

1. On the **MaxCompute** page, click **O&M** in the upper-right corner, and then click the **Clusters** tab.

On the Clusters page, click the **Health Status** tab.

2. In the checker list, click a column heading or the Sort icon in the column heading to sort checkers in ascending order or descending order.



Checker

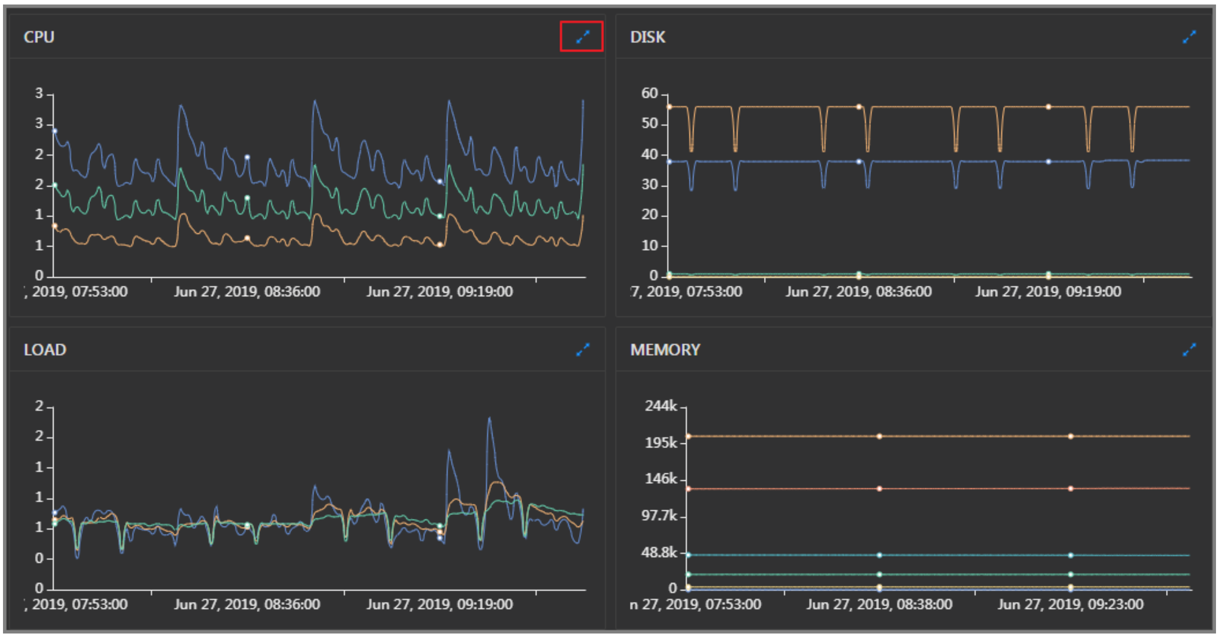
	Checker	Source	Critical	Warning	Exception	Actions
+	bcc_check_ntp	tcheck	0	10	0	Details
+	bcc_disk_usage_checker	tcheck	0	1	0	Details
+	eodps_check_fuximaster_auto_stop_work_item_timeout	tcheck	0	1	0	Details
+	eodps_check_meta	tcheck	1	0	0	Details
+	eodps_tubo_coredump_check	tcheck	0	0	0	Details
+	eodps_check_apsara_coredump	tcheck	0	0	0	Details
+	eodps_check_nuwa_zookeeper_log	tcheck	0	0	0	Details
+	eodps_check_nuwa_server_disk	tcheck	0	0	0	Details
+	eodps_check_pangumaster_memory	tcheck	0	0	0	Details
+	eodps_check_pangu_master_log_content	tcheck	0	0	0	Details

< 1 2 3 4 5

The highlighted up arrow indicates that the checkers are sorted in ascending order. The highlighted down arrow indicates that the checkers are sorted in descending order.

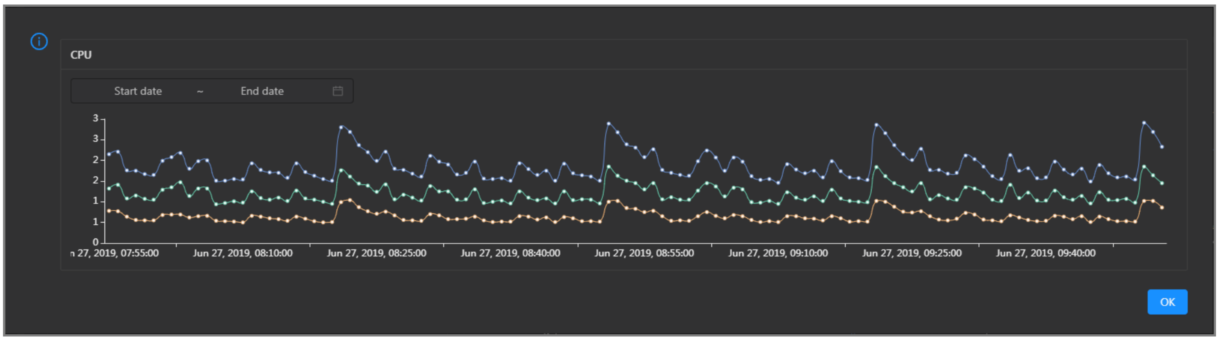
Trend chart 1

On the **MaxCompute** page, click **O&M** in the upper-right corner, and then click the **Clusters** tab. On the Clusters page, you can view relevant metrics, such as CPU and memory, of the selected cluster.



Take CPU as an example. The trend chart displays the trend lines of the total CPU usage (cpu), CPU usage for executing code in kernel space (sys), and CPU usage for executing code in user space (user) for the specified cluster over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU usage of the cluster in the specified period.

11.9.4.3. DataHub O&M overview

This topic describes the features of DataHub O&M and how to go to the DataHub O&M page.

Modules and features

DataHub O&M includes the business O&M, service O&M, cluster O&M, and host O&M modules. The following table describes the submodules and features contained in each module.

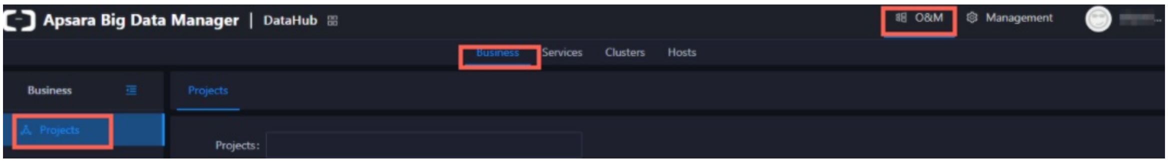
Module	Submodule or feature		Description
Business O&M	Projects		Displays the name, owner, the number of topics, read traffic, write traffic, storage usage of each project, and the time when a project was created.
	Topics		Displays the name, number of shards, storage usage, read traffic, and write traffic of each topic, the name of the project to which a topic belongs, and the time when a topic was created.
	Hotspot Analysis		Displays the distribution of shards on the hosts of a cluster for you to perform hotspot analysis.
	Fuxi	Overview	Displays the key operation metrics of Job Scheduler, including the service overview, service status, health check result, health check history, resource usage, and overview of compute nodes. You can also view the trend charts of CPU and memory usage on this page.
		Instances	Displays the information about the Job Scheduler service roles, including the name, host, IP address, and status of a service role, and host status.
		Health Status	Displays the information about the checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts. In addition, you can log on to a host and perform manual checks on the host.

Module	Submodule or feature		Description
Service O&M		Compute Nodes	Displays the information about compute nodes of a cluster, including the total CPU, idle CPU, total memory, and idle memory of each compute node. You can also check whether a node is added to the blacklist and whether it is active. In addition, you can add compute nodes to or remove compute nodes from the blacklist or read-only list on the Compute Nodes page.
	Pangu	Overview	Displays the key operation metrics of Apsara Distributed File System, including the service overview, service status, health check result, health check history, storage usage, and overview of storage nodes. You can also view the trend charts of storage usage and file count on this page.
		Instances	Displays the information about the Apsara Distributed File System service roles, including the name, host, IP address, and status of a service role, and host status.
		Health Status	Displays the information about the checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts. In addition, you can log on to a host and perform manual checks on the host.
		Storage Nodes	Displays the information about the storage nodes of Apsara Distributed File System, including the total storage size, available storage size, status, TTL, and send buffer size. You can also set the status of storage nodes and data disks on this page.
Clusters	Overview		Displays the overall running information about a cluster, including the host status, service status, health check result, and health check history. You can also view the trend charts of CPU usage, disk usage, memory usage, load, and packet transmission.
	Health Status		Displays the information about the checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts. In addition, you can log on to a host and perform manual checks on the host.
	Hosts		Displays the information about all hosts in a cluster, including the CPU usage, memory usage, root disk usage, packet loss rate, and packet error rate.
	Scale in Cluster and Scale out Cluster operations		Allow you to scale in or out a DataHub cluster by removing or adding physical hosts.

Module	Submodule or feature	Description
	Delete Topic from Smoke Testing operation	Allows you to delete topics from a DataHub test project and view the execution history.
	Reverse Parse Request ID operation	Allows you to reverse parse RequestId to obtain the time when a job was run and the IP address of the host. You can use the obtained information to query logs for troubleshooting.
Hosts	Overview	Displays the overall running information about a host in a DataHub cluster. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.
	Charts	Displays the enlarged trend charts of CPU usage, memory usage, storage usage, load, and packet transmission of a host.
	Health Status	Displays the information about the checkers of a host, including the checker details, check results, and schemes to clear alerts. In addition, you can log on to the host and perform manual checks on the host.
	Services	Displays the information about service instances and service roles of a host.

DataHub O&M entry

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataHub**.
3. On the DataHub page, click **O&M** in the upper-right corner. The **Business** tab appears.



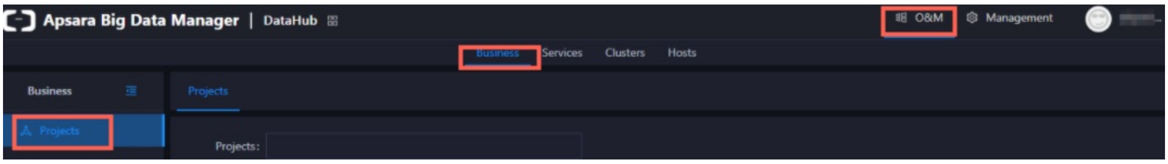
The **O&M** page includes four modules, namely, **Business**, **Services**, **Clusters**, and **Hosts**.

11.9.4.4. Business O&M

11.9.4.4.1. Business O&M

This topic describes how to go to the business O&M page for DataHub in the Apsara Big Data Manager console.

1. Log on to the Apsara Big Data Manager console.
2. Click the ⊞ icon in the upper-left corner, and then click **DataHub**.
3. On the DataHub page, click **O&M** in the upper-right corner, and then click the **Business** tab. The **Projects** page appears.



11.9.4.4.2. Projects

The Projects page displays the name, owner, number of topics, read traffic, write traffic, storage, and creation time of each project.

Go to the Projects page

On the **Business** tab, click **Projects** in the left-side navigation pane to view the information of all projects.

View project overview

On the **Projects** page, click the name of a project that you want to view. The **Overview** tab for the project appears.

View topics of a project

On the **Projects** page, click the name of a project that you want to view. On the page that appears, click the **Topics** tab. On this tab, you can view the information of all topics in the project.

11.9.4.4.3. Topics

The topic list displays the name, project, number of shards, storage, read traffic, write traffic, and creation time of each topic.

View the topic list

On the **Business** tab, click **Topics** in the left-side navigation pane to view the topic list.

View the details of a topic

On the **List** page, click the name of the topic that you want to view. On the page that appears, you can view the number of shards, the time when the topic was created and modified, the current storage usage, the lifecycle, the type, and the description of the topic. You can also view more details about monitoring metrics, shards, subscriptions, DataConnectors, and schema.

The Metric, Shard, Subscriptions, DataConnector, and Schema tabs provide more details about the topic.

- Metric: On the **Metric** tab, you can view the throughput and latency of the topic in near real time.
- Shard: Shards are concurrent tunnels used for data transmission in the topic.

  On the Shard tab, you can view the ID, status, and active time of each shard.

- Subscriptions: The subscription feature allows you to save consumption offsets to the server and resume data consumption from a saved consumption offset.

  On the Subscriptions tab, you can view the ID, status, owner, and description of each subscription and the time when the subscription was modified.

- DataConnector: DataConnectors synchronize the streaming data from DataHub to other Apsara Stack services. You can configure a DataConnector so that the data you write to DataHub can be used in other Apsara Stack services.

  On the DataConnector tab, you can view the name, ID, owner, and status of each DataConnector, and the time when the DataConnector was created and modified.

- Schema: Schemas define the data types of fields.

  On the Schema tab, you can view the data type and name of each field.

Disable or enable a topic

When you view the topic information, you may find that the DataHub instance has abnormal traffic or its cluster resources are nearly full. In this case, you need to temporarily disable data read/write for abnormal topics and low-priority topics. When abnormal Meta requests increase, you also need to temporarily disable requests related to abnormal topics to ensure cluster stability.

In this case, you can click **Disable** in the Actions column. In the dialog box that appears, specify the topic that you want to disable. After you disable a topic, all requests for the topic trigger errors, including read and write requests.

After the issue is solved, you can click **Enable** in the Actions column to enable the topic. After the topic is enabled, you can use the topic again.

You can view the information in the Status column to check whether a topic is disabled or enabled. The off status indicates that the topic is disabled, and the on status indicates that the topic is enabled.

11.9.4.4.4. Hotspot analysis

The Hotspot Analysis page displays the distribution of shards on the servers of a cluster.

Go to the Hotspot Analysis page

On the **Business** tab, click **Hotspot Analysis** in the left-side navigation pane. On the Hotspot Analysis page, you can view the distribution of shards on the servers of a specific cluster in the column chart.

Refresh the column chart and filter the data

On the **Hotspot Analysis** page, you can click **Shards** to refresh the column chart. You can also set conditions in the list below the chart to filter the data.

qps indicates the number of machine-level requests per second in the cluster. If the qps of a server is high, the request quantity of this server may be higher than that of other servers. In this case, hot spots may exist.

Note

- If a cluster is running, at least four rows of data are displayed. This is because a cluster can contain a minimum of four servers.
- At least two qps values in the four rows are not N/A, that is, at least two of the four servers play Frontend roles. If the qps value of a server is N/A, the server plays the Chunckserver role. In this case, the server is not in a Frontend hybrid deployment or the server is not running.

11.9.4.4.5. Archiving latency

The Archiving Tasks page displays the latency during data archiving.

View the archiving tasks

On the **Business** tab, click **Archiving Latency** in the left-side navigation pane to view the archiving tasks.

View the archiving latency

On the **Archiving Tasks** page, the archiving latency of each topic is displayed in the min_done_time column.

For archived MaxCompute data (sink_type is sink_odps), if the time in the min_done_time column is more than 30 minutes later than the current time, check whether the task encounters exceptions.

For other archived data, if the time in the min_done_time column is more than 5 minutes later than the current time, check whether the task encounters exceptions.

You can click the **topic name** to go to the DataConnector tab on the **Topics** page. On this tab, you can view the detailed archive information and perform O&M.

11.9.4.5. Service O&M

11.9.4.5.1. Control Service O&M

The Overview page for the control service displays the overall running information about the service, including the service overview, service status, health check result, health check history, and trends of resource usage.

Go to the O&M page for the control service

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataHub**.
3. On the DataHub page, click **O&M** in the upper-right corner, and then click the **Services** tab.
4. On the **Services** tab, click **Manage Service** in the left-side navigation pane. The **Overview** page for the control service appears.

11.9.4.5.2. Service O&M for Job Scheduler

11.9.4.5.2.1. Job Scheduler O&M entry

This topic describes how to go to the service O&M page for Job Scheduler in DataHub in the ABM console.

1. Log on to the ABM console.
2. Click ▦ in the upper-left corner and select **DataHub**.
3. On the DataHub page, click **O&M** in the upper-right corner, and then click the **Services** tab.
4. On the **Services** tab, click **Fuxi** in the left-side navigation pane and select a cluster from the drop-down list. The **Overview** page for Job Scheduler appears.

11.9.4.5.2.2. Service overview

The Overview page displays the key operation metrics of Job Scheduler, including the service overview, service status, health check result, health check history, resource usage, and overview of compute nodes. You can also view the trend charts of CPU and memory usage on this page.

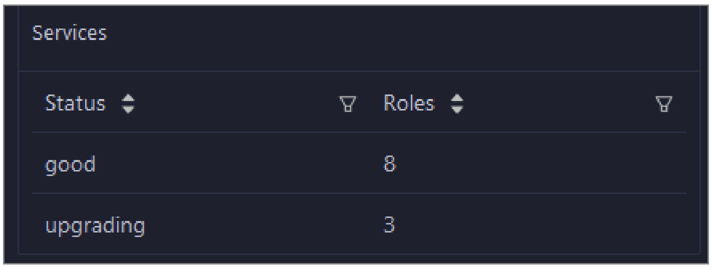
Go to the Overview page

1. On the **Services** tab, click **Fuxi** in the left-side navigation pane.
2. Select a cluster from the drop-down list and click the **Overview** tab. The **Overview** page for Job Scheduler appears.

   The **Overview** page displays the key operation metrics of Job Scheduler, including the service overview, service status, health check result, health check history, resource usage, and overview of compute nodes. You can also view the trend charts of CPU and memory usage on this page.

Services

This section shows the numbers of available services, unavailable services, and services that are being updated.

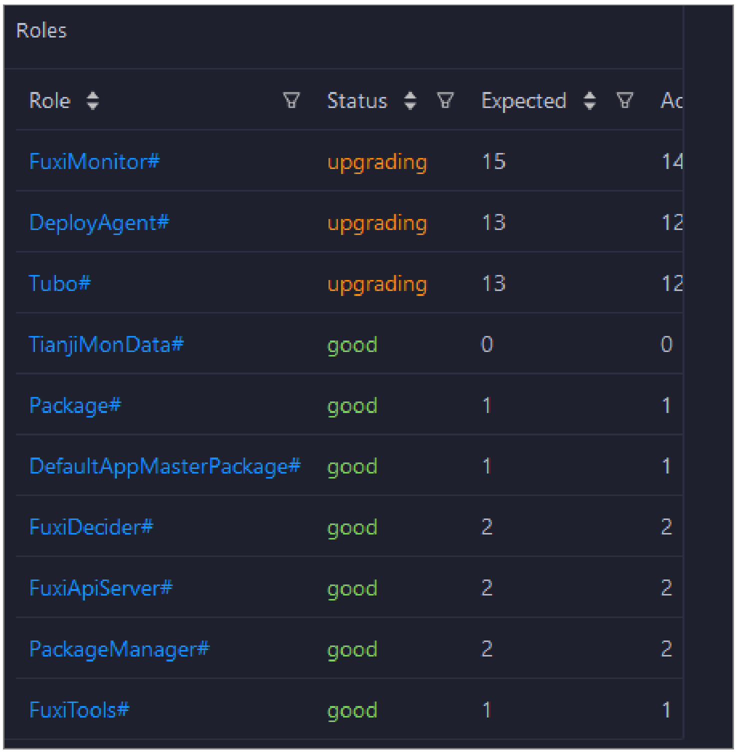


Services

Status	Roles
good	8
upgrading	3

Roles

This section shows all Job Scheduler server roles and their states. You can also view the expected and actual numbers of machines for each server role.



Roles

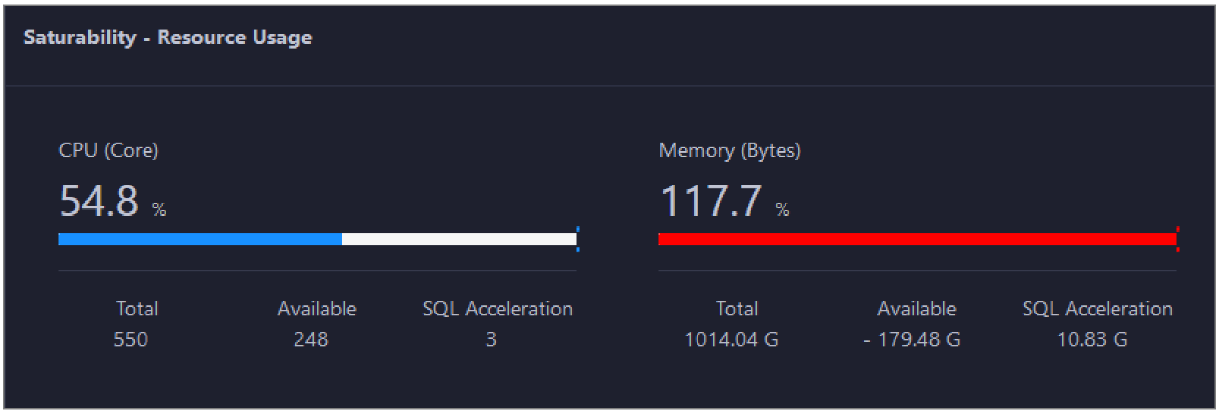
Role	Status	Expected	Ac
FuxiMonitor#	upgrading	15	14
DeployAgent#	upgrading	13	12
Tubo#	upgrading	13	12
TianjiMonData#	good	0	0
Package#	good	1	1
DefaultAppMasterPackage#	good	1	1
FuxiDecider#	good	2	2
FuxiApiServer#	good	2	2
PackageManager#	good	2	2
FuxiTools#	good	1	1

Click the name of a server role to go to the Apsara Infrastructure Management Framework console and view its details.

Saturability - Resource Usage

This section shows the allocation of CPU and memory resources.

- CPU (Core): shows the CPU utilization, the total number of CPU cores, the number of available CPU cores, and the CPU cores for SQL acceleration.
- Memory (Bytes): shows the memory usage, the total memory size, the available memory size, and the memory size for SQL acceleration.



Saturability - Resource Usage

CPU (Core)

54.8 %

Total	Available	SQL Acceleration
550	248	3

Memory (Bytes)

117.7 %

Total	Available	SQL Acceleration
1014.04 G	- 179.48 G	10.83 G

View the trend charts of CPU and memory usage

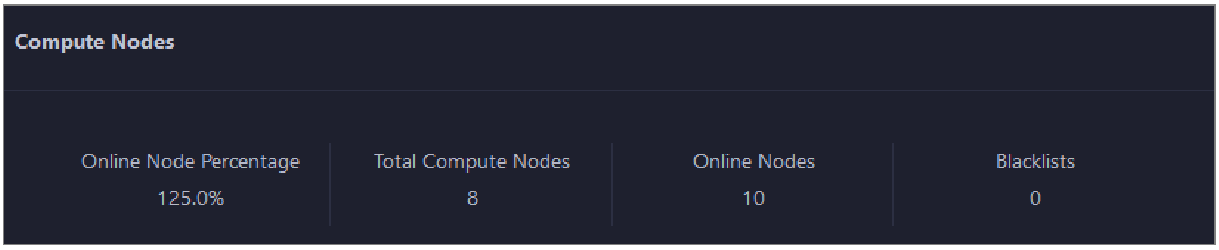
In the CPU Usage (1/100 Core) and Memory Usage (MB) sections, you can view the trend charts of CPU and memory usage of the selected cluster. Each trend chart displays the trend lines of the used quota, idle quota, and total quota of the relevant resource over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU usage of the cluster in the specified period.

Compute Nodes

This section shows the details of compute nodes in Job Scheduler. The details include the percentage of online compute nodes, the total number of compute nodes, the number of online compute nodes, and the number of compute nodes in a blacklist.



Compute Nodes

Online Node Percentage	Total Compute Nodes	Online Nodes	Blacklists
125.0%	8	10	0

11.9.4.5.2.3. Service instances

The Instances page displays information about the Job Scheduler service roles, including the name, host, IP address, and status of a service role, and host status.

1. On the **Services** page, click **Fuxi** in the left-side navigation pane.
2. Select a cluster from the drop-down list, and then click the **Instances** tab. The **Instances** page for Job Scheduler appears.

   On the **Instances** page, you can view information about the Job Scheduler service roles, including the name, host, IP address, and status of a service role, and host status.

11.9.4.5.2.4. Service health

On the Health Status page for Job Scheduler, you can view all checkers of Job Scheduler, including the checker details, check results, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Go to the Health Status page

1. On the **Services** tab, click **Fuxi** in the left-side navigation pane.
2. Select a cluster from the drop-down list and click the **Health Status** tab. The **Health Status** page for Job Scheduler appears.

   On the **Health Status** page, you can view all checkers of the Job Scheduler service and the check results for all hosts in the cluster. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

Supported operations

On the Health Status page, you can view the information about the checkers of a cluster, including the checker details, hosts with alerts and alert causes, and schemes to clear alerts. In addition, you can log on to a host and perform manual checks on the host. For more information, see Cluster health.

11.9.4.5.2.5. Compute nodes

You can view the details of compute nodes on the Compute Nodes page for Job Scheduler, including the total CPU, idle CPU, total memory, and idle memory of each compute node. You can also check whether a node is added to the blacklist and whether it is active. In addition, you can add compute nodes to or remove compute nodes from the blacklist or read-only list on the Compute Nodes page.

Go to the Compute Nodes page

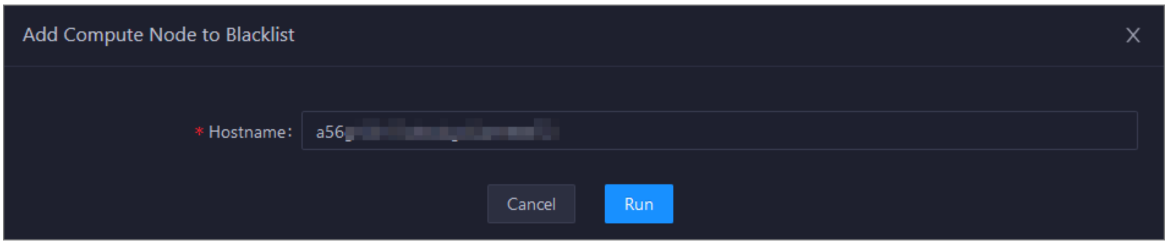
1. On the **Services** tab, click **Fuxi** in the left-side navigation pane.
2. Select a cluster from the drop-down list and click the **Compute Nodes** tab. The **Compute Nodes** page for Job Scheduler appears.

   On this page, you can view the details of compute nodes, including the total CPU, idle CPU, total memory, and idle memory of each compute node. You can also check whether a node is added to the blacklist and whether it is active.

Blacklist and read-only setting

You can add compute nodes to or remove compute nodes from the blacklist or read-only list. To add compute nodes to the blacklist, follow these steps:

1. On the **Compute Nodes** page, click **Actions** for the target compute node and then select **Add to Blacklist**.
2. In the dialog box that appears, click **Run**. A message appears, indicating that the action has been submitted.

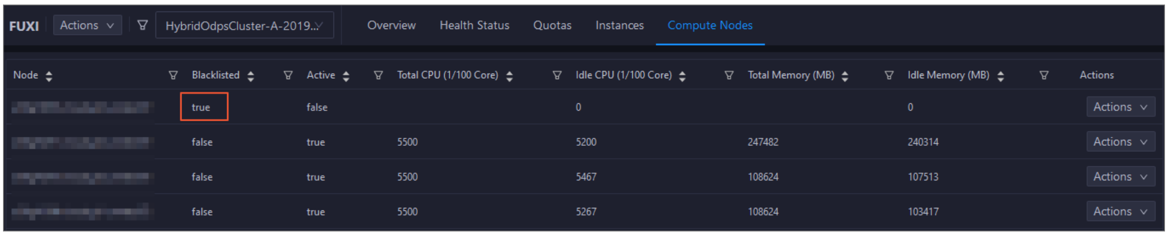
   

   Add Compute Node to Blacklist

   * Hostname: a56[redacted]

   The value of the **Hostname** parameter is automatically filled. You do not need to specify a value for this parameter.

   You can check whether a compute node is added to the blacklist in the compute node list after the configuration is completed.

Node	Blacklisted	Active	Total CPU (1/100 Core)	Idle CPU (1/100 Core)	Total Memory (MB)	Idle Memory (MB)	Actions
[redacted]	true	false		0		0	Actions
[redacted]	false	true	5500	5200	247482	240314	Actions
[redacted]	false	true	5500	5467	108624	107513	Actions
[redacted]	false	true	5500	5267	108624	103417	Actions

11.9.4.5.3. Service O&M for Apsara Distributed File System

11.9.4.5.3.1. Apsara Distributed File System O&M entry

This topic describes how to go to the service O&M page for Apsara Distributed File System in DataHub in the ABM console.

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataHub**.
3. On the DataHub page, click **O&M** in the upper-right corner, and then click the **Services** tab.
4. On the **Services** tab, click **Pangu** in the left-side navigation pane and select a cluster from the drop-down list. The **Overview** page for Apsara Distributed File System appears.

11.9.4.5.3.2. Service overview

The Overview tab shows the key operating information about Apsara Distributed File System. The information includes the service overview, service status, storage usage, storage node overview, and the trend charts of storage usage and file count.

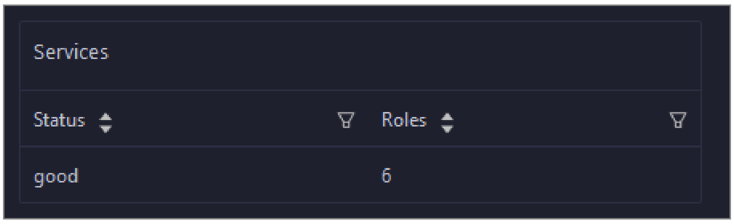
Go to the Overview page

1. On the **Services** tab, click **Pangu** in the left-side navigation pane.
2. Select a cluster from the drop-down list and click the **Overview** tab. The **Overview** page for Apsara Distributed File System appears.

   The **Overview** page displays the key operation metrics of Apsara Distributed File System, including the service overview, service status, health check result, health check history, storage usage, and overview of storage nodes. You can also view the trend charts of storage usage and file count on this page.

Services

This section shows the status of Apsara Distributed File System and the number of server roles.

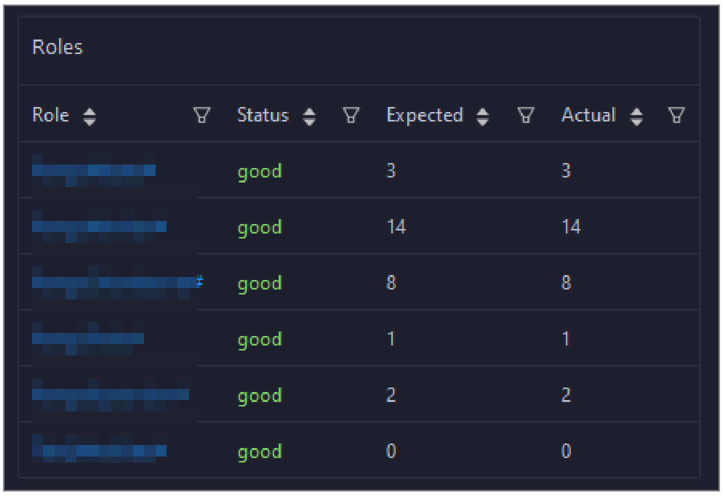


Services

Status	Roles
good	6

Roles

This section shows all server roles of Apsara Distributed File System and their states. You can also view the expected and actual numbers of hosts for each server role.



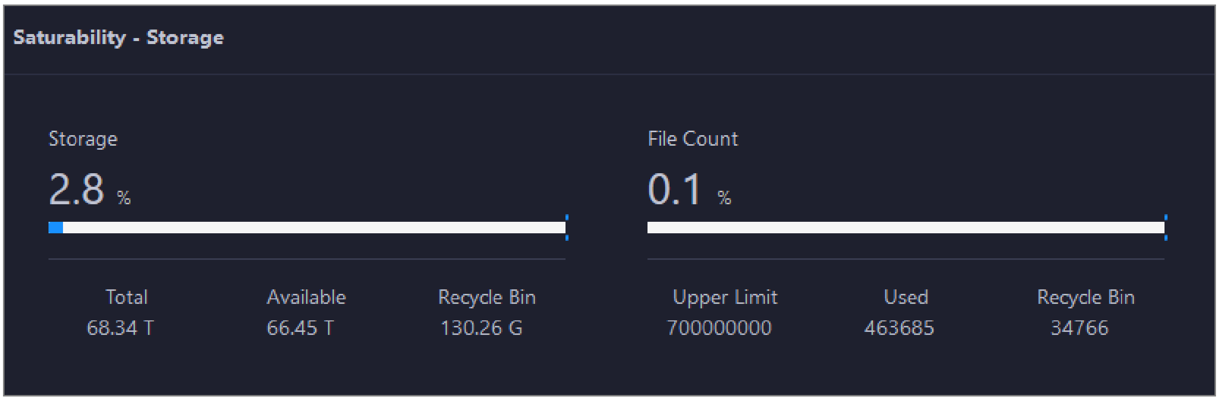
Roles

Role	Status	Expected	Actual
[redacted]	good	3	3
[redacted]	good	14	14
[redacted]	good	8	8
[redacted]	good	1	1
[redacted]	good	2	2
[redacted]	good	0	0

Saturability - Storage

This section shows the storage usage and file count.

- Storage: shows the storage usage, total storage space, available storage space, and recycle bin size.
- File Count: shows the file count usage, maximum number of files, number of existing files, and number of files in the recycle bin.



Saturability - Storage

Storage

2.8 %

Total	Available	Recycle Bin
68.34 T	66.45 T	130.26 G

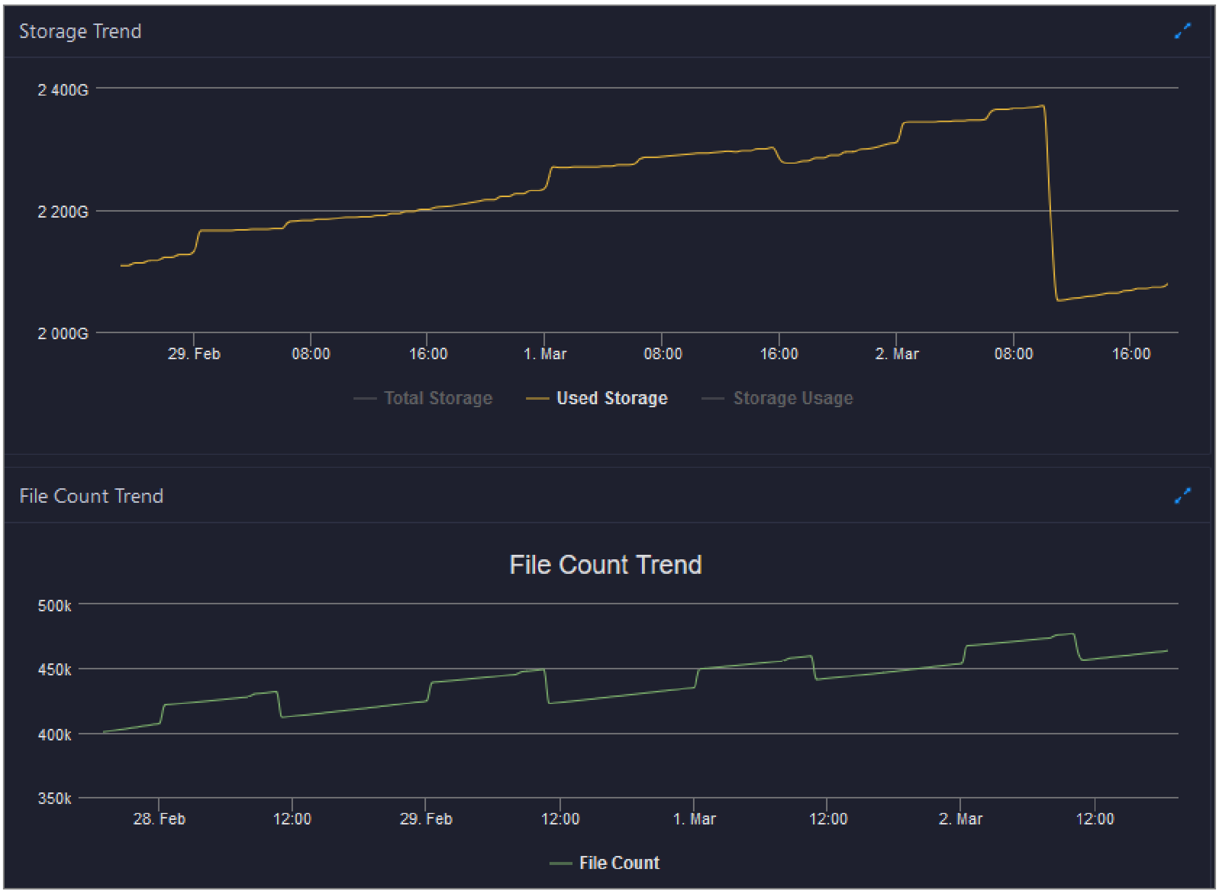
File Count

0.1 %

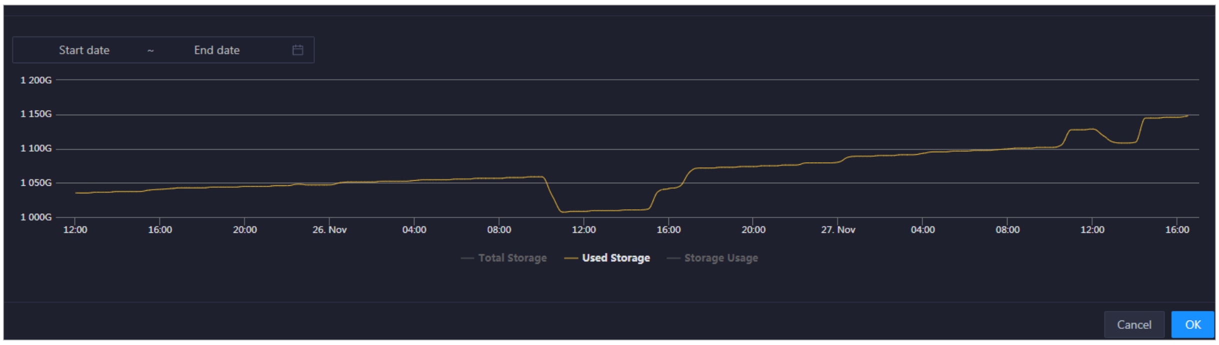
Upper Limit	Used	Recycle Bin
700000000	463685	34766

Storage Trend and File Count Trend

This section shows the trend charts of the storage usage and file count. The storage usage chart shows the trend lines of the total storage space, used storage space, and storage usage in different colors. The file count chart shows the trend line of the file count.



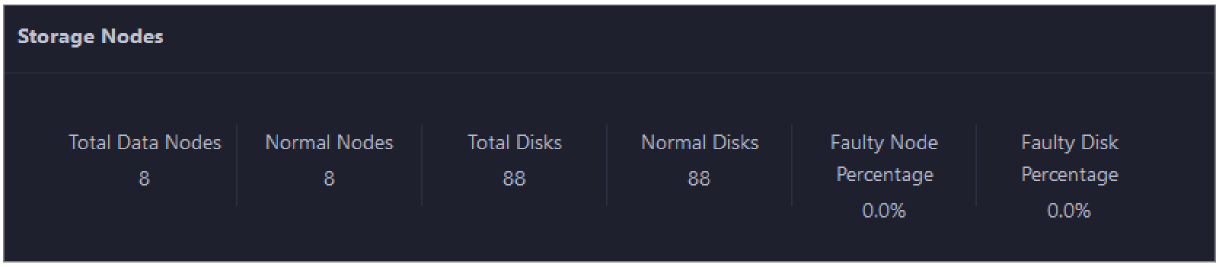
In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart. The following figure shows an enlarged chart of storage usage.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

Storage Nodes

This section shows information about the storage nodes of Apsara Distributed File System. The information includes the numbers of data nodes, normal nodes, disks, and normal disks. You can also view the faulty node percentage and faulty disk percentage.



Storage Nodes

Total Data Nodes	Normal Nodes	Total Disks	Normal Disks	Faulty Node Percentage	Faulty Disk Percentage
8	8	88	88	0.0%	0.0%

11.9.4.5.3.3. Service roles

The Instances page displays information about the Apsara Distributed File System service roles, including the name, host, IP address, and status of a service role, and host status.

Go to the Instances page

1. On the **Services** tab, click **Pangu** in the left-side navigation pane.
2. Select a cluster from the drop-down list and click the **Instances** tab. The **Instances** page for Apsara Distributed File System appears.

   On the **Instances** page, you can view information about the Apsara Distributed File System service roles, including the name, host, IP address, and status of a service role, and host status.

Supported operations

You can filter or sort service roles by column to facilitate information retrieval. For more information, see Common operations.

You can change the primary master node or run a checkpoint on a master node of Apsara Distributed File System. For more information, see Change the primary master node for Apsara Distributed File System and Run a checkpoint on the master nodes of Apsara Distributed File System.

11.9.4.5.3.4. Service health

On the Health Status page for Apsara Distributed File System, you can view all checkers of Apsara Distributed File System, including the checker details, check results, and schemes to clear alerts (if any). In addition, you can log on to a host and perform manual checks on the host.

Go to the Health Status page

1. On the **Services** tab, click **Pangu** in the left-side navigation pane.
2. Select a cluster from the drop-down list and click the **Health Status** tab. The **Health Status** page for Apsara Distributed File System appears.

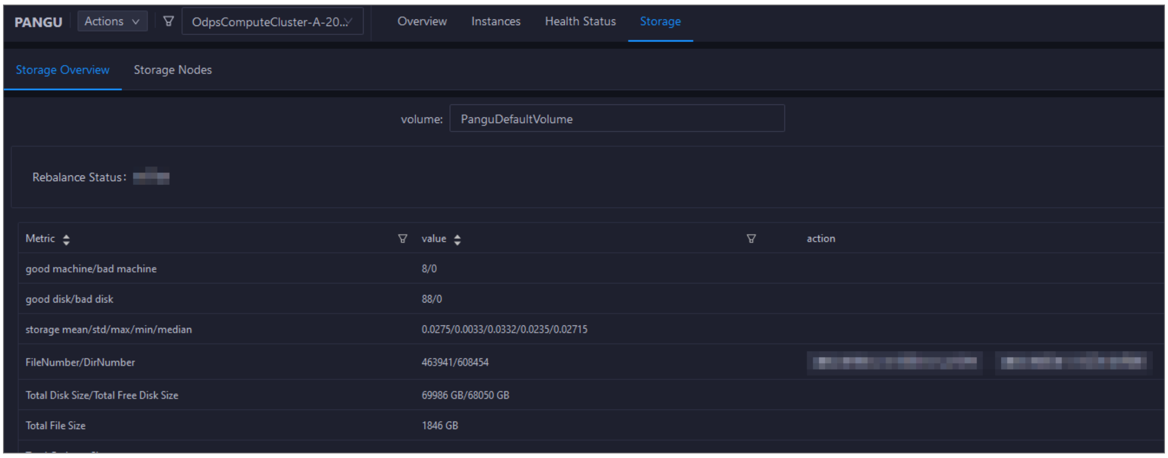
   On the **Health Status** page, you can view all checkers of Apsara Distributed File System and the check results for all hosts in the cluster. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

11.9.4.5.3.5. Storage nodes

This topic describes how to view the storage overview and storage node information of Apsara Distributed File System, and how to set the status of storage nodes and data disks.

Entry to the Storage Overview page

1. On the **Services** page, click **Pangu** in the left-side navigation pane.
2. Select a cluster from the drop-down list, and then click the **Storage** tab. The **Storage Overview** page for Apsara Distributed File System appears.



volume: PanguDefaultVolume

Rebalance Status: [redacted]

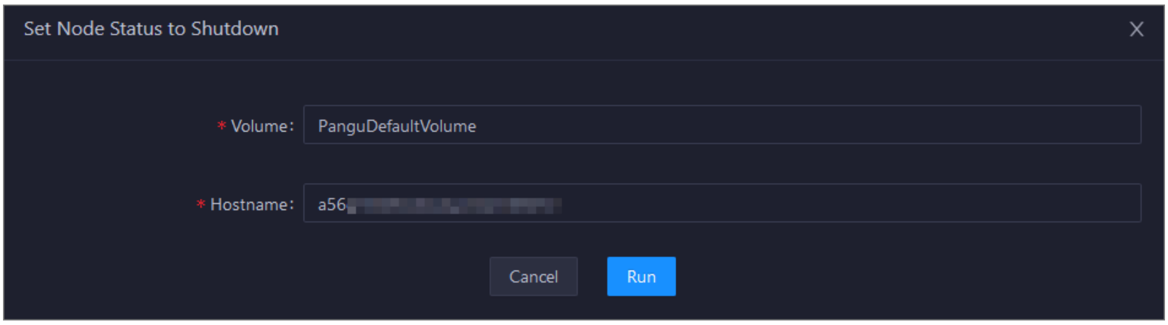
Metric	value	action
good machine/bad machine	8/0	
good disk/bad disk	88/0	
storage mean/std/max/min/median	0.0275/0.0033/0.0332/0.0235/0.02715	
FileNumber/DirNumber	463941/608454	[redacted] [redacted]
Total Disk Size/Total Free Disk Size	69986 GB/68050 GB	
Total File Size	1846 GB	

The **Storage Overview** page displays whether data rebalancing is enabled, key metrics and their values, suggestions to handle exceptions, and rack specifications of Apsara Distributed File System. The **Storage Nodes** page displays the information about all storage nodes of Apsara Distributed File System, including the total storage size, available storage size, status, time to live (TTL), and send buffer size. You can also set the status of storage nodes and data disks on this page.

Set the storage node status

You can set the storage node status to Disabled or Normal. This section describes how to set the status of a storage node to Disabled.

1. On the **Storage Nodes** page, find the target storage node and choose **Actions** > **Set Node Status to Disabled** in the Actions column.
2. In the dialog box that appears, click **Run**. A message appears, indicating that the action has been submitted.


Set Node Status to Shutdown

* Volume: PanguDefaultVolume

* Hostname: a56[redacted]

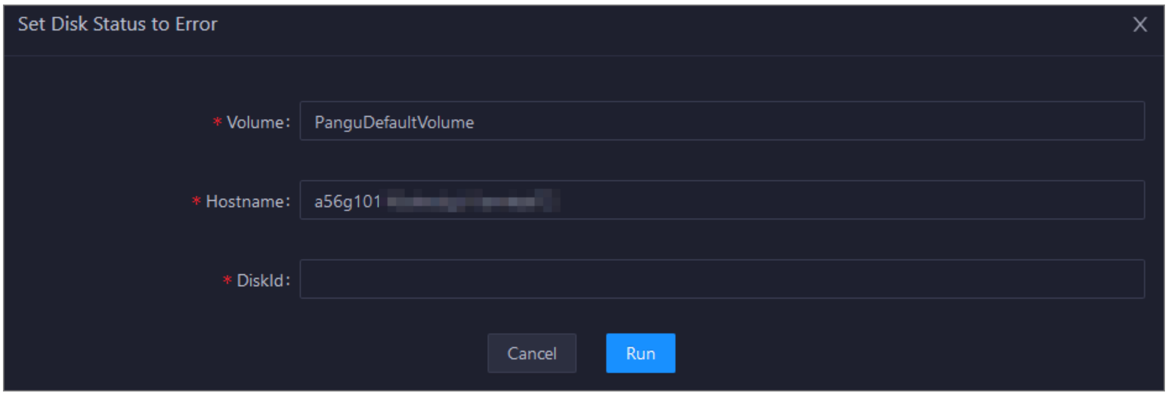
The values of the **Volume** and **Hostname** parameters are automatically filled based on the selected storage node. You do not need to specify values for the parameters.

You can check whether the status of storage node is changed in the storage node list.

Set the data disk status

You can set the data disk status to Error or Normal. This section describes how to set the status of a data disk to Error.

1. On the **Storage Nodes** page, find the target storage node and choose **Actions** > **Set Disk Status to Error** in the Actions column.
2. In the dialog box that appears, set the **Diskid** parameter.

   Set Disk Status to Error

   * Volume: PanguDefaultVolume

   * Hostname: a56g101 [redacted]

   * DiskId:

   The values of the **Volume** and **Hostname** parameters are automatically filled based on the selected storage node. You do not need to specify values for the parameters.
3. Click **Run**. A message appears, indicating that the action has been submitted.

11.9.4.5.3.6. Clear the recycle bin of Apsara Distributed File System

Apsara Big Data Manager (ABM) allows you to clear the recycle bin of Apsara Distributed File System to release storage space.

Prerequisites

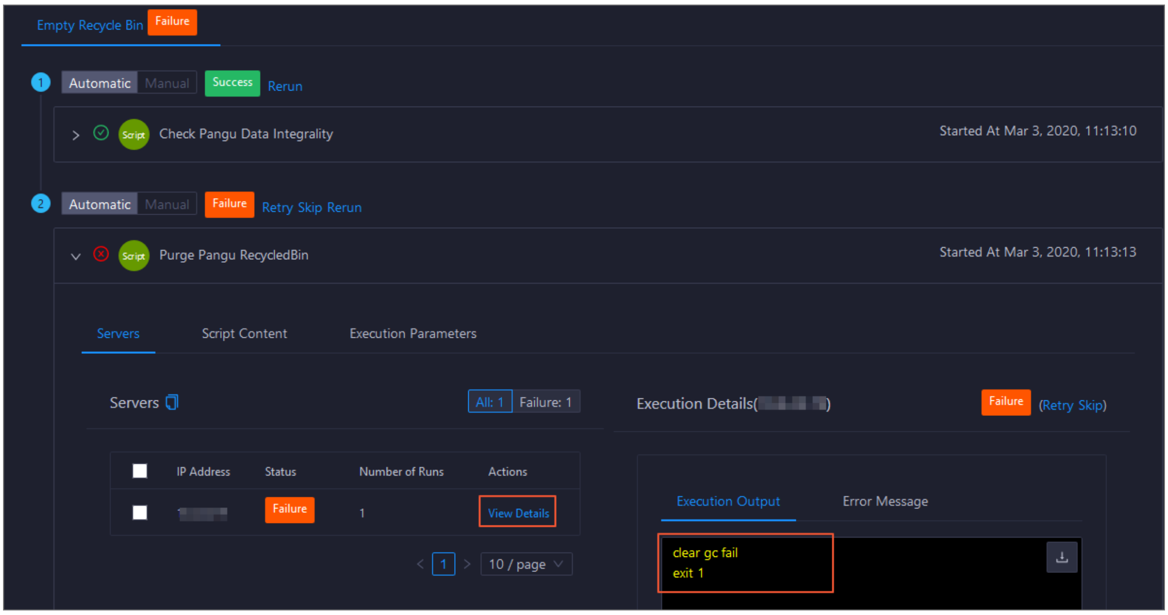
Your Apsara Big Data Manager account has the permission to manage DataHub.

Procedure

1. On the **Services** tab, click **Pangu** in the left-side navigation pane and select a cluster from the drop-down list. The **Overview** page for Apsara Distributed File System appears.
2. Choose **Actions** > **Empty Recycle Bin** in the upper-right corner.
3. In the right-side pane that appears, set the **volume** parameter. The default value is **PanguDefaultVolume**.
4. Click **Run**. A message appears, indicating that the request has been submitted.
5. View the execution status.

   Click **Actions** in the upper-right corner and select **Execution History** next to **Empty Recycle Bin**. In the right-side pane that appears, view the execution history.

   In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.
6. If the status is FAILED, click **Details** in the Details column to identify the cause of the failure.



Execution Details([redacted])

	IP Address	Status	Number of Runs	Actions
□	[redacted]	Failure	1	View Details

```
clear gc fail
exit 1
```

You can view information about parameter settings, host details, script, and runtime parameters to identify the cause of the failure.

11.9.4.5.3.7. Enable or disable data rebalancing for Apsara Distributed File System

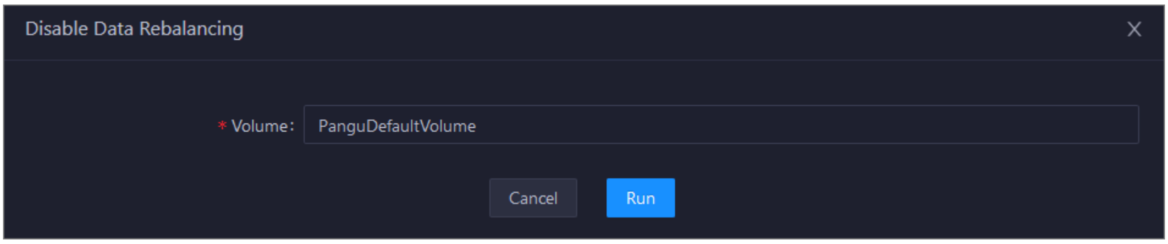
ABM allows you to enable or disable data rebalancing for Apsara Distributed File System.

Prerequisites

Your ABM account has the permission to manage DataHub.

Disable data rebalancing

1. On the **Services** tab, click **Pangu** in the left-side navigation pane and select a cluster from the drop-down list. The Overview page for Apsara Distributed File System appears.
2. Choose **Actions** > **Disable Data Rebalancing** in the upper-right corner.
3. In the right-side pane that appears, set the **volume** parameter. The default value is **PanguDefaultVolume**.



* Volume: PanguDefaultVolume

4. Click **Run**. A message appears, indicating that the request has been submitted.
5. View the execution status.

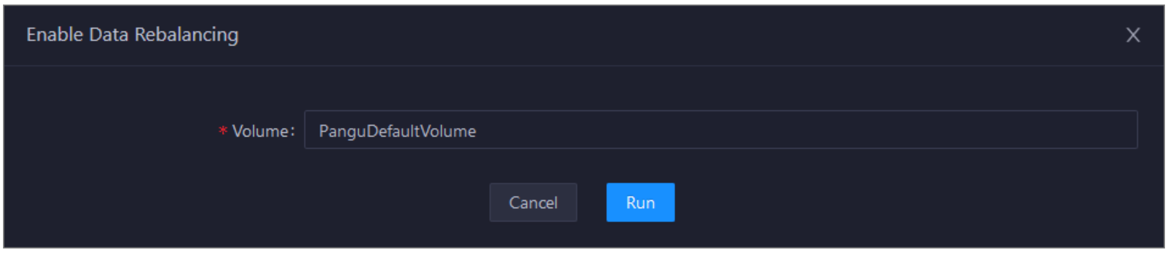
   Move the pointer over **Actions** in the upper-right corner and select **Execution History** next to **Disable Data Rebalancing**. In the right-side pane that appears, view the execution history.

In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.

6. If the status is FAILED, click **Details** in the Details column to locate the failure cause. For more information, see Locate the failure cause.

Enable data rebalancing

1. On the **Services** tab, click **Pangu** in the left-side navigation pane and select a cluster from the drop-down list. The Overview page for Apsara Distributed File System appears.
2. Choose **Actions** > **Enable Data Rebalancing** in the upper-right corner.
3. In the right-side pane that appears, set **volume**. The default value is **PanguDefaultVolume**.



Enable Data Rebalancing

* Volume: PanguDefaultVolume

4. Click **Run**. A message appears, indicating that the request has been submitted.
5. View the execution status.

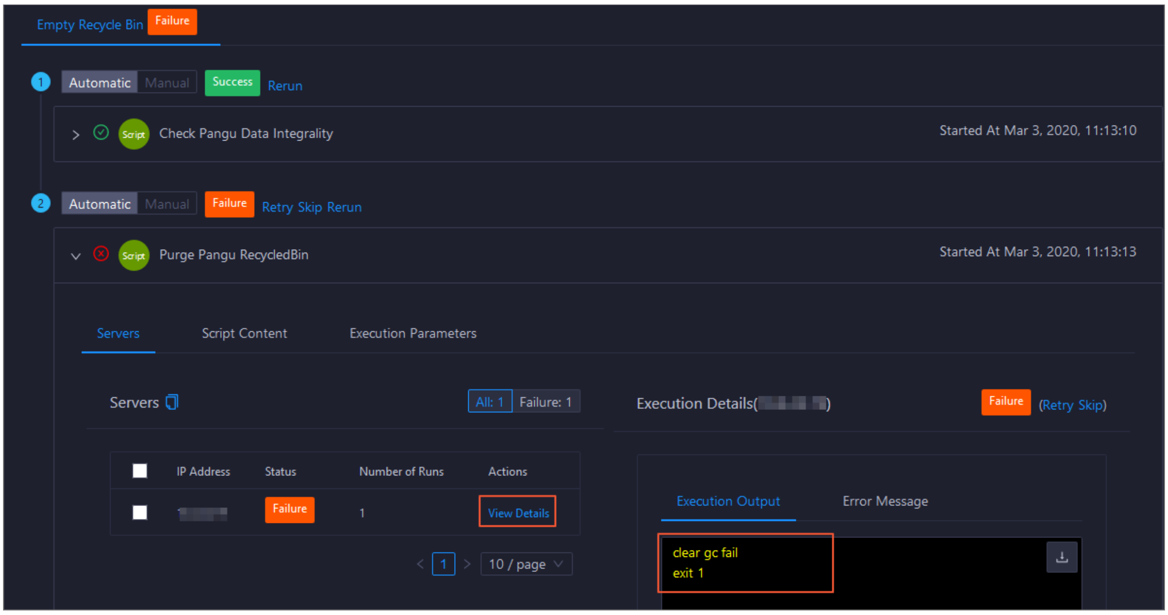
   Move the pointer over **Actions** in the upper-right corner and select **Execution History** next to **Enable Data Rebalancing**. In the right-side pane that appears, view the execution history.

   In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.
6. If the status is FAILED, click **Details** in the Details column to locate the failure cause. For more information, see Locate the failure cause.

Locate the failure cause

This section uses the procedure of locating the failure cause for enabling data reblancing as an example.

1. Find the target failed execution and click **Details** in the Details column.
2. In the right-side pane that appears, click **View Details** for a failed step to locate the failure cause.


Empty Recycle Bin Failure
1 Automatic Manual Success Rerun
Check Pangu Data Integrality
Started At Mar 3, 2020, 11:13:10
2 Automatic Manual Failure Retry Skip Rerun
Purge Pangu RecycledBin
Started At Mar 3, 2020, 11:13:13
Servers
Script Content
Execution Parameters
Servers
All: 1
Failure: 1
Execution Details([redacted])
Failure
(Retry Skip)
IP Address
Status
Number of Runs
Actions
[redacted]
Failure
1
View Details
1
10 / page
Execution Output
Error Message

```
clear gc fail
exit 1
```

You can also view information about parameter settings, host details, script, and execution parameters to locate the failure cause.

11.9.4.5.3.8. Run a checkpoint on master nodes of Apsara Distributed File System

ABM allows you to run checkpoints on master nodes of Apsara Distributed File System. This operation writes memory data to disks. When a failure occurs in Apsara Distributed File System, you can use checkpoints to restore data to the status before the failure. This guarantees data consistency.

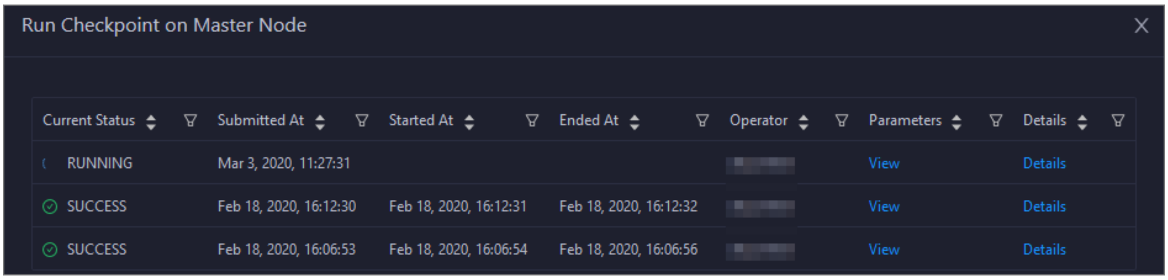
Prerequisites

Your ABM account has the permission to manage DataHub.

Procedure

1. On the **Services** tab, click **Pangu** in the left-side navigation pane and select a cluster from the drop-down list. The Overview page for Apsara Distributed File System appears.
2. Choose **Actions** > **Run Checkpoint on Master Node** in the upper-right corner.
3. In the right-side pane that appears, set the **volume** parameter. The default value is **PanguDefaultVolume**.
4. Click **Run**. A message appears, indicating that the request has been submitted.
5. View the execution status.

   Move the pointer over **Actions** in the upper-right corner and select **Execution History** next to **Run Checkpoint on Master Node**. In the right-side pane that appears, view the execution history.

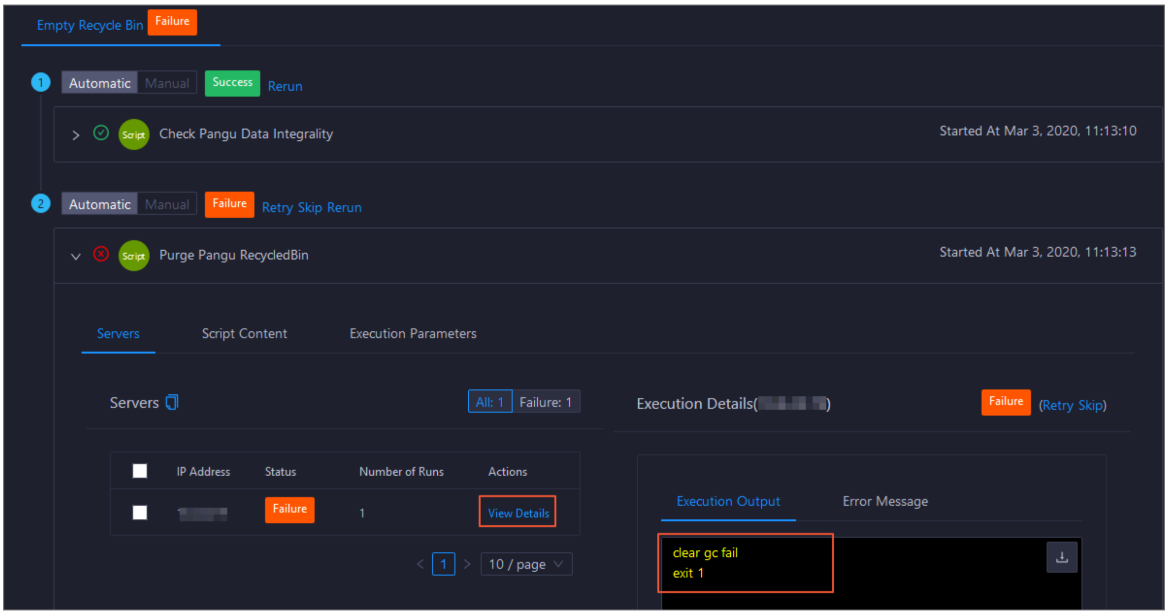


Run Checkpoint on Master Node

Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
RUNNING	Mar 3, 2020, 11:27:31			[redacted]	View	Details
SUCCESS	Feb 18, 2020, 16:12:30	Feb 18, 2020, 16:12:31	Feb 18, 2020, 16:12:32	[redacted]	View	Details
SUCCESS	Feb 18, 2020, 16:06:53	Feb 18, 2020, 16:06:54	Feb 18, 2020, 16:06:56	[redacted]	View	Details

In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.

6. If the status is FAILED, click **Details** in the Details column to locate the failure cause.



□	IP Address	Status	Number of Runs	Actions
□	[redacted]	Failure	1	View Details

```
clear gc fail
exit 1
```

You can also view information about parameter settings, host details, script, and execution parameters to locate the failure cause.

11.9.4.5.3.9. Change the primary master node of Apsara Distributed File System

ABM allows you to perform primary/secondary switchover on the master nodes of Apsara Distributed File System. After the primary/secondary switchover is completed, a secondary master node becomes the new primary master node, and the original primary master node becomes a new secondary master node.

Prerequisites

- Your ABM account has the permission to manage DataHub.
- You have obtained the roles of the primary and secondary master nodes in a volume. To view the role of a master node, log on to the Apsara Infrastructure Management Framework console and access the **PanguTools#** host in the DataHub cluster. Then, run the **puadmin gems** command on the host.
- You have obtained the hostname of the secondary master node that is to be changed to the new primary master node. To view the hostname, perform the following steps: Log on to the ABM console, go to the O&M page for DataHub, and then click **Services**. On the page that appears, click

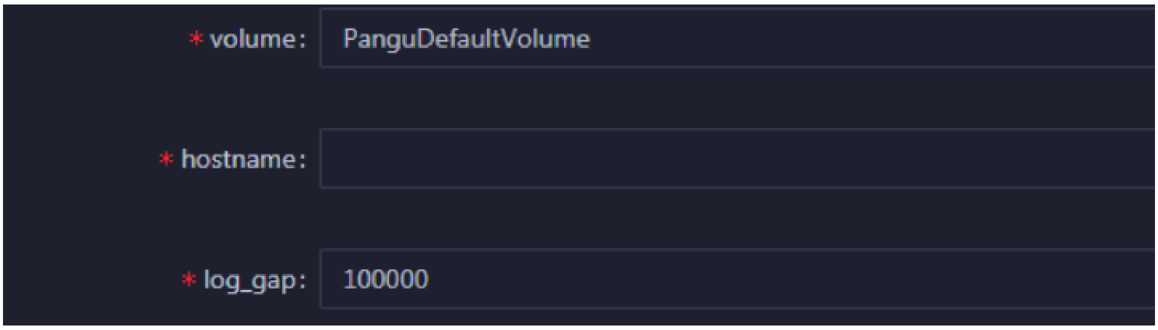
Pangu in the left-side navigation pane and click the **Instances** tab. On the **Instances** page, view the hostnames of **PanguMaster#** hosts.

Background information

A volume in Apsara Distributed File System is similar to a namespace in Hadoop Distributed File System (HDFS). The default volume is PanguDefaultVolume. Multiple volumes may exist if a cluster consists of numerous nodes. A volume has three master nodes. One of the nodes serves as the primary master node, whereas the other two nodes serve as secondary master nodes.

Procedure

1. On the **Services** tab, click **Pangu** in the left-side navigation pane and select a cluster from the drop-down list. The **Overview** page for Apsara Distributed File System appears.
2. Choose **Actions** > **Change Primary Master Node** in the upper-right corner. In the right-side pane that appears, set the parameters.



* volume: PanguDefaultVolume

* hostname:

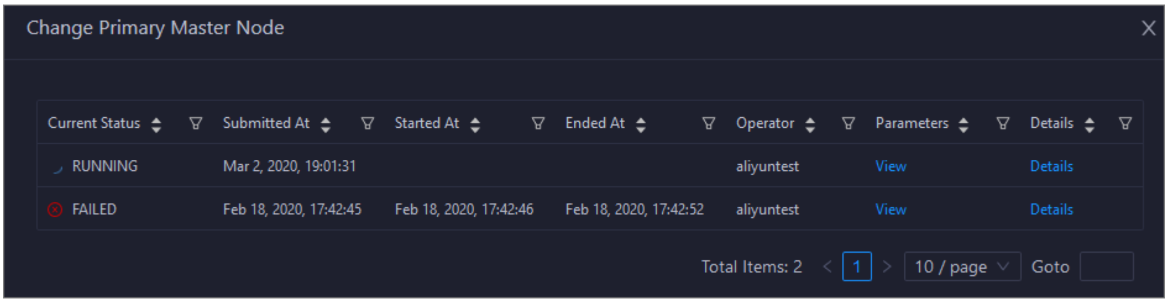
* log_gap: 100000

You must set the following parameters in this step:

- **volume**: the volume whose primary master node is to be changed. Default value: **PanguDefaultVolume**. If a cluster consists of multiple volumes, set this parameter to the name of the actual volume whose primary master node is to be changed.
- **hostname**: the hostname of the secondary master node that is changed to be the new primary master node.
- **log_gap**: the maximum log number gap between the original primary and secondary master nodes. During the switchover, the system checks the log number gap between the original primary and secondary master nodes. If the gap is less than the specified value, switchover is allowed. Otherwise, you cannot change the primary master node. Default value: **100000**.

3. Click **Run**. A message appears, indicating that the request has been submitted.
4. View the execution status.

   Move the pointer over **Actions** in the upper-right corner and select **Execution History** next to **Change Primary Master Node**. In the right-side pane that appears, view the execution history.



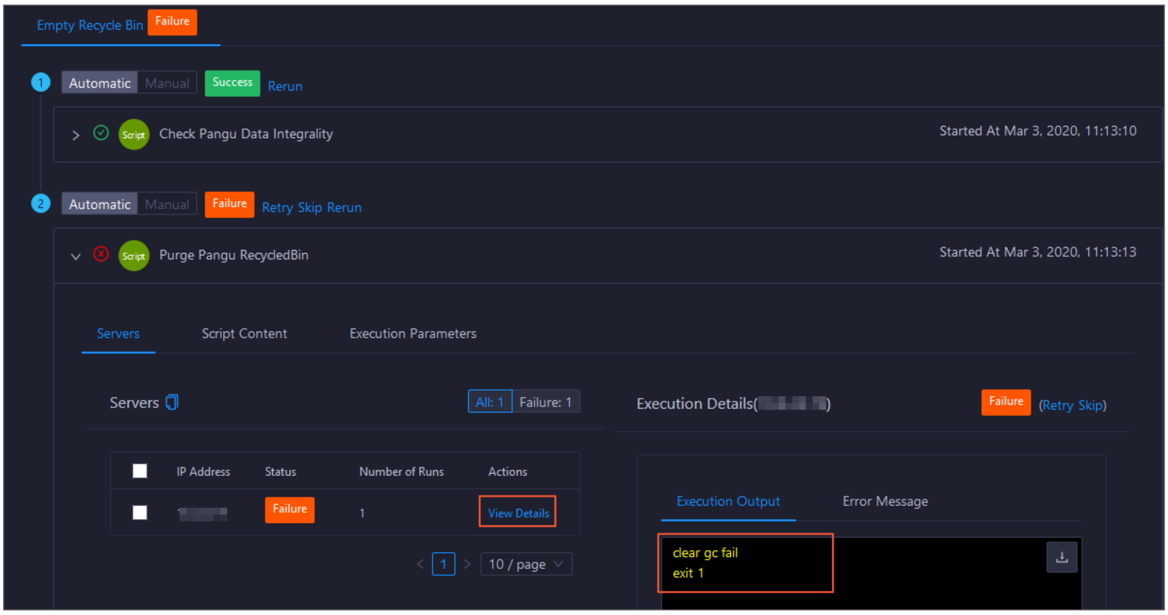
Change Primary Master Node

Current Status	Submitted At	Started At	Ended At	Operator	Parameters	Details
RUNNING	Mar 2, 2020, 19:01:31			aliyuntest	View	Details
FAILED	Feb 18, 2020, 17:42:45	Feb 18, 2020, 17:42:46	Feb 18, 2020, 17:42:52	aliyuntest	View	Details

Total Items: 2 < 1 > 10 / page Goto

In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.

5. If the status is FAILED, click **Details** in the Details column to locate the failure cause.



```
clear gc fail
exit 1
```

You can also view information about parameter settings, host details, script, and execution parameters to locate the failure cause.

11.9.4.6. Cluster O&M

11.9.4.6.1. Cluster O&M entry

This topic describes how to go to the cluster O&M page for DataHub in the ABM console.

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataHub**.
3. On the DataHub page, click **O&M** in the upper-right corner, and then click the **Clusters** tab.
4. On the **Clusters** tab, select a cluster in the left-side navigation pane. The **Overview** page for the cluster appears.

11.9.4.6.2. Cluster overview

The cluster overview page displays the overall running and health check information about a cluster. On this page, you can view the host status, service status, health check result and health check history of the cluster. You can also view the trend charts of CPU usage, disk usage, memory usage, load, and packet transmission for the cluster.

Go to the Overview page for a cluster

1. On the **O&M** page, click the **Clusters** tab.
2. On the **Clusters** tab, select a cluster in the left-side navigation pane and click the **Overview** tab. The Overview page for the cluster appears.

Hosts

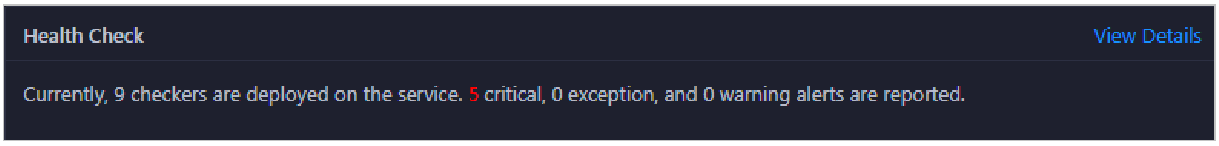
This section displays the respective number of hosts in different states in the cluster. A host may be in one of the following states: good, bad, and upgrading.

Services

This section displays all services deployed in the cluster and the respective number of services in the good and bad states.

Health Check

This section displays the number of checkers deployed for the cluster and the respective number of Critical, Warning, and Exception alerts.



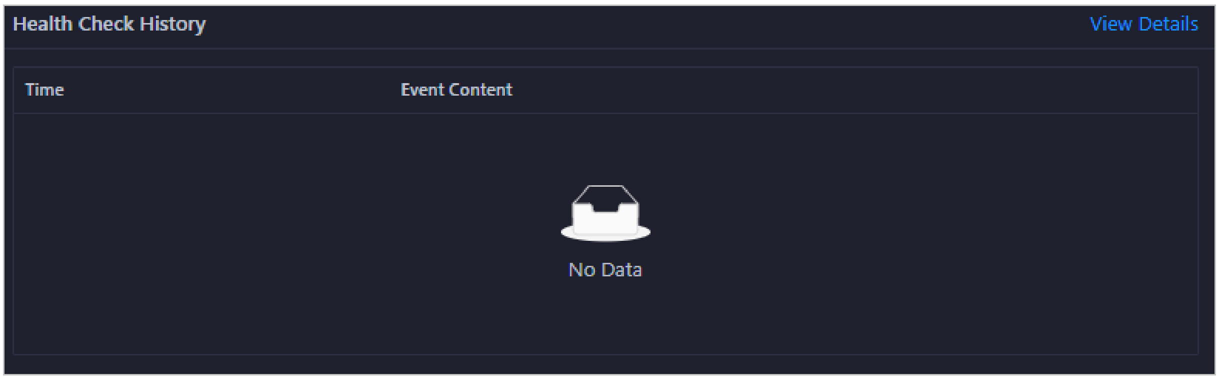
Currently, 9 checkers are deployed on the service. 5 critical, 0 exception, and 0 warning alerts are reported.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Cluster health.

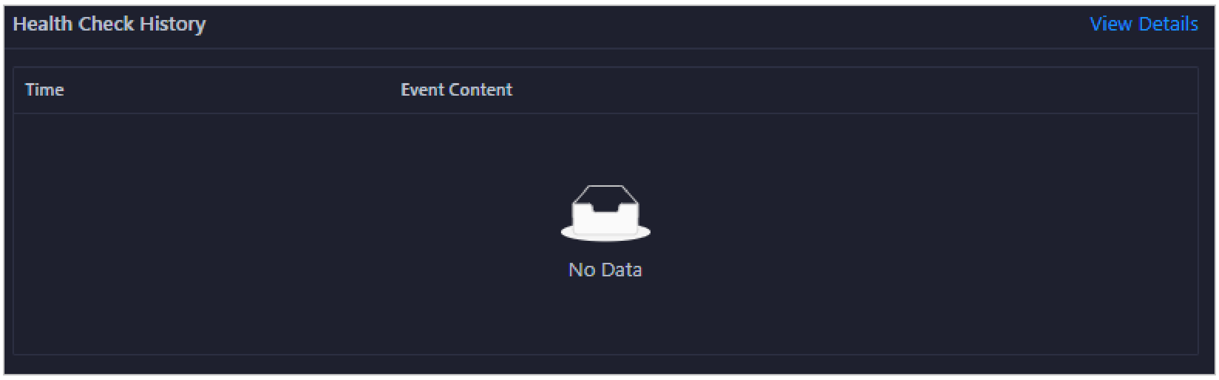
Health Check History

This section displays a record of the health checks performed on the cluster.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Cluster health.



You can click the event content of a check to view the anomalous items.

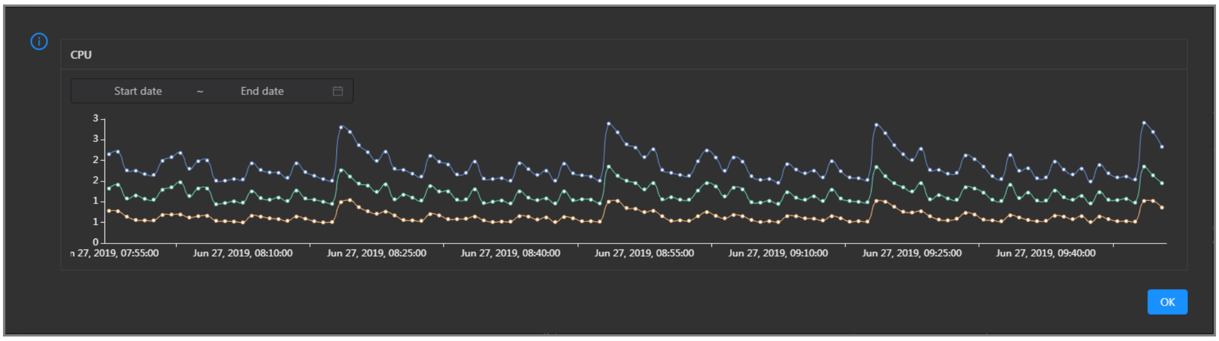


CPU

This chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

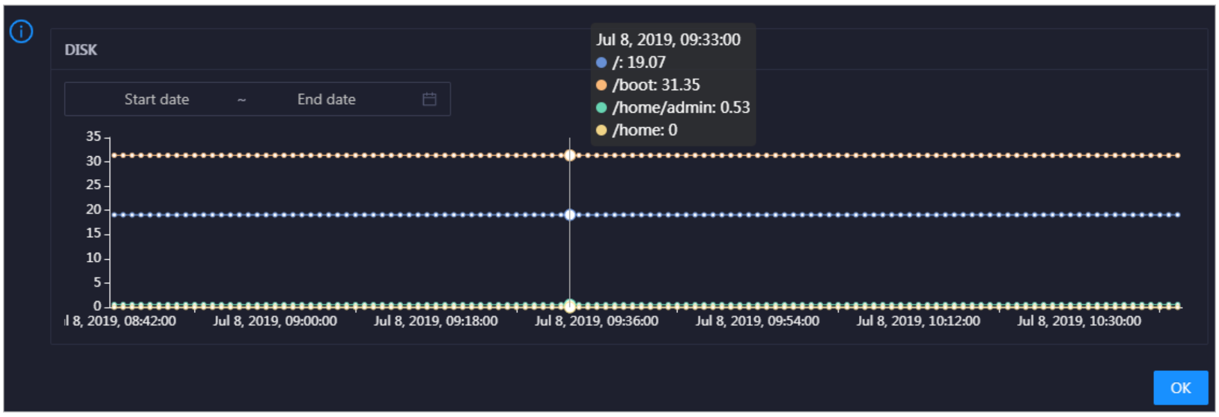
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the cluster in the specified period.



DISK

This chart shows the trend lines of the storage usage on the */*, */boot*, */home/admin*, and */home* directories for the cluster over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

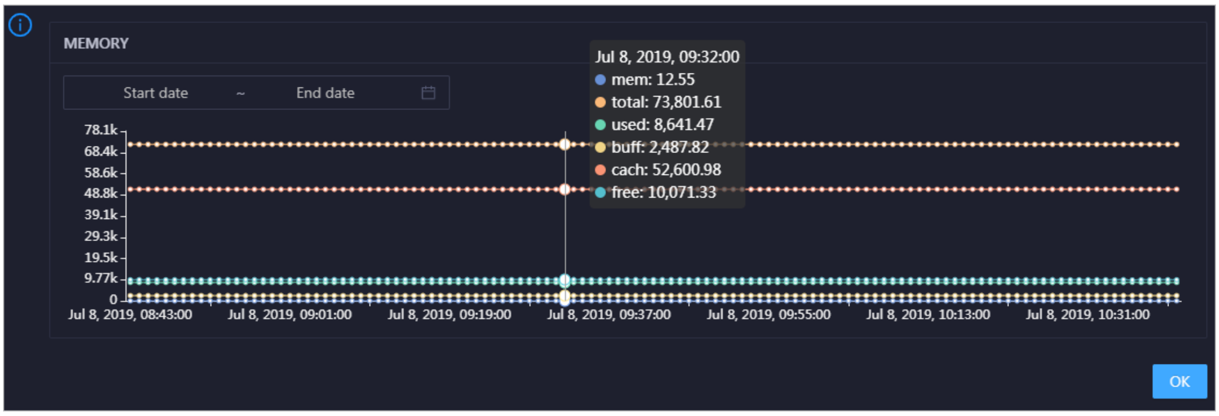


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

MEMORY

This chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

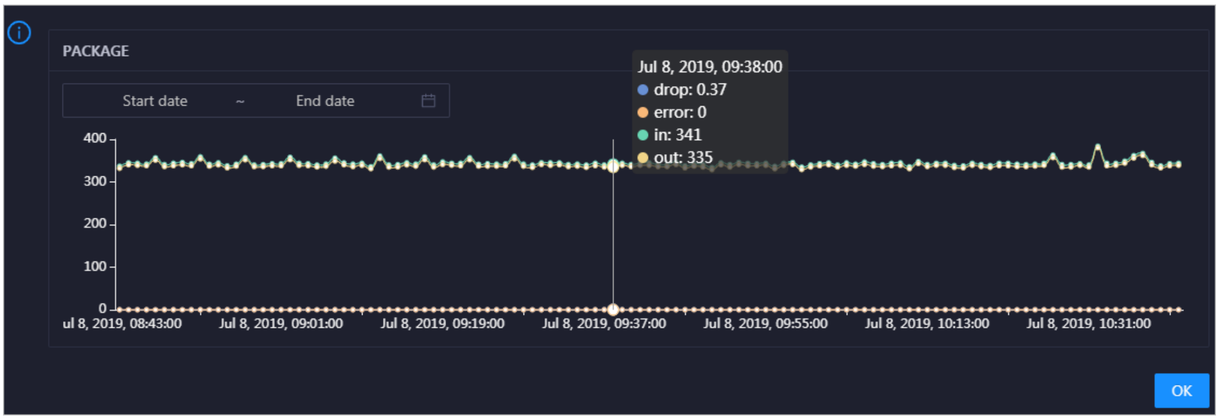


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the cluster in the specified period.

PACKAGE

This chart shows the trend lines of the numbers of dropped packets (drop), error packets (error), received packets (in), and sent packets (out) for the cluster in different colors. These trend lines reflect the data transmission status of the cluster.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

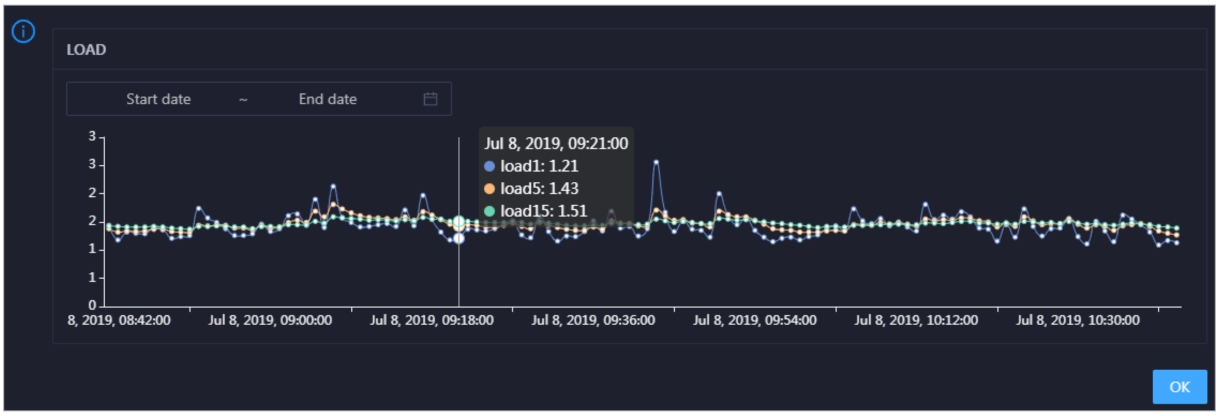


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the cluster in the specified period.

LOAD

This chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the cluster in the specified period.

11.9.4.6.3. Cluster health

The Health Status page displays the information about the checkers of the selected cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts. In addition, you can log on to a host and perform manual checks on the host.

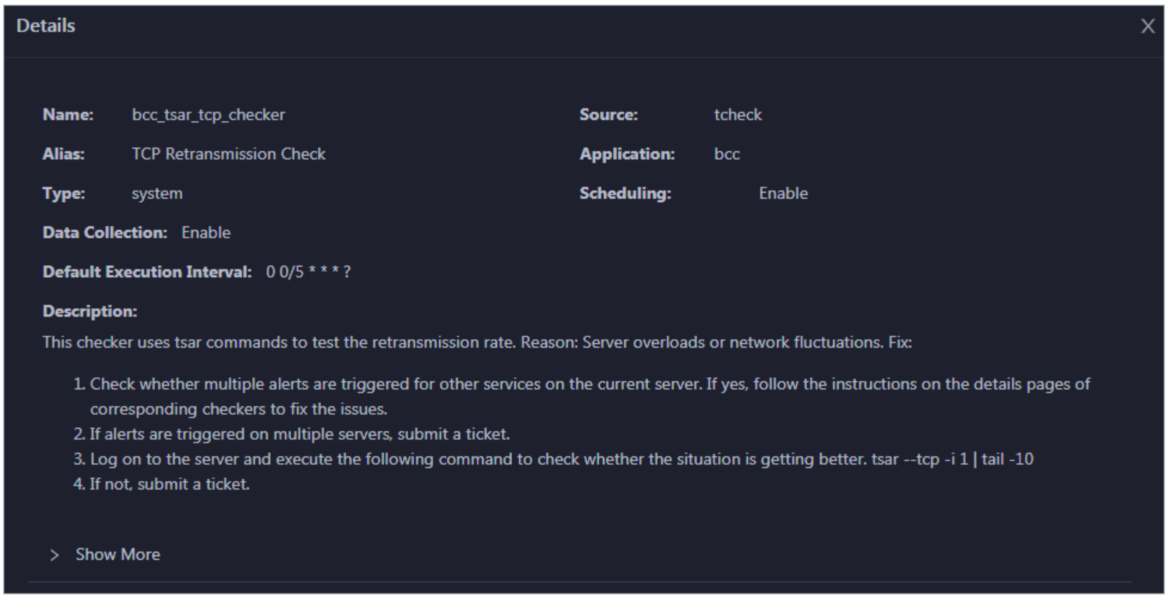
Go to the Health Status page

On the **Clusters** tab, select a cluster in the left-side navigation pane and click the **Health Status** tab. The Health Status page for the cluster appears.

On the **Health Status** tab, you can view all checkers for the cluster and the check results for the hosts in the cluster. The following alerts may be reported on a host: **CRITICAL**, **WARNING**, and **EXCEPTION**. The alerts are represented in different colors. You must handle the alerts in a timely manner, especially the **CRITICAL** and **WARNING** alerts.

View checker details

1. On the Health Status tab, click **Details** in the Actions column of a checker. On the Details page, view checker details.



Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

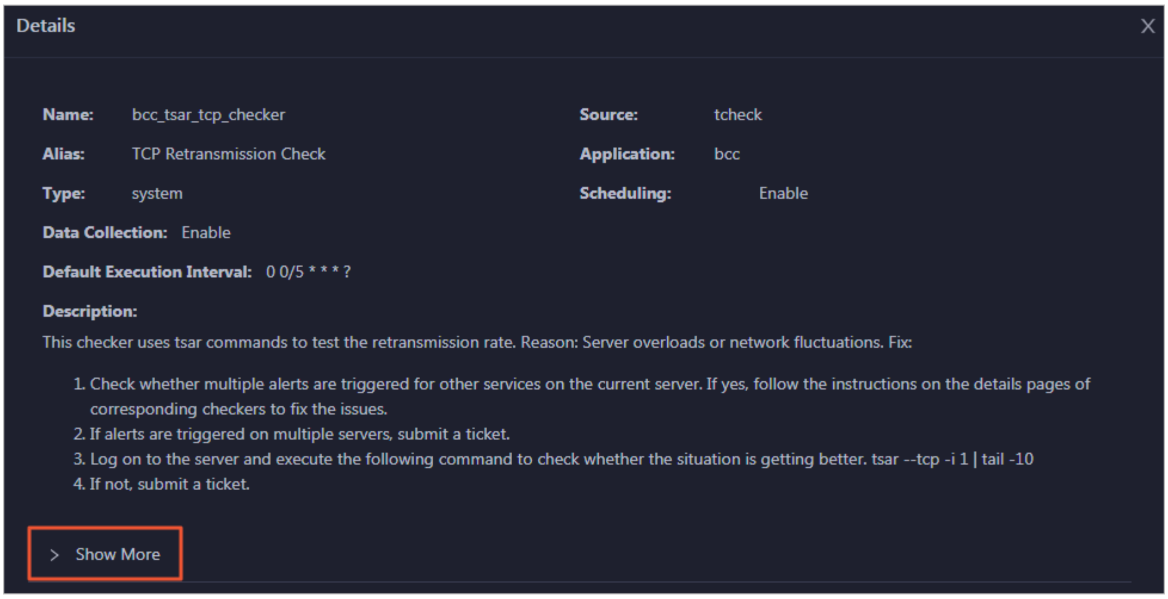
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include **Name**, **Source**, **Alias**, **Application**, **Type**, **Scheduling**, **Data Collection**, **Default Execution Interval**, and **Description**. The schemes to clear alerts are provided in the description.

2. Click **Show More** to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker
Source: tcheck
Alias: TCP Retransmission Check
Application: bcc
Type: system
Scheduling: Enable
Data Collection: Enable
Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

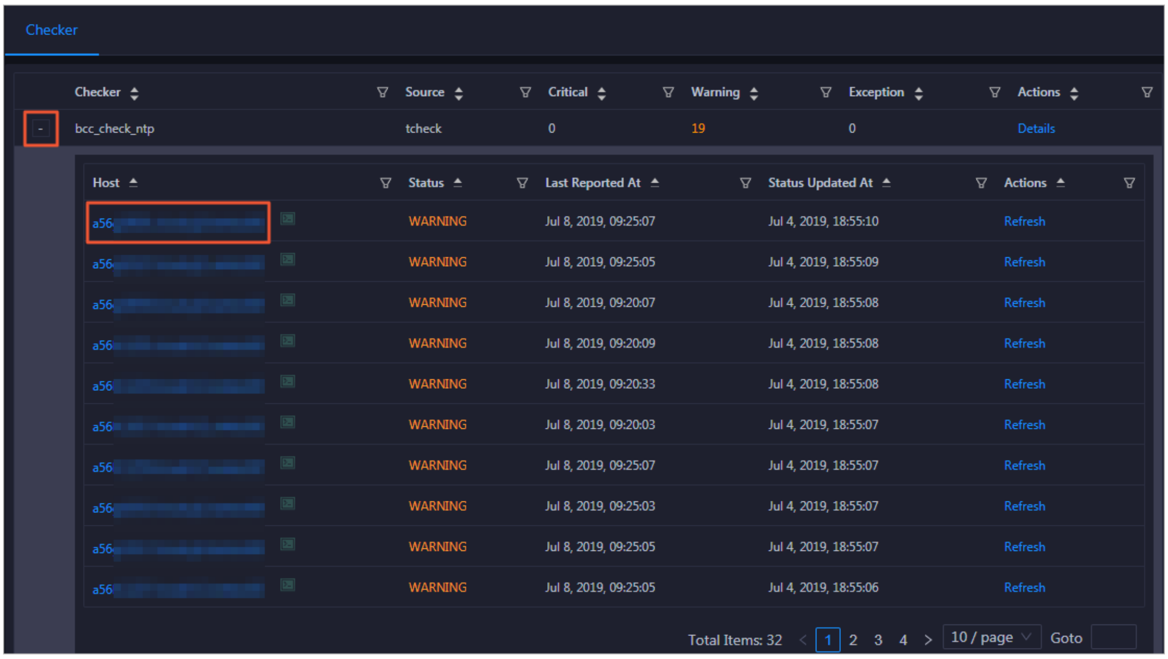
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about **Script**, **Target (TianJi)**, **Default Threshold**, and **Mount Point**.

View the hosts for which alerts are reported and causes for the alerts

You can view the check history and check results of a checker on a host.

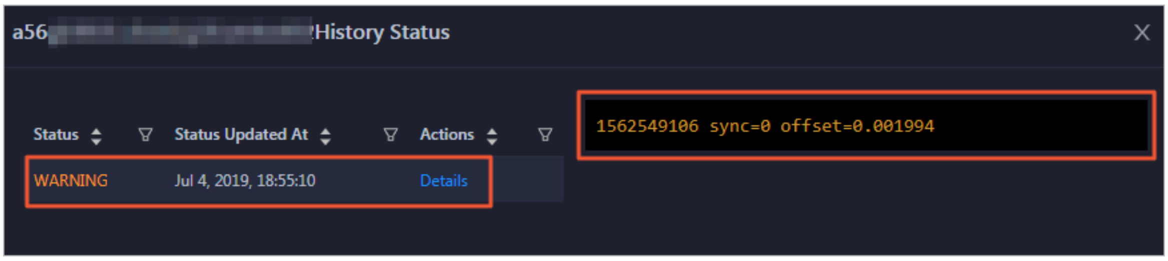
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported. You can view all hosts where the checker is run.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:06	Refresh

2. Click a hostname. In the panel that appears, click **Details** in the Actions column of a check result to view the cause of the alert.



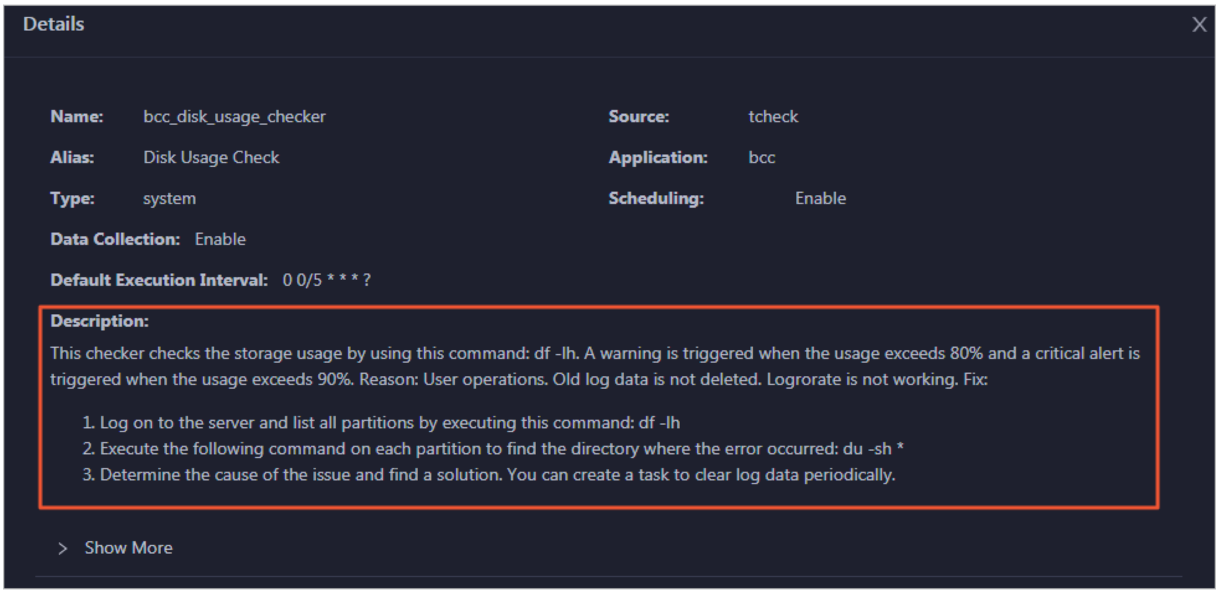
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status tab, click **Details** in the Actions column of a checker for which alerts are reported. On the Details page, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

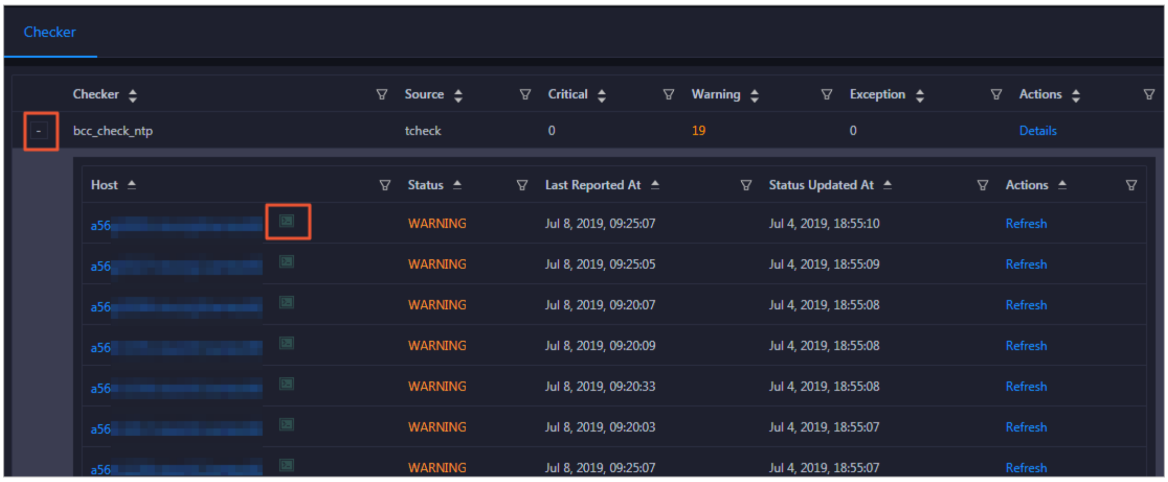
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

You may need to log on to a host to handle alerts or other issues that occurred on the host.

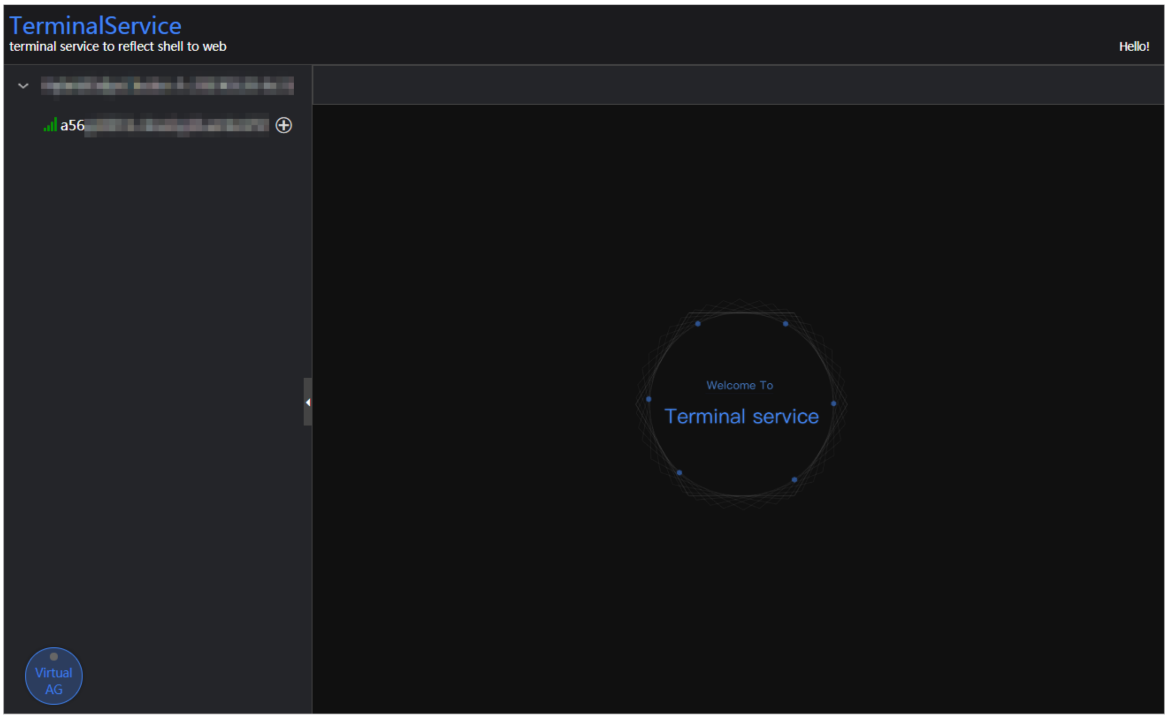
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported.



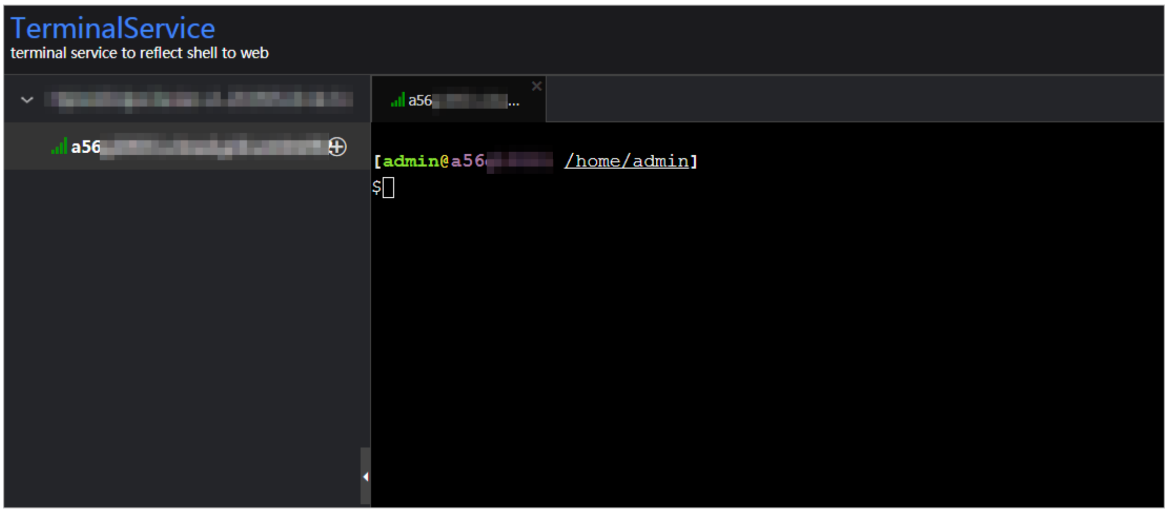
Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

2. Click the **Login in** icon of a host. The **TerminalService** page appears.



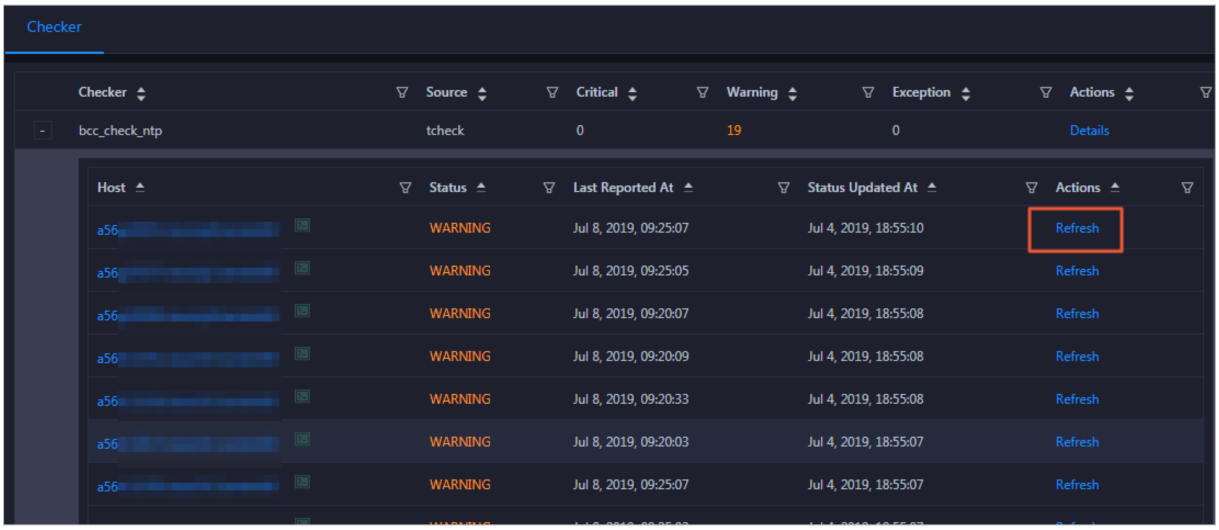
3. On the **TerminalService** page, click the hostname in the left-side navigation pane to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. This way, you can check whether the alert is cleared.



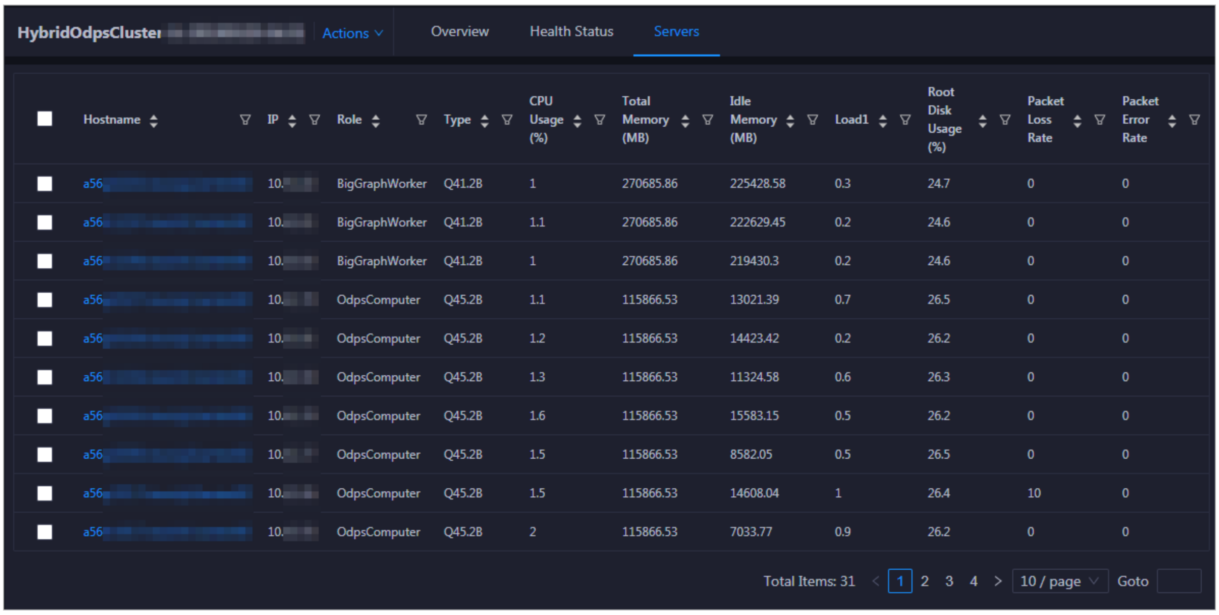
Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

11.9.4.6.4. Cluster hosts

The cluster hosts page displays information about hosts, including the hostname, IP address, role, type, CPU usage, total memory size, available memory size, load, root disk usage, packet loss rate, and packet error rate.

On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Hosts** tab. The **Hosts** page for the cluster appears.



Hostname	IP	Role	Type	CPU Usage (%)	Total Memory (MB)	Idle Memory (MB)	Load1	Root Disk Usage (%)	Packet Loss Rate	Packet Error Rate
a56[redacted]	10.[redacted]	BigGraphWorker	Q41.2B	1	270685.86	225428.58	0.3	24.7	0	0
a56[redacted]	10.[redacted]	BigGraphWorker	Q41.2B	1.1	270685.86	222629.45	0.2	24.6	0	0
a56[redacted]	10.[redacted]	BigGraphWorker	Q41.2B	1	270685.86	219430.3	0.2	24.6	0	0
a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.1	115866.53	13021.39	0.7	26.5	0	0
a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.2	115866.53	14423.42	0.2	26.2	0	0
a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.3	115866.53	11324.58	0.6	26.3	0	0
a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.6	115866.53	15583.15	0.5	26.2	0	0
a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.5	115866.53	8582.05	0.5	26.5	0	0
a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	1.5	115866.53	14608.04	1	26.4	10	0
a56[redacted]	10.[redacted]	OdpsComputer	Q45.2B	2	115866.53	7033.77	0.9	26.2	0	0

To view more information about a host, click the name of the host. The Overview tab of the Hosts page appears. For more information, see Host overview.

11.9.4.6.5. Cluster scale-out

This topic describes how to scale out a DataHub cluster in the ABM console. Cluster scale-out refers to the process of adding physical hosts in the default cluster of Apsara Infrastructure Management Framework to a DataHub cluster. The physical hosts of a DataHub cluster include chunkserver and frontend hosts.

Prerequisites

- The physical hosts to be added to a DataHub cluster are available in the default cluster of Apsara Infrastructure Management Framework.
- The default cluster of Apsara Infrastructure Management Framework has hosts whose **project** is **datahub**.

> ? **Note** Scale-out is only available for **chunkserver** and **frontend** hosts in a DataHub cluster.

Background information

In Apsara Stack, scaling out a cluster involves complex operations. You must configure a new physical host on Deployment Planner so that it can be added to the default cluster of Apsara Infrastructure Management Framework. The default cluster can be considered as an idle resource pool that provides resources for scaling out clusters for your business. To scale out a cluster, add physical hosts in the default cluster of Apsara Infrastructure Management Framework to the cluster. To scale in a cluster, remove physical hosts from the cluster to the default cluster of Apsara Infrastructure Management Framework.

Step 1: Obtain the name of the host to be added to a DataHub cluster

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **TIANJI** to log on to the Apsara Infrastructure Management Framework console.
3. In the left-side navigation pane, choose **Operations > Machine Operations**.
4. On the **Machine Operations** page, search for a host whose project is **datahub** in the **default** cluster. Then, copy the name of the host.

Step 2: Add the host to the target DataHub cluster

You can add multiple hosts to a DataHub cluster at a time to scale out the cluster. To scale out a cluster, you must first specify an existing host as the template host. When you scale out the DataHub cluster, the hosts copy configurations from the template host so that the hosts can be added to the cluster at a time.

1. On the O&M page of the ABM console, click the **Clusters** tab. On the Clusters tab, select the target cluster in the left-side navigation pane, click the **Hosts** tab, and then select a host whose role is **chunkserver** or **frontend** as the template host.
2. Choose **Actions > Scale out Cluster** in the upper-right corner. In the **Scale out Cluster** right-side pane, set relevant parameters.

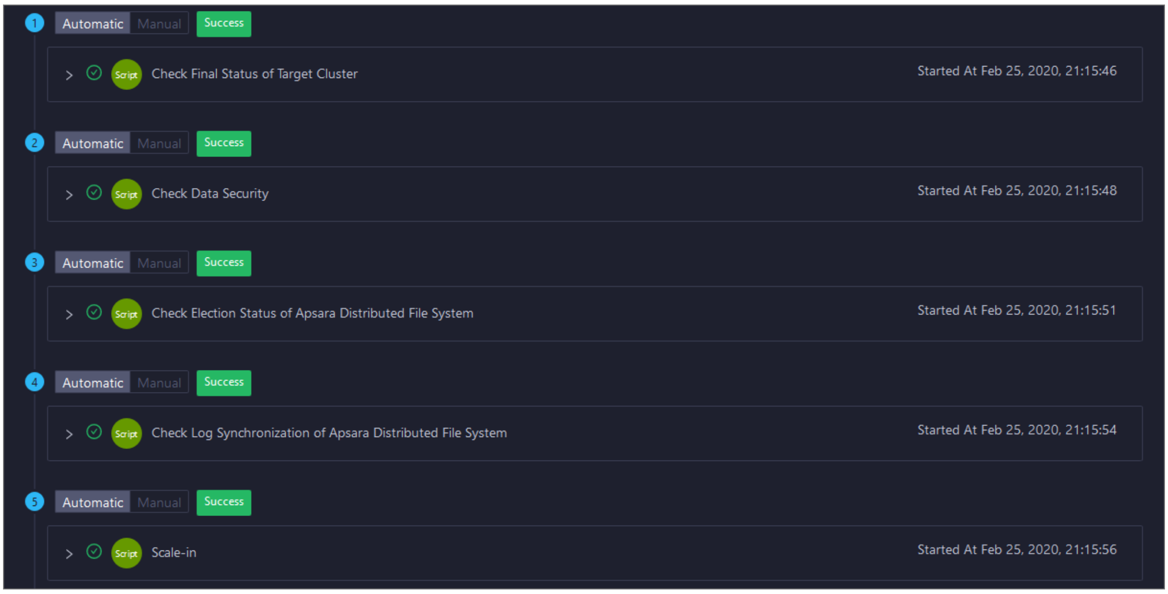
   You must set the following parameters in this step:

   - **Refer Hostname**: the name of the template host. The name of the selected host is used by default.
   - **hostname**: the name of the host to be added to the DataHub cluster. The drop-down list displays all available hosts in the default cluster for scale-out. You can select one or more hosts from the drop-down list.

3. Click **Run**. A message appears, indicating that the request has been submitted.
4. View the scale-out status.

   Move the pointer over **Actions** in the upper-right corner and select **Execution History** next to **Scale out Cluster**. In the right-side pane that appears, view the execution status.

   It may take some time for the cluster to be scaled out. In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.
5. If the status is RUNNING, click **Details** in the Details column to view the steps and progress of the scale-out.



1 Check Final Status of Target Cluster — Started At Feb 25, 2020, 21:15:46

2 Check Data Security — Started At Feb 25, 2020, 21:15:48

3 Check Election Status of Apsara Distributed File System — Started At Feb 25, 2020, 21:15:51

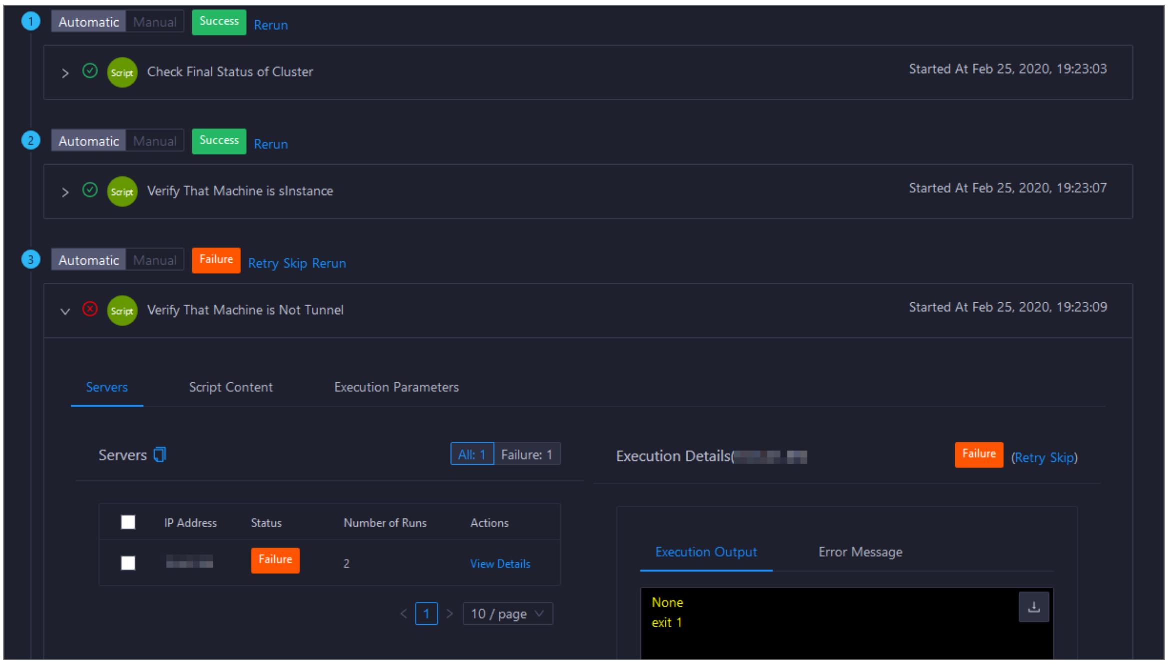
4 Check Log Synchronization of Apsara Distributed File System — Started At Feb 25, 2020, 21:15:54

5 Scale-in — Started At Feb 25, 2020, 21:15:56

6. If the status is **FAILED**, click **Details** to locate the failure cause. For more information, see Locate the failure cause.

Locate the failure cause

1. On the **Clusters** tab, move the pointer over **Actions** in the upper-left corner and select **Execution History** next to **Scale out Cluster**. In the right-side pane that appears, view the execution history.
2. If the status of a record is FAILED, click **Details** to locate the failure cause.



1 Automatic Manual Success Rerun
Script Check Final Status of Cluster
Started At Feb 25, 2020, 19:23:03
2 Automatic Manual Success Rerun
Script Verify That Machine is sInstance
Started At Feb 25, 2020, 19:23:07
3 Automatic Manual Failure Retry Skip Rerun
Script Verify That Machine is Not Tunnel
Started At Feb 25, 2020, 19:23:09
Servers
Script Content
Execution Parameters
Servers
All: 1
Failure: 1
Execution Details([redacted]
Failure
(Retry Skip)
Execution Output
Error Message
10 / page

☐	IP Address	Status	Number of Runs	Actions
☐	[redacted]	Failure	2	View Details

```
None
exit 1
```

You can also view the parameter settings, host details, script, and execution parameters to locate the failure cause.

11.9.4.6.6. Cluster scale-in

This topic describes how to scale in a DataHub cluster in the ABM console. Cluster scale-in refers to the process of removing physical hosts from a DataHub cluster to the default cluster of Apsara Infrastructure Management Framework. The physical hosts of a DataHub cluster include chunkserver and frontend hosts.

Prerequisites

- Scale-in is only available for **chunkserver** and **frontend** hosts in a DataHub cluster.
- The following operations are performed before you remove one or more **chunkserver** hosts:
  - Run the df command to check the disk usage on each host. Calculate whether the disk will be full after a specific number of hosts are removed. If so, we recommend that you do not perform the scale-in.
  - Shards on the removed hosts will be migrated to other hosts. Therefore, you must log on to the webconsole host to calculate the shard load on each host after the scale-in. If the number of shards on a host exceeds 1,000, performance may be affected. In this case, we recommend that you do not perform the scale-in.
- The following operations are performed before you remove one or more **frontend** hosts:
  - Run the df command to check the disk usage on each host. Calculate whether the disk will be full after a specific number of hosts are removed. If so, we recommend that you do not perform the scale-in.
  - Shards on the removed hosts will be migrated to other hosts. Therefore, you must log on to the webconsole host to calculate the shard load on each host after the scale-in. If the number of shards on a host exceeds 1,000, performance may be affected. In this case, we recommend that you do not perform the scale-in.

- Check the traffic and queries per second (QPS). If the traffic exceeds 400 MBit/s or the QPS exceeds 15,000, we recommend that you do not perform the scale-in.

Background information

In Apsara Stack, scaling out a cluster involves complex operations. You must configure a new physical host on Deployment Planner so that it can be added to the default cluster of Apsara Infrastructure Management Framework. The default cluster can be considered as an idle resource pool that provides resources for scaling out clusters for your business. To scale out a cluster, add physical hosts in the default cluster of Apsara Infrastructure Management Framework to the cluster. To scale in a cluster, remove physical hosts from the cluster to the default cluster of Apsara Infrastructure Management Framework.

Procedure

1. On the O&M page of the ABM console, click the **Clusters** tab. On the Clusters tab, select the target cluster in the left-side navigation pane, click the **Hosts** tab, and then select one or more hosts whose role is **chunkserver** or **frontend**.
2. On the Clusters tab, choose **Actions > Scale in Cluster** in the upper-right corner. In the **Scale in Cluster** right-side pane, set the following parameter:

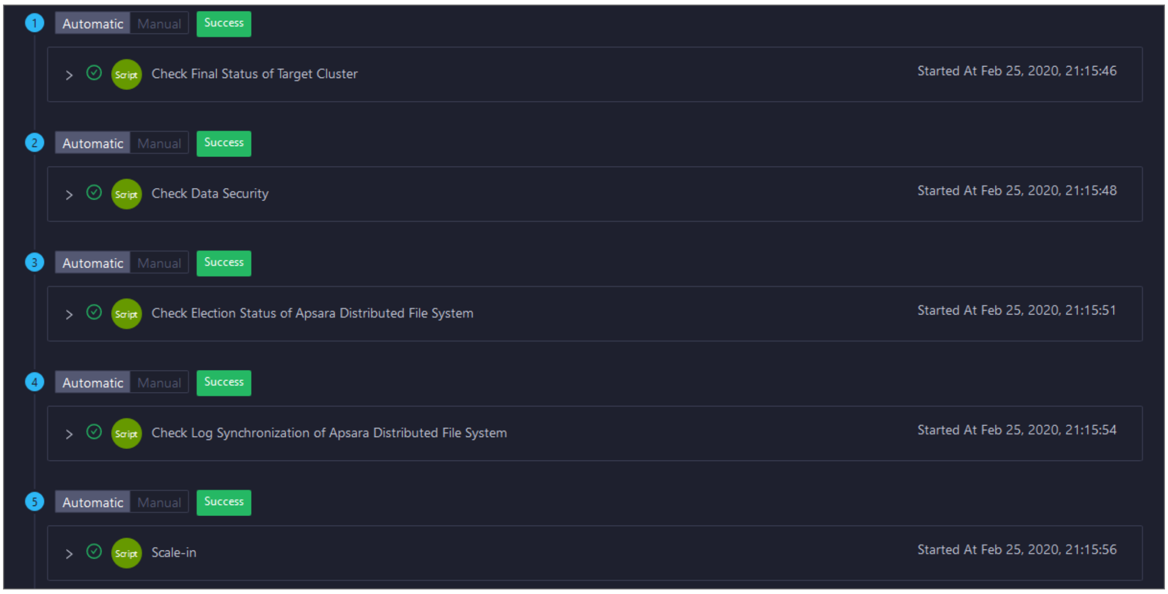
   Hostname: the name of the host to be removed from the DataHub cluster. The name of the selected host is used by default.
3. Click **Run**. A message appears, indicating that the request has been submitted.
4. View the scale-in status.

   Move the pointer over **Actions** in the upper-right corner and select **Execution History** next to **Scale in Cluster**. In the right-side pane that appears, view the execution status.

   It may take some time for the cluster to be scaled in. In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.

   > **Note** If the status is **FAILED**, click Details in the Details column to locate the failure cause. For more information, see Locate the failure cause.
5. (Optional)View the scale-in progress.

If the status is **RUNNING**, click **Details** to view the steps and progress of the scale-in.



1 Automatic Manual Success
Check Final Status of Target Cluster — Started At Feb 25, 2020, 21:15:46

2 Automatic Manual Success
Check Data Security — Started At Feb 25, 2020, 21:15:48

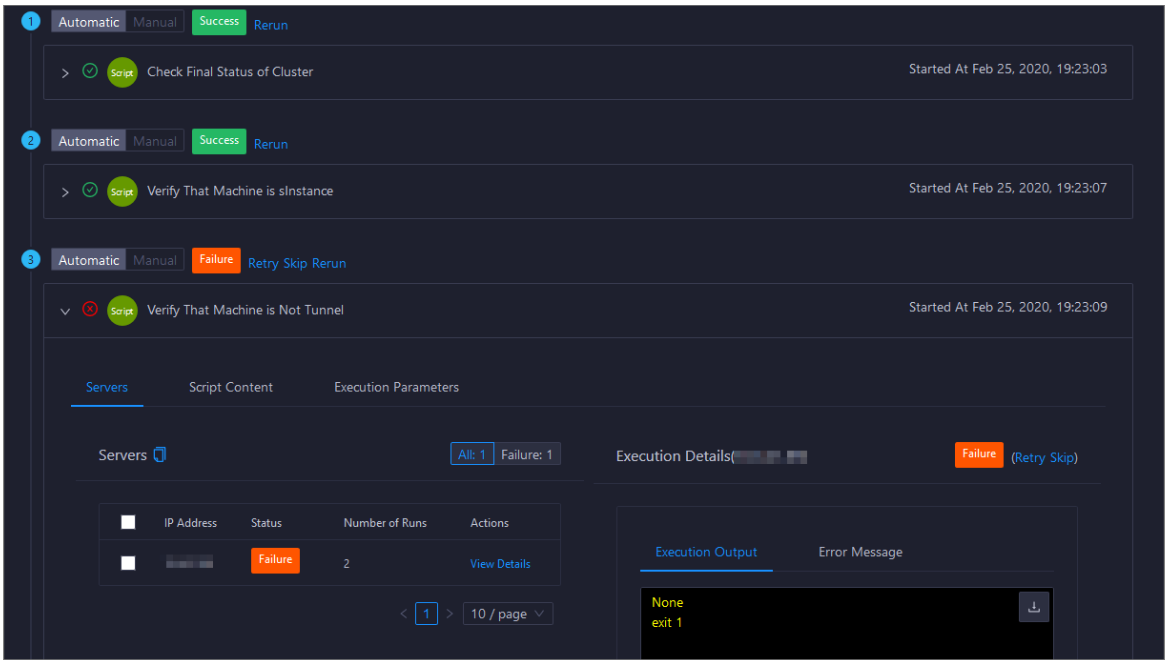
3 Automatic Manual Success
Check Election Status of Apsara Distributed File System — Started At Feb 25, 2020, 21:15:51

4 Automatic Manual Success
Check Log Synchronization of Apsara Distributed File System — Started At Feb 25, 2020, 21:15:54

5 Automatic Manual Success
Scale-in — Started At Feb 25, 2020, 21:15:56

Locate the failure cause

1. On the **Clusters** tab, move the pointer over **Actions** in the upper-left corner and select **Execution History** next to **Scale in Cluster**. In the right-side pane that appears, view the execution history.
2. If the status of a record is FAILED, click **Details** to locate the failure cause.



1 Automatic Manual Success Rerun
Check Final Status of Cluster — Started At Feb 25, 2020, 19:23:03

2 Automatic Manual Success Rerun
Verify That Machine is sInstance — Started At Feb 25, 2020, 19:23:07

3 Automatic Manual Failure Retry Skip Rerun
Verify That Machine is Not Tunnel — Started At Feb 25, 2020, 19:23:09

Servers

	IP Address	Status	Number of Runs	Actions
□	[redacted]	Failure	2	View Details

Execution Details([redacted]) Failure (Retry Skip)

```
None
exit 1
```

You can also view the parameter settings, host details, script, and execution parameters to locate the failure cause.

11.9.4.6.7. Delete topics from a smoke testing project

Apsara Big Data Manager allows you to delete topics from a DataHub test project and view the execution history.

1. On the **Clusters** page, select a cluster in the left-side navigation pane. Click the **Hosts** tab. The **Hosts** page for the cluster appears.
2. On the Clusters page, choose **Actions > Delete Topic from Smoke Testing**. The **Delete Topic from Smoke Testing** dialog box appears.
3. Click **Run**. A message appears, indicating that the action has been submitted.
4. View the history of deleting topics.

   Click **Actions** in the upper-left corner, and then click **Execution History** next to **Delete Topic from Smoke Testing** to view the execution history.

   In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.

   - If the status is FAILED, click **Details** in the Details column to locate the failure cause.

     You can also view information about parameter settings, host details, script, and execution parameters to locate the failure cause.

   - If the status is SUCCESS, click **Details** to view the execution result. On the page that appears, click **View Details** in the **Actions** column. The execution result appears in the Execution Details section in the lower-right corner. The execution result includes the time when the job was run and the IP address of the host.

11.9.4.6.8. Reverse parse request ID

Apsara Big Data Manager allows you to reverse parse request ID in DataHub to obtain the time when a job was run and the IP address of the host. You can use the obtained information to query logs for troubleshooting.

1. On the **Clusters** page, select a cluster in the left-side navigation pane. Click the **Hosts** tab. The **Hosts** page for the cluster appears.
2. On the Clusters page, choose **Actions > Reverse Parse Request ID**. In the **Reverse Parse Request ID** dialog box that appears, set **Request Id**.
3. Click **Run**. A message appears, indicating that the action has been submitted.
4. View the reverse parsing status.

   Click **Actions** in the upper-left corner, and then click **Execution History** next to **Reverse Parse Request ID** to view the execution history.

   In the Current Status column, **RUNNING** indicates that the execution is in progress, **SUCCESS** indicates that the execution is successful, and **FAILED** indicates that the execution fails.

   - If the status is FAILED, click **Details** in the Details column to locate the failure cause.

     You can also view information about parameter settings, host details, script, and execution parameters to locate the failure cause.

   - If the status is SUCCESS, click **Details** to view the execution result. On the page that appears, click **View Details** in the **Actions** column. The execution result appears in the Execution Details section in the lower-right corner. The execution result includes the time when the job was run and the IP address of the host.

11.9.4.7. Host O&M

11.9.4.7.1. Host O&M entry

This topic describes how to go to the host O&M page for DataHub in the ABM console.

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and select **DataHub**.
3. On the DataHub page, click **O&M** in the upper-right corner, and then click the **Hosts** tab.
4. On the **Hosts** page, select a host in the left-side navigation pane. The **Overview** page for the host appears.

11.9.4.7.2. Host overview

The host overview page displays the overall running information about a host in a DataHub cluster. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.

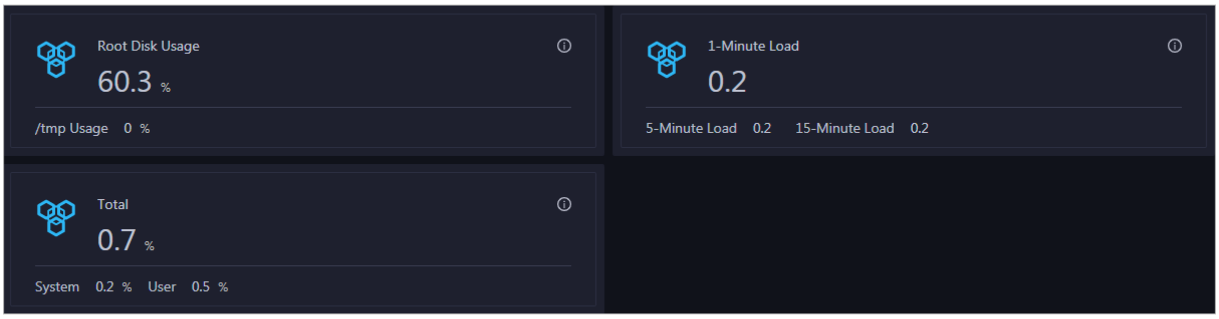
Entry

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Overview** tab. The **Overview** page for the host appears.

On the **Overview** page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.

Root Disk Usage, Total, and 1-Minute Load

These sections display the root disk usage, total usage, and 1-minute load for the selected host. The Root Disk Usage section provides the usage of the */tmp* directory. The Total section provides the system usage and user usage. The 1-Minute Load section provides the 1-minute, 5-minute, and 15-minute load averages.



Root Disk Usage
60.3 %
/tmp Usage 0 %

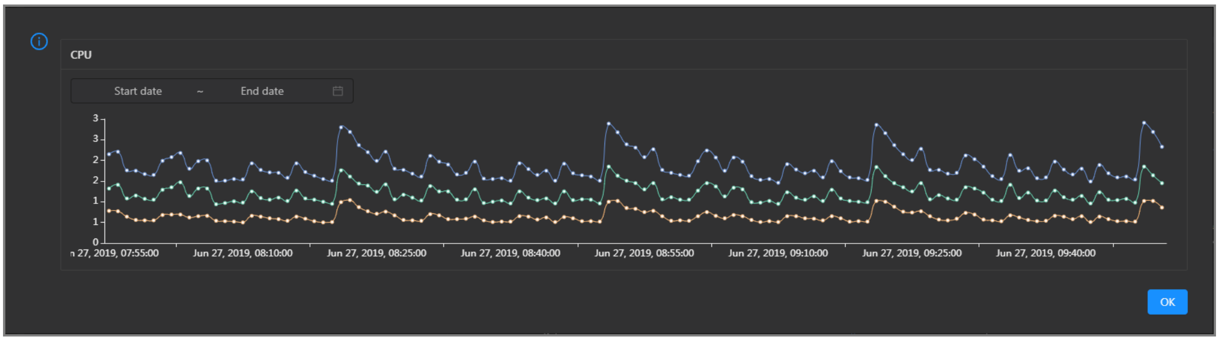
1-Minute Load
0.2
5-Minute Load 0.2 15-Minute Load 0.2

Total
0.7 %
System 0.2 % User 0.5 %

CPU

The CPU chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) of the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

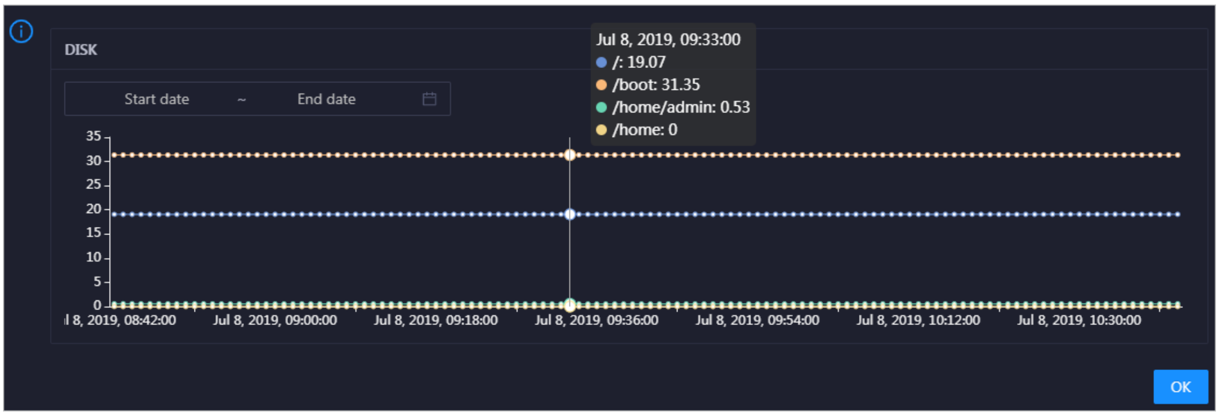


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the host in the specified period.

DISK

The DISK chart shows the trend lines of the storage usage in the */*, */boot*, */home/admin*, and */home* directories for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

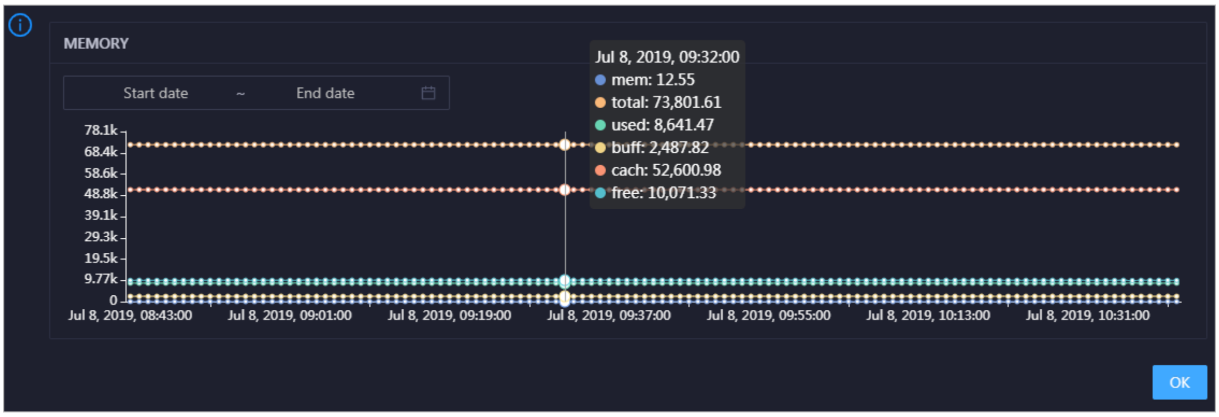


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the host in the specified period.

MEMORY

The MEMORY chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

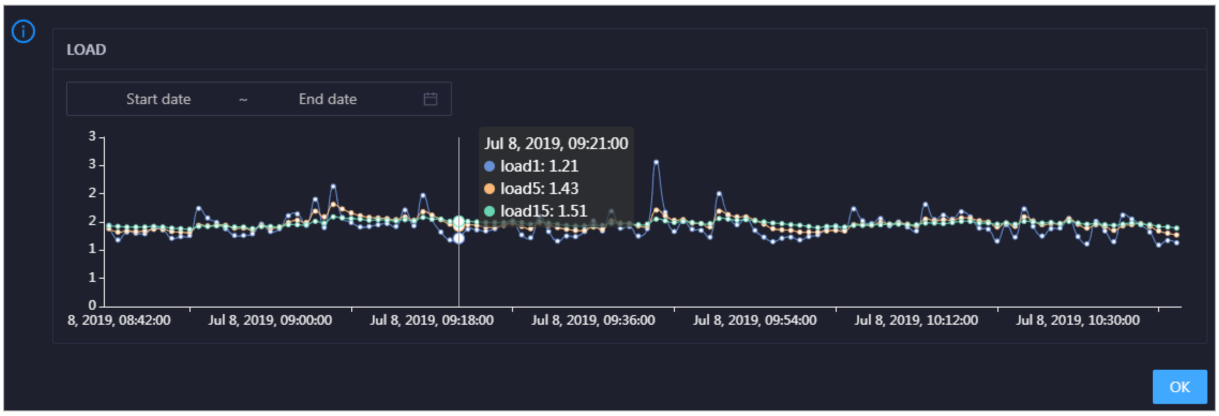


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the host in the specified period.

LOAD

The LOAD chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

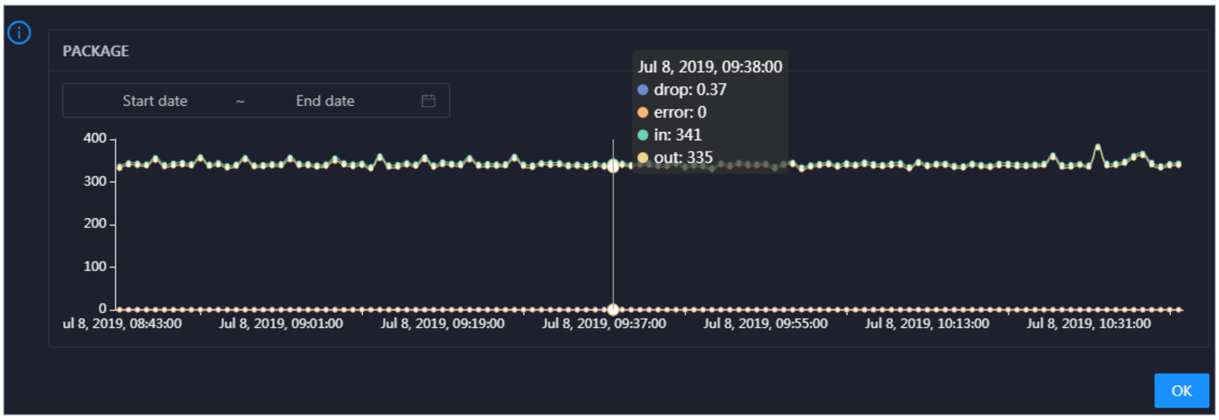


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the host in the specified period.

PACKAGE

The PACKAGE chart shows the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the host over time in different colors. These trend lines reflect the data transmission status of the host.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

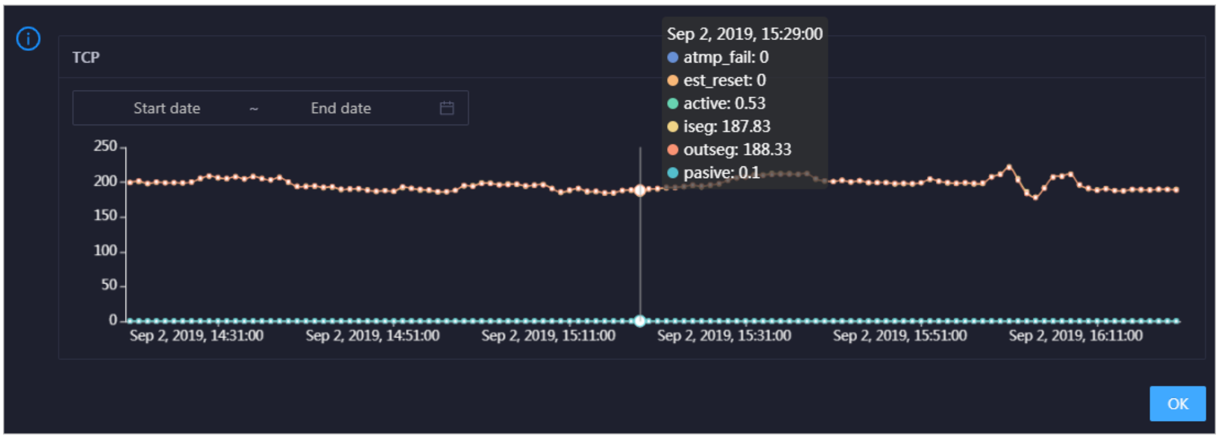


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the host in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the host over time in different colors. These trend lines reflect the TCP connection status of the host.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

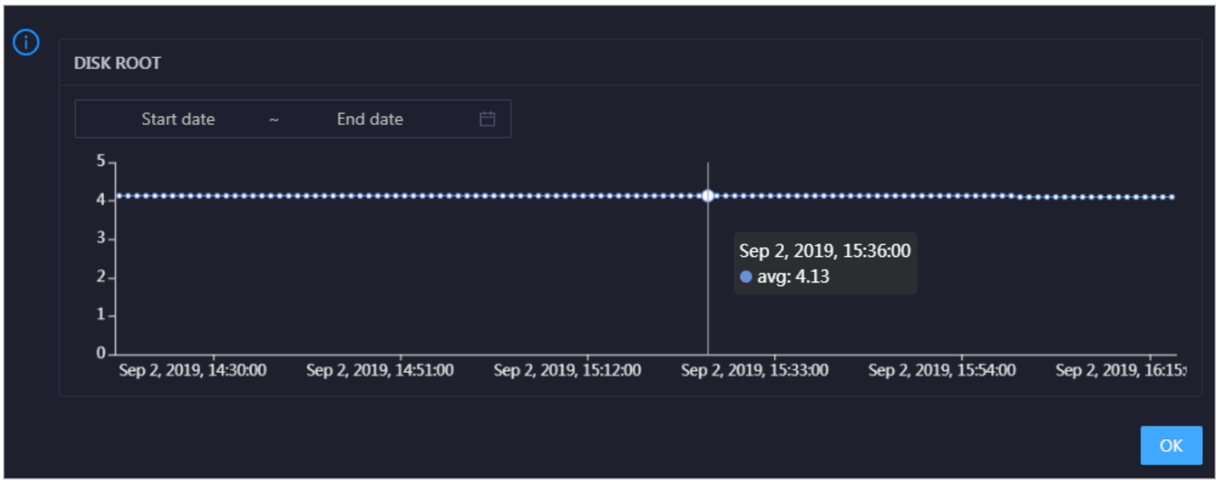


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the host in the specified period.

DISK ROOT

This chart displays the trend line of the average usage of the root disk (/) for the host over time.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the host in the specified period.

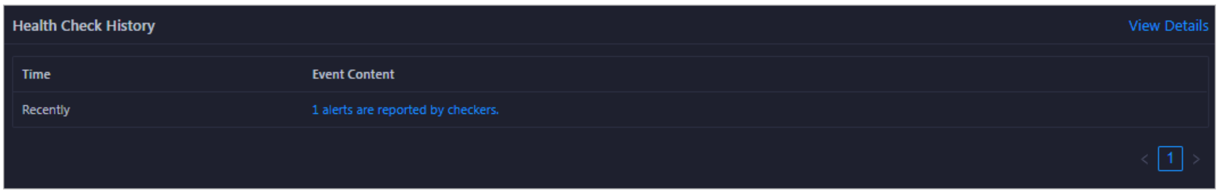
Health Check

This section displays the number of checkers deployed for the host and the respective number of Critical, Warning, and Exception alerts.

Click **View Details** to go to the Host health page. On this page, you can view the health check details.

Health Check History

This section displays a record of the health checks performed on the host.

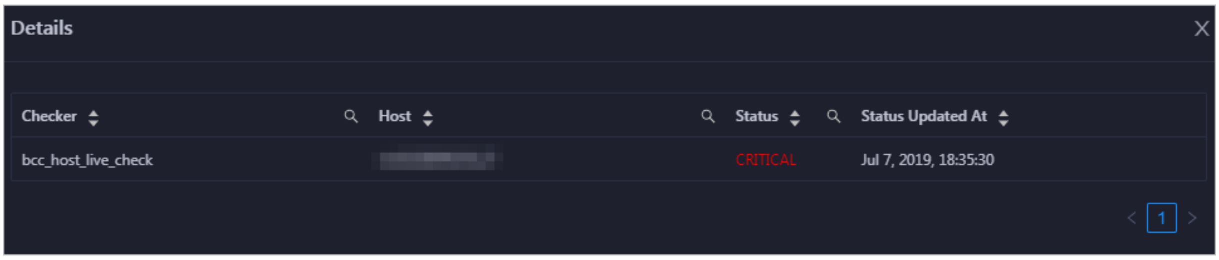

Health Check History

View Details

Time	Event Content
Recently	1 alerts are reported by checkers.

Click **View Details** to go to the Host health page. On this page, you can view the health check details.

You can click the event content of a check to view the exception items.

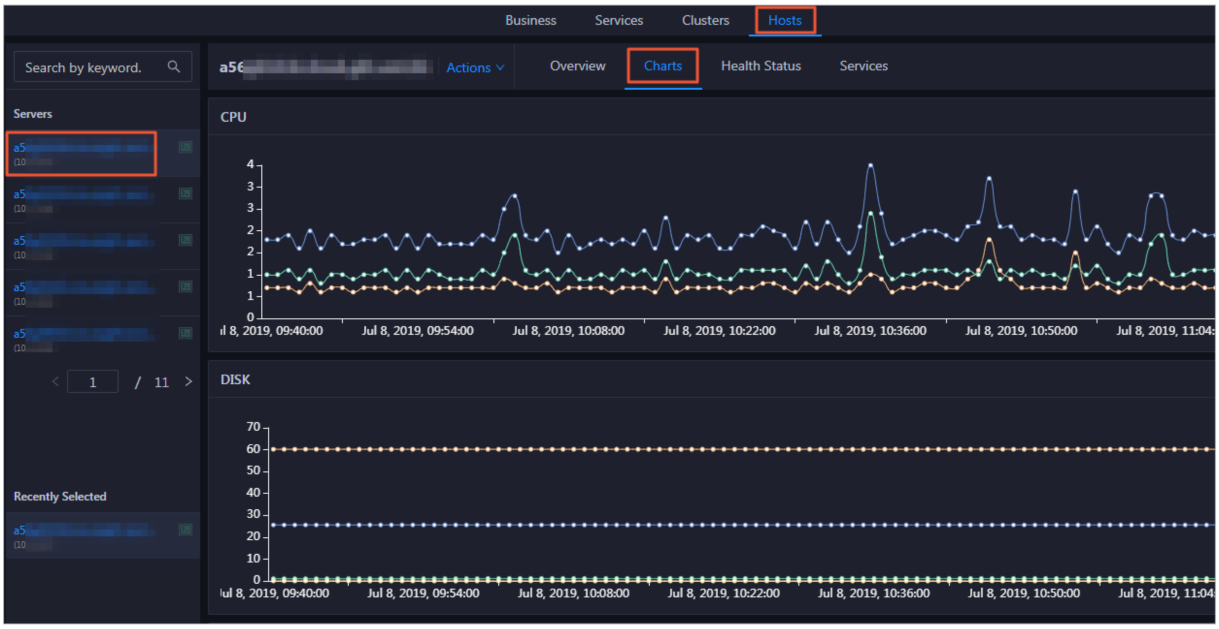

Details

Checker	Host	Status	Status Updated At
bcc_host_live_check	[redacted]	CRITICAL	Jul 7, 2019, 18:35:30

11.9.4.7.3. Host charts

On the host chart page, you can view the enlarged trend charts of CPU usage, memory usage, storage usage, load, and packet transmission.

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Charts** tab. The **Charts** page for the host appears.



The **Charts** page displays trend charts of CPU usage, disk usage, memory usage, load, and packet transmission for the host. For more information, see Host overview.

11.9.4.7.4. Host health

The Health Status page displays the information about the checkers of the selected host, including the checker details, check results, and schemes to clear alerts. In addition, you can log on to the host and perform manual checks on the host.

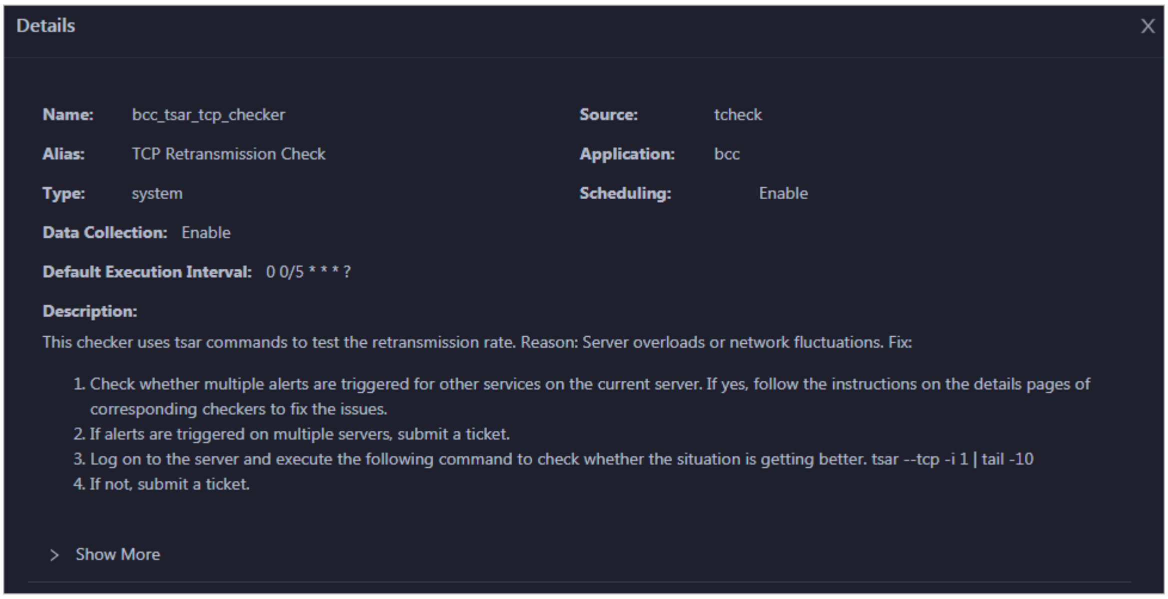
Go to the Health Status page

On the **Hosts** tab, select a host in the left-side navigation pane and click the **Health Status** tab. The **Health Status** page for the host appears.

On the **Health Status** page, you can view all checkers and the check results for the host. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

View checker details

1. On the Health Status page, click **Details** in the Actions column of a checker. In the dialog box that appears, view the checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

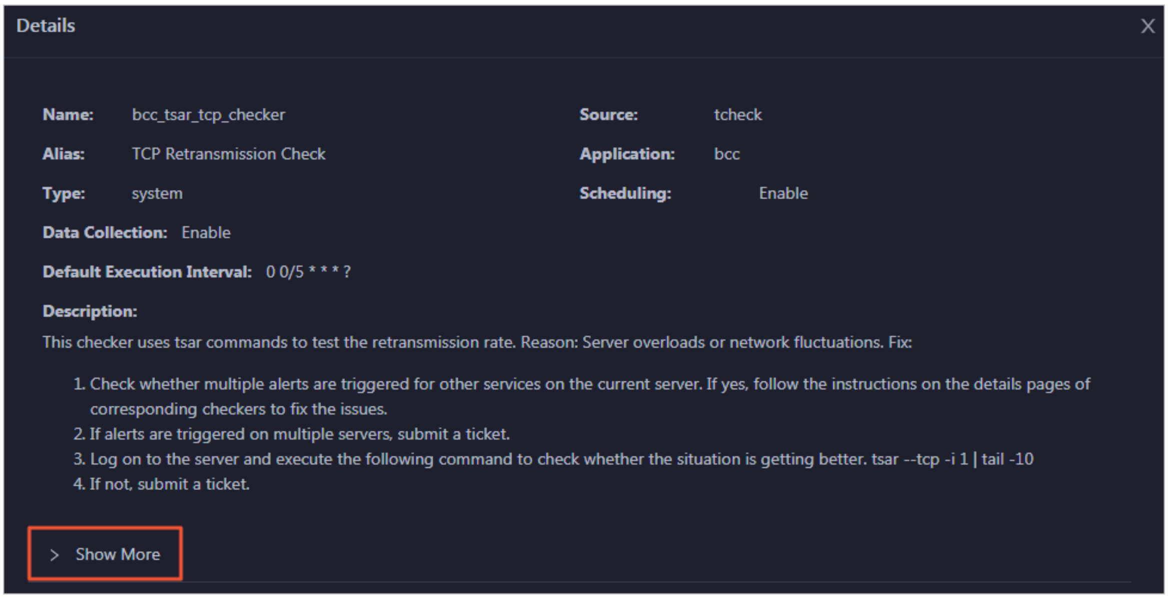
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include the name, source, alias, application, type, default execution interval, and description of the checker, whether scheduling is enabled, and whether data collection is enabled. The schemes to clear alerts are provided in the description.

2. Click **Show More** at the bottom to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

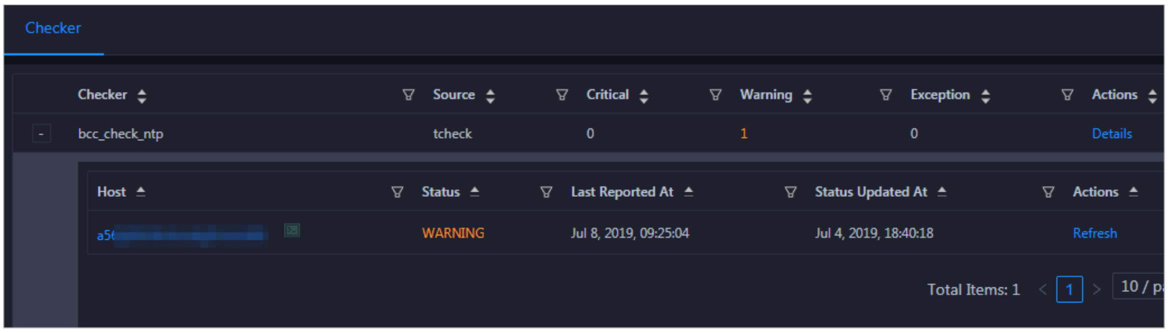
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about the execution script, execution target, default threshold, and mount point for data collection.

View alert causes

You can view the check history and check results of a checker.

1. On the Health Status page, click **+** to expand a checker with alerts.

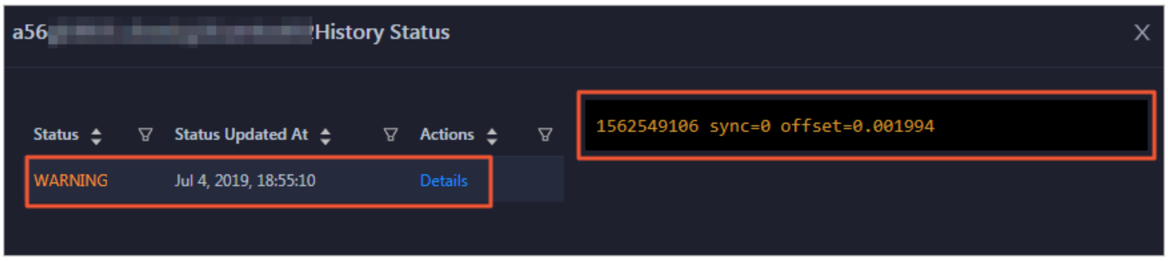


	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

2. Click the hostname. In the dialog box that appears, click **Details** in the Actions column of a check result to view the alert causes.



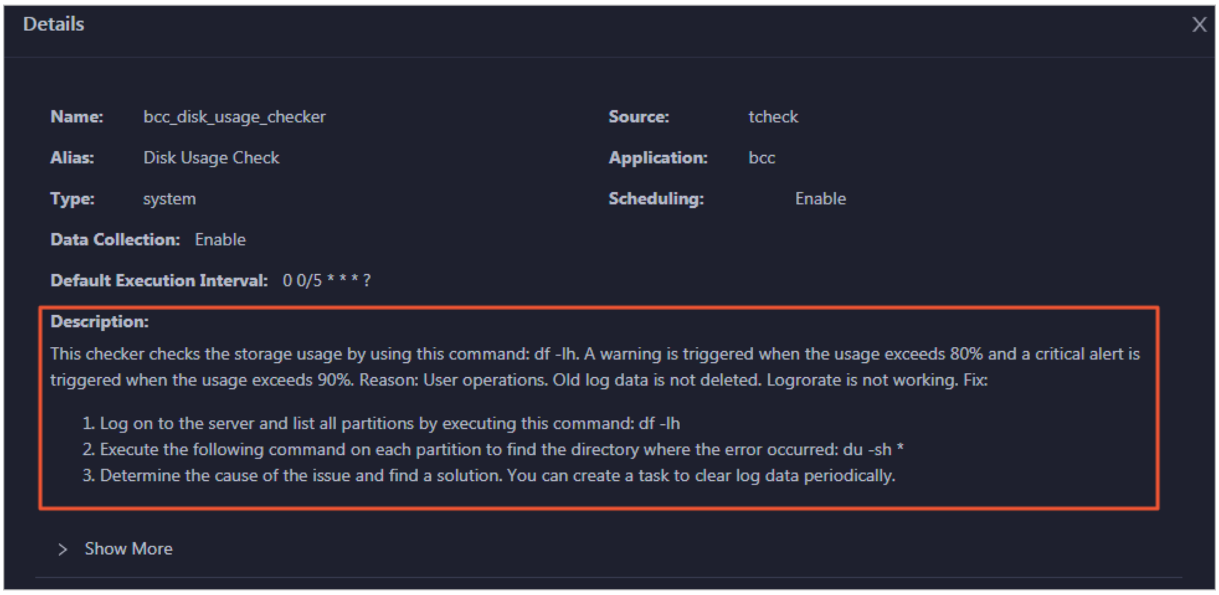
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status page, click **Details** in the Actions column of a checker with alerts. In the dialog box that appears, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

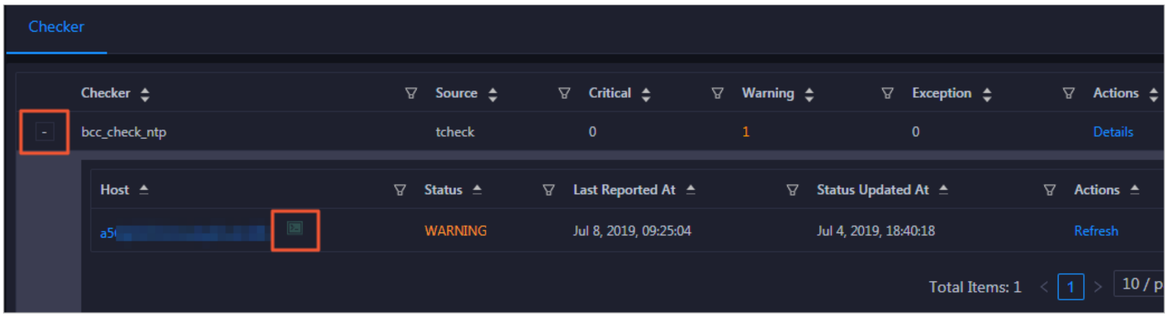
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

To log on to a host to clear alerts or perform other operations, follow these steps:

1. On the Health Status page, click **+** to expand a checker with alerts.



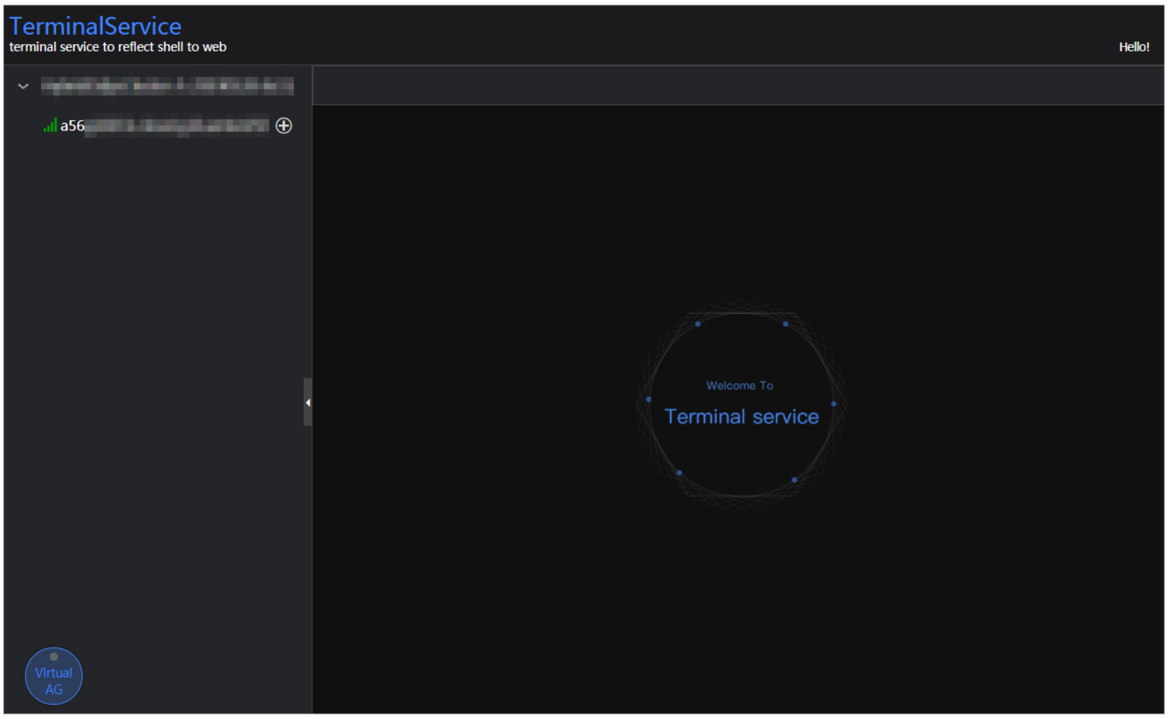
Checker

	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

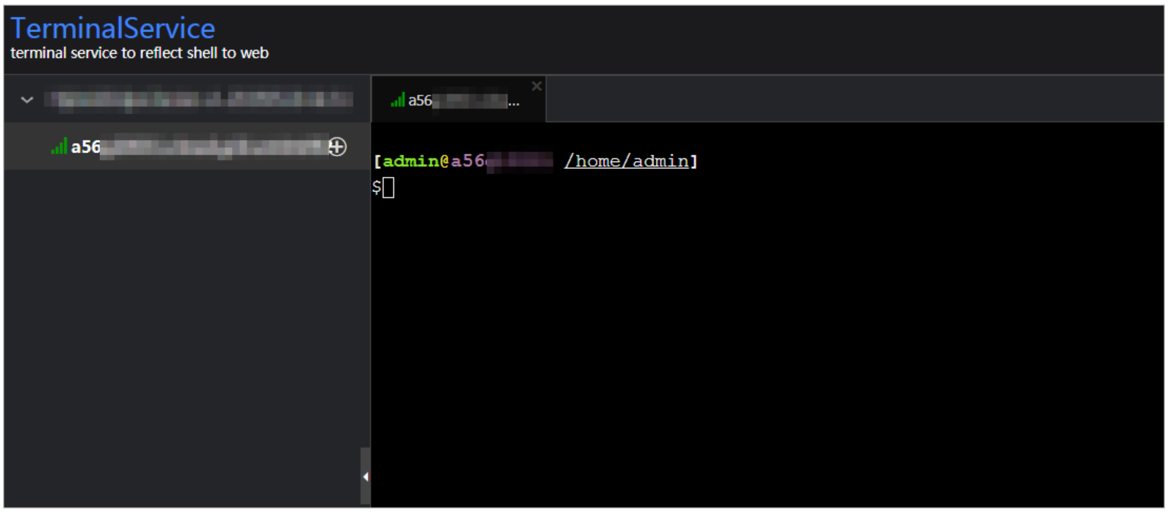
Total Items: 1 < 1 > 10 / p

2. Click the **Log On** icon of a host. The **TerminalService** page appears.



TerminalService
terminal service to reflect shell to web

3. On the **TerminalService** page, click the hostname on the left to log on to the host.

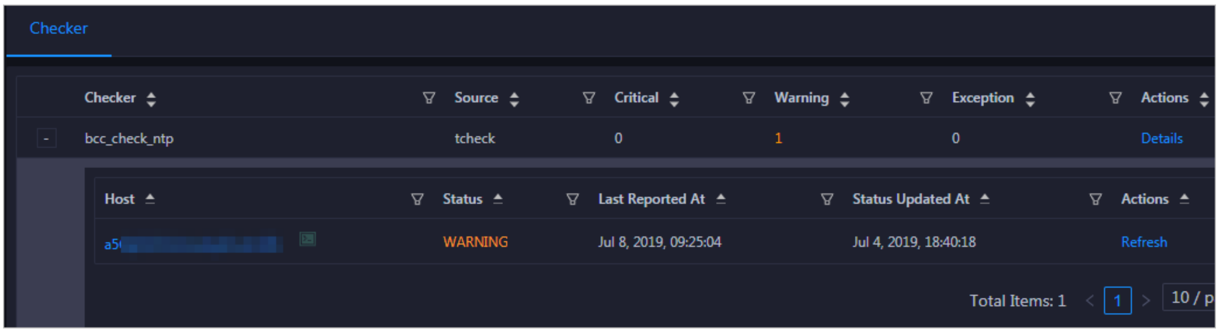


TerminalService
terminal service to reflect shell to web

```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. In this way, you can check whether the alert is cleared.



Checker

	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

11.9.4.7.5. Host services

On the Services page, you can view information about service instances and service instance roles of a host.

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Services** tab. The **Services** page for the host appears.

On the **Services** page, you can view the cluster, service instances, and service instance roles of the host.

11.9.5. Exceptions and solutions

This section describes some of the common error codes in the current version and corresponding solutions.

Error Code: LimitEceeded

Cause: The error code is returned because you can create up to 5 projects and 20 topics in a project in the previous version of DataHub.

Solution: In the latest version, you can create up to 10 projects and 1,000 topics in a project. Perform the following operations to change the project or topic limits:

1. Obtain the hostname of the ApsaraDB RDS for MySQL database from the following path: */home/admin/datahub/service/deploy/env.cfg*.
2. Access the corresponding ApsaraDB RDS for MySQL database. In the config_meta table, check the values of ProjectLimit4User and TopicLimit4Project.
3. Run the following commands to update the configurations. The new configurations take about 1 minute to take effect. You do not need to restart the database.

```
update config_meta set config_value = 10 where config_type = ‘ProjectLimit4User’ ;
```

```
update config_meta set config_value = 1000 where config_type = ‘TopicLimit4Project’ ;
```

Error code: IanlnvalidParameter

Cause: The error code is returned when StreamCompute attempts to capture records from DataHub by using an invalid timestamp. The timestamp you submit to the StreamCompute task is later than the current time, which may be caused by inaccurate local system time.

Solution: Correct your local system time by using the Network Time Protocol (NTP) or specify a timestamp that is for example 10 minutes earlier than the local system time.

Error code: InvalidCursor

Cause: The error code is returned when StreamCompute attempts to capture records from DataHub by using an invalid or expired cursor. An error may have occurred while StreamCompute is processing records from several days ago. When the time-to-live of the records expires and the records are deleted from DataHub, the cursor of these records is invalid.

Solution: Contact technical support for StreamCompute to learn about the cause of the task.

Error code: Parse response failed

Cause: This is probably caused by an invalid endpoint. For example, you may enter the console address as endpoint.

Solution: Perform a smoke test to check whether the system is running properly. If yes, check whether the endpoint is incorrect in the Apsara Infrastructure Management Framework console. Find the endpoint from the following path in the console: **DataHubCluster > Cluster Dashboard > Cluster Resource > Service: datahub-frontend > dns in the Parameters and Result columns.**

Error code: InternalServerError

Cause: Retry the smoke test or StreamCompute task. If the error code is still returned, an internal server error may occur. If the galaxy logs record this type of errors that occurred a long time ago, ignore these errors.

Solution: Use the following methods to search for corresponding logs to diagnose the issue. If you have any problems, screenshot the logs and contact technical support.

- In the logs directory of DataHubServer, search for the log files based on the specific time that the error occurred. The specific time can be found in the RequestId. RequestId is the unique ID of the request generated by DataHubServer.
- If more than one error occur, find the logs that are marked as **ERROR** in the logs directory of DataHubServer.

11.9.6. Appendix

11.9.6.1. Installation environment

Operation system: AliOS5U7-x86-64

Template: Bigdata

11.9.6.2. Deployment directories and services

Services

Name	Type	Description
service-datahub-service	Controller	The service that is used to deploy DataHub backend services and used as the admin gateway of Apsara system.
service-datahub-webconsole	Controller	The service that is used to deploy the DataHub console and configured on the same container as service-datahub-service.

Name	Type	Description
service-datahub-frontend	Worker	The service that is used to deploy frontend servers and used as chunk servers.
Chunkserver	Worker	The service that is used to deploy chunk servers in Apsara Distributed File System.
PanguMaster	Controller	The service that is used to deploy three masters in Apsara Distributed File System.
NuwaMaster	Controller	The service that is used to deploy three masters of Apsara Name Service and Distributed Lock Synchronization System.
FuxiMaster	Controller	The service that is used to deploy two masters of Job Scheduler.

Deployment directories and corresponding services

Module	Directory	Service
Datahub/XStreamServicex	/home/admin/datahub_service	service-datahub-service
Datahub/ShipperServicex	/home/admin/datahub_service	service-datahub-service
Datahub/CoordinatorServicex	/home/admin/datahub_service	service-datahub-service
WebConsole	/home/admin/datahub_webconsole	service-datahub-webconsole
Smoke	/home/admin/datahub_smoke	service-datahub-frontend
Frontend	/home/admin/datahub_frontend_server	service-datahub-frontend

11.9.6.3. Error codes

Error codes

Error code	HTTP status code	Description
InvalidUriSpec	400	The error code is returned when the request URI is invalid. This is probably caused by invalid topic or project names.
InvalidParameter	400	The error code is returned when a parameter is invalid. For more information about the cause of the error, see the error message.

Error code	HTTP status code	Description
Unauthorized	401	The error code is returned when the signature is incorrect. This is usually caused by an incorrect AccessKey or a time difference of more than 15 minutes between the client and the server.
NoPermission	403	The error code is returned when you do not have the permission to perform the operation.
InvalidSchema	400	The error code is returned when the schema format is invalid.
InvalidCursor	400	The error code is returned when the cursor is invalid or has expired.
NoSuchProject	404	The error code is returned when the specified project does not exist.
NoSuchTopic	404	The error code is returned when the specified topic does not exist.
NoSuchShard	404	The error code is returned when the specified shard ID does not exist.
ProjectAlreadyExist	400	The error code is returned when the project name already exists.
TopicAlreadyExist	400	The error code is returned when the topic name already exists.
InvalidShardOperation	405	The error code is returned when the operation on the shard is not allowed. For example, you are not allowed to write data into a shard when it is in Deactivated status.
LimitExceeded	400	The error code is returned when a specified threshold is exceeded. For example, you create no more than 512 shards in a topic and 20 topics in a project.
InternalServerError	500	The error code is returned when an unknown or internal error occurs or when the system is being upgraded. For more information about the cause of the error, obtain the request ID or search DataHub server logs for **InternalServerError**.

11.10. E-MapReduce (EMR)

11.10.1. Methods for logging on to O&M platforms

11.10.1.1. Log on to Apsara Infrastructure Management Framework

This topic describes how to log on to Apsara Infrastructure Management Framework.

Prerequisites

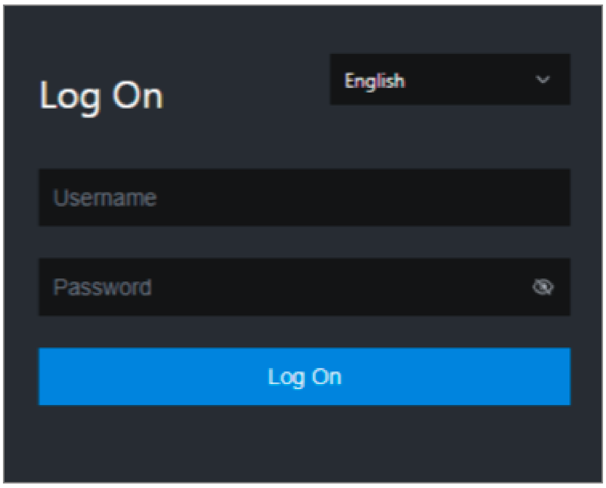
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.

   Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

   When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   For security reasons, your password must meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number

signs (#), dollar signs ($), and percent signs (%).

  - The password must be 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Product Management > Products**.
7. In the **Apsara Stack O&M** section, click **Apsara Infrastructure Management Framework**.

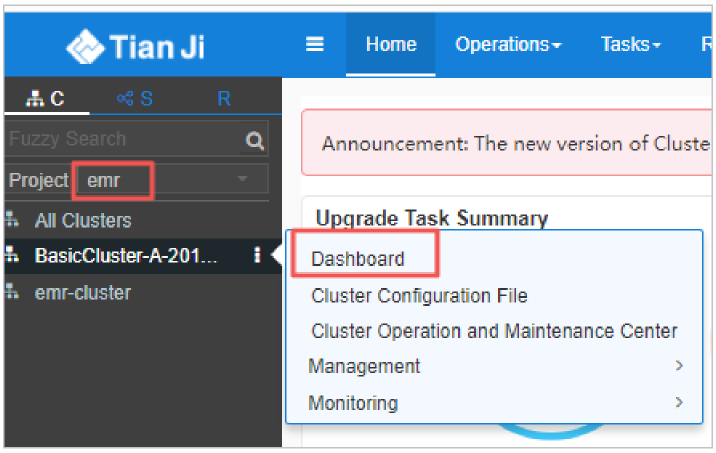
11.10.2. Routine maintenance

11.10.2.1. O&M in the Apsara Infrastructure Management Framework console

This topic describes how to perform O&M in the Apsara Infrastructure Management Framework console.

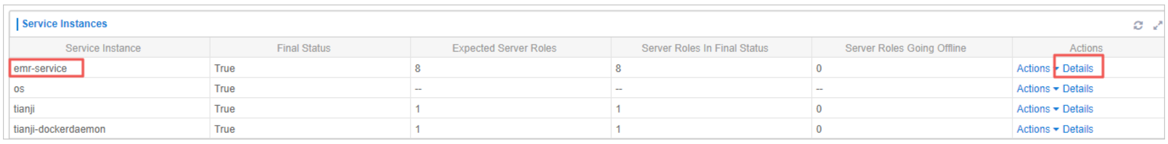
Procedure

1. Log on to the Apsara Infrastructure Management Framework console.
2. In the left-side navigation pane, click the C tab and select emr from the Project drop-down list.



Announcement: The new version of Cluste

3. Move the pointer over the ⁝ icon next to an EMR cluster and select **Dashboard** to go to the Cluster Dashboard page.
4. In the **Service Instances** section, click **Details** in the Actions column that corresponds to emr-service to go to the Service Instance Information Dashboard page.



Service Instances

Service Instance	Final Status	Expected Server Roles	Server Roles In Final Status	Server Roles Going Offline	Actions
emr-service	True	8	8	0	Actions ▾ Details
os	True	--	--	--	Actions ▾ Details
tianji	True	1	1	0	Actions ▾ Details
tianji-dockerdaemon	True	1	1	0	Actions ▾ Details

5. On the **Services** tab, find the **emr-service** service and click **Details** in the Action column.
6. On the **Service Details** page, click a server role.
7. In the **Machines** section, click **Restart Server Role** in the **Actions** column for a machine. Perform this operation for the other machines.The service is restarted.

11.10.3. Troubleshooting

11.10.3.1. Troubleshooting methods

If you detect a system fault during routine maintenance, read the Routine Maintenance part of this documentation for reference.

If you fail to rectify the fault, collect related information such as system information and fault symptoms and contact Alibaba Cloud technical support for help.

After you rectify a fault, analyze its causes, review the troubleshooting process, and make improvements.

11.11. Dataphin

11.11.1. What is Apsara Big Data Manager?

Apsara Big Data Manager (ABM) is an operations and maintenance (O&M) platform that is tailored for big data products. As an O&M tool for Dataphin, ABM allows you to perform O&M on Dataphin from a variety of perspectives such as the business, services, clusters, and hosts. In addition, ABM allows you to install patches for Dataphin, customize alert configurations, and view the O&M history.

Apsara Stack field engineers can manage Dataphin by using ABM. For example, they can view operational metrics, modify configurations, and check and handle alerts for Dataphin.

11.11.2. Log on to the ABM console

This topic describes how to log on to the Apsara Big Data Manager (ABM) console.

Prerequisites

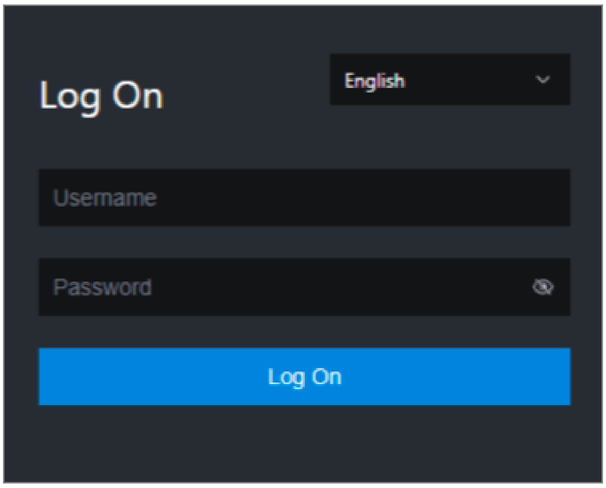
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.



Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

   When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   For security reasons, your password must meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password must be 10 to 20 characters in length.
4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Product Management** > **Products**.
7. In the **Big Data Services** section, choose **General-Purpose O&M** > **Apsara Big Data Manager**.

11.11.3. O&M overview and entry

This topic describes the O&M features of Dataphin and how to access the Dataphin O&M page.

Modules

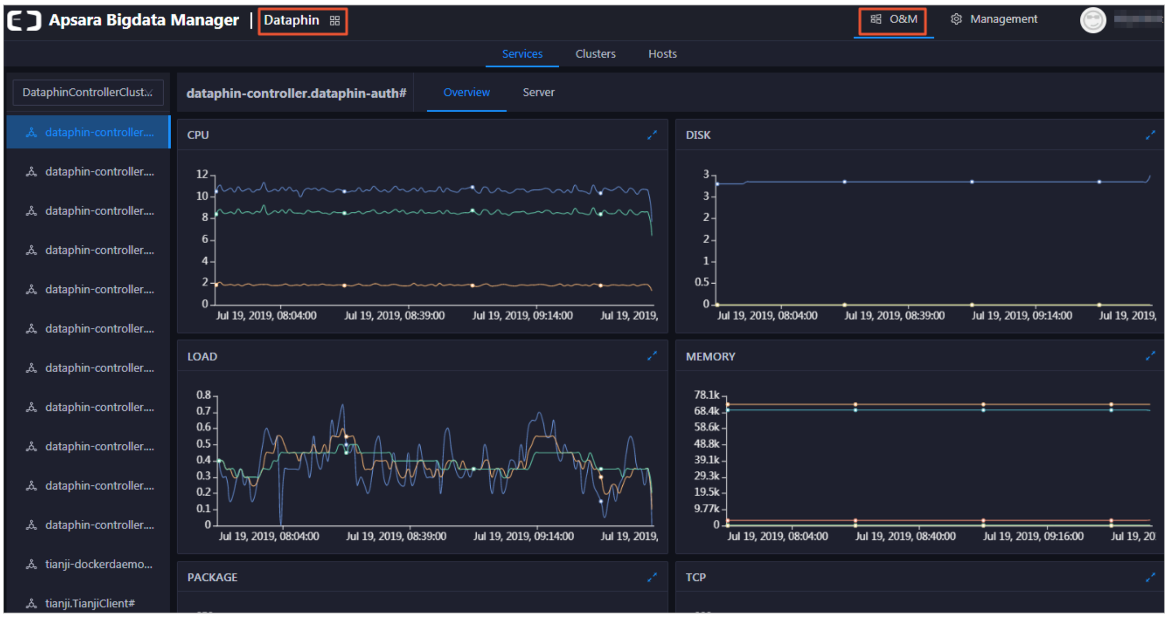
Dataphin O&M includes service O&M, cluster O&M, and host O&M. The following table describes them in detail.

Module	Feature	Description

Module	Feature	Description
Services	Overview	Displays the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for each service in a cluster.
	Server	Displays the host list of each service in a cluster so that you can understand the service deployment on hosts.
Clusters	Overview	Displays the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for a cluster.
	Health Status	Displays all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts. In addition, you can log on to a host and perform manual checks on the host.
Hosts	Overview	Displays the overall running and health check information about a host. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.
	Health Status	Displays the checkers of the selected host, including the checker details, check results, check history, and schemes to clear alerts. In addition, you can log on to the host and perform manual checks on the host.

Entry

1. Log on to the ABM console.
2. Click ⊞ in the upper-left corner and click **Dataphin**.
3. On the page that appears, click **O&M** in the top navigation bar. The **Services** page appears.



The **O&M** page includes three modules, namely, **Services**, **Clusters**, and **Hosts**.

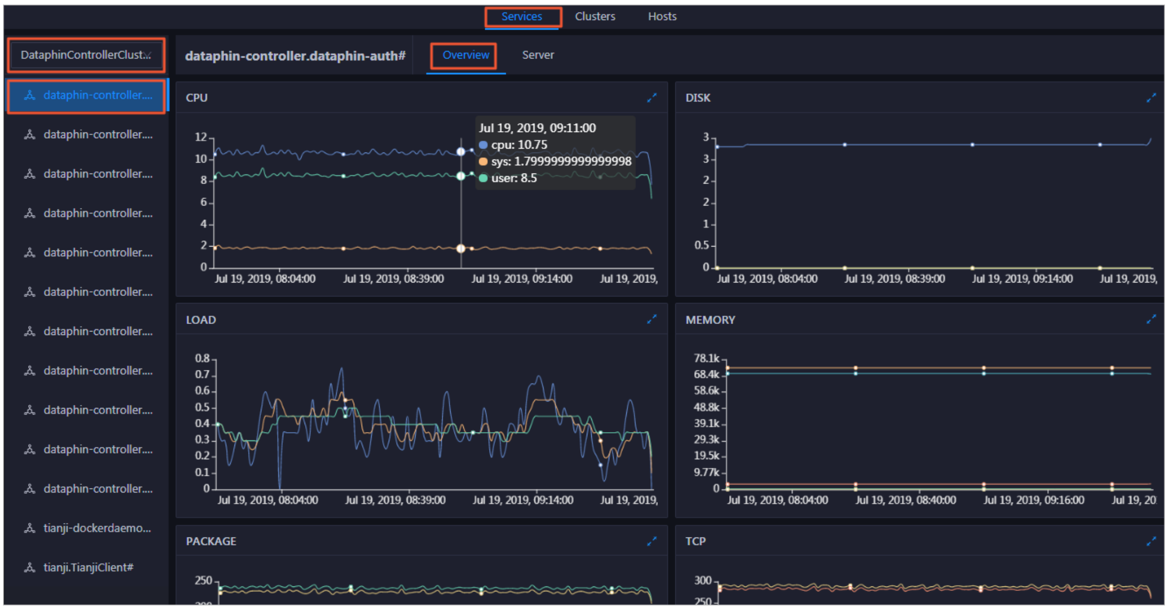
11.11.4. Service O&M

11.11.4.1. Service overview

The Overview tab lists all Dataphin services in a cluster. You can view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for each service.

Entry

1. At the top of the **O&M** page, click **Services**.
2. On the **Services** page, search for a cluster in the search box above the left-side service list, and then select a service in the service list.
3. Click the **Overview** tab to go to the **Overview** tab for the service.



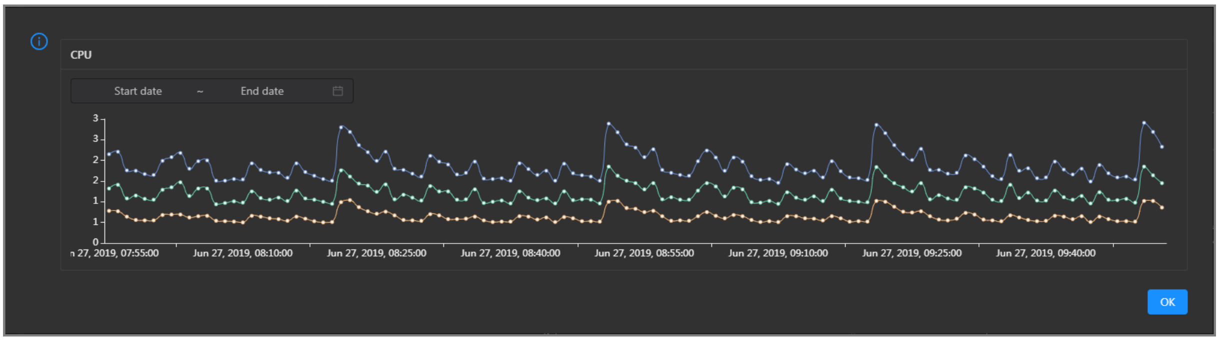
On the **Overview** tab, you can view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the selected service.

CPU

This chart displays the trend lines of the total CPU usage (cpu), CPU usage for executing code in kernel space (sys), and CPU usage for executing code in user space (user) for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

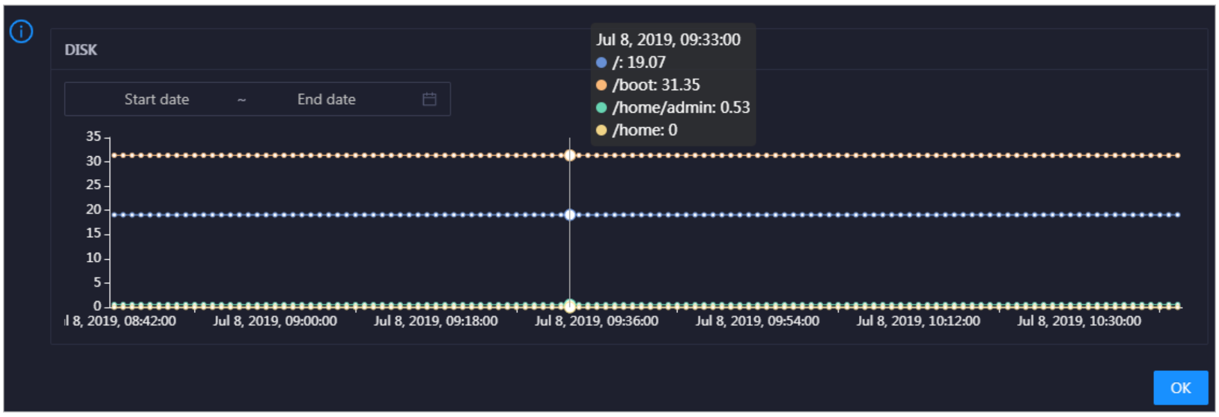
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU usage of the service in the specified period.



DISK

This chart displays the trend lines of the storage space usage on the */*, */boot*, */home/admin*, and */home* directories for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

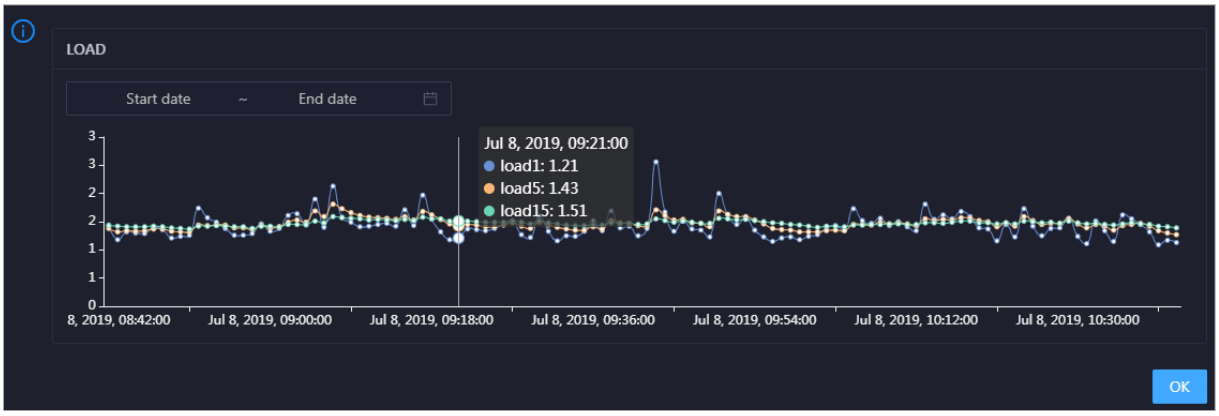


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage space usage of the service in the specified period.

LOAD

This chart displays the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

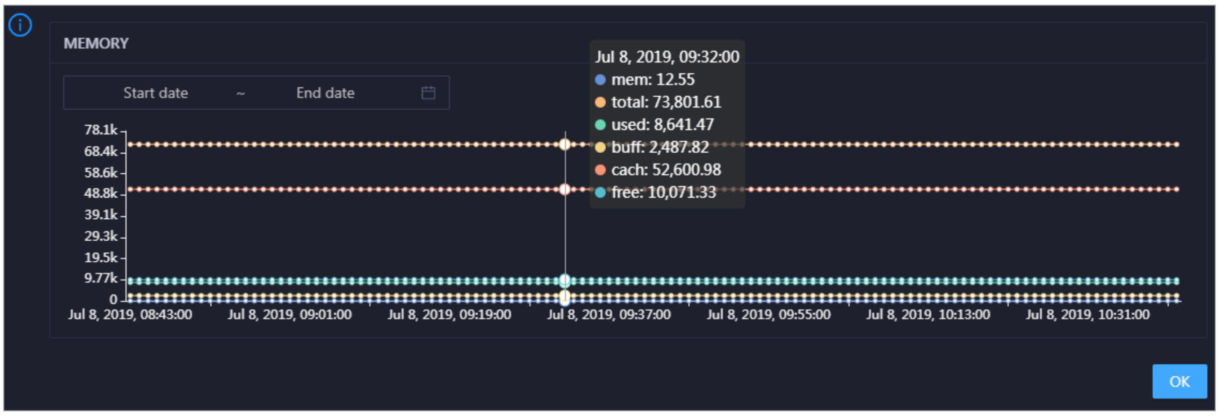


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the selected service in the specified period.

MEMORY

This chart displays the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

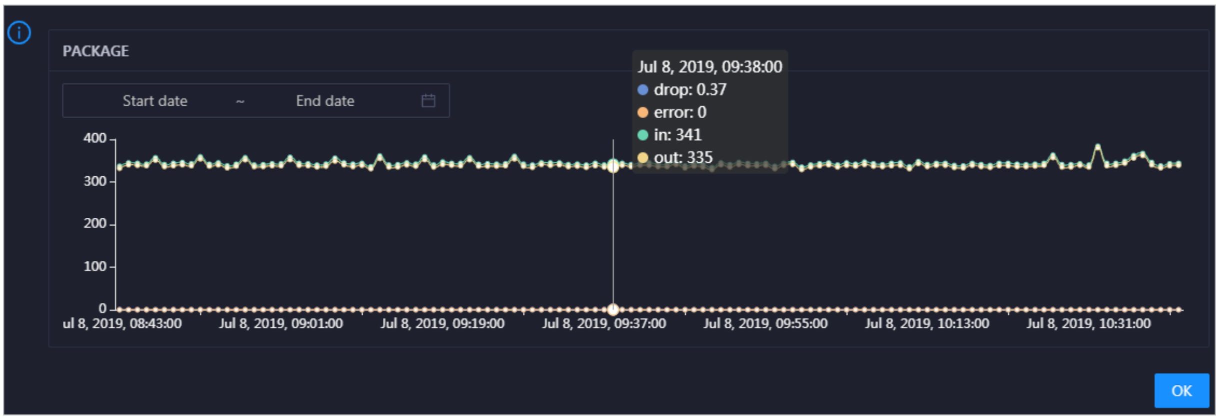


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the selected service in the specified period.

PACKAGE

This chart displays the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the selected service over time in different colors. These trend lines reflect the data transmission status of the service.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

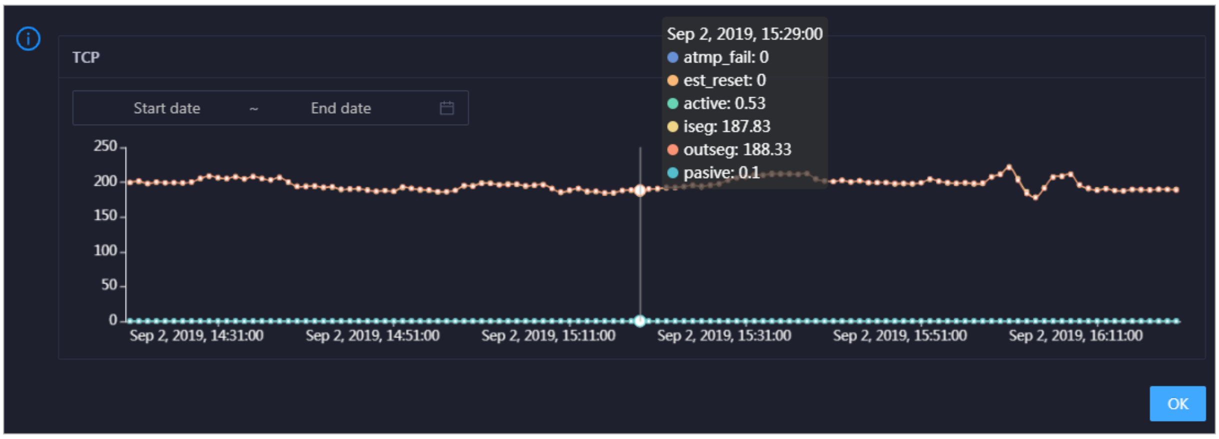


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the selected service in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the selected service over time in different colors. These trend lines reflect the TCP connection status of the service.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

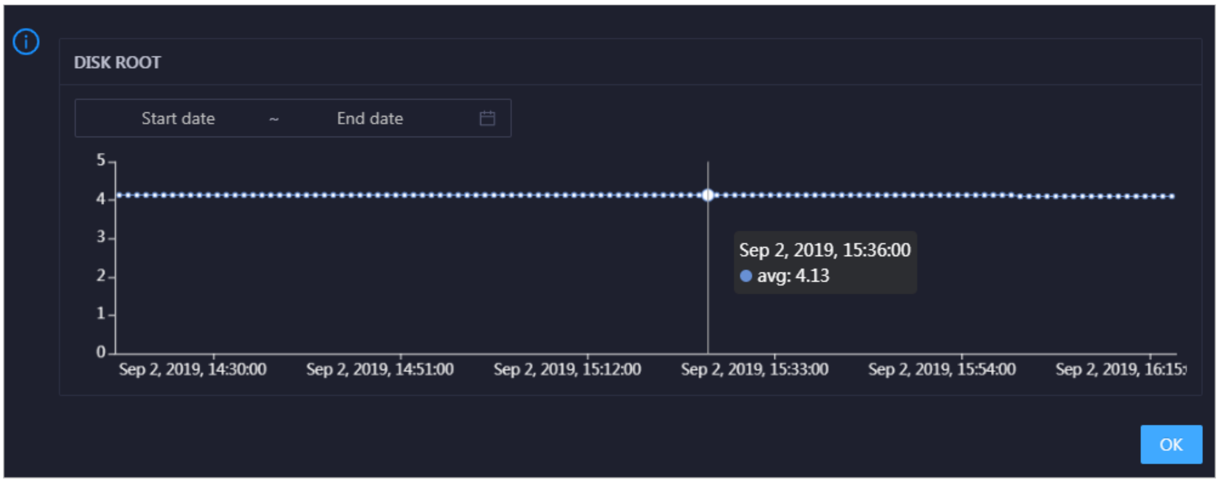


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the selected service in the specified period.

DISK ROOT

This chart displays the trend line of the average root disk usage (avg) for the selected service over time.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

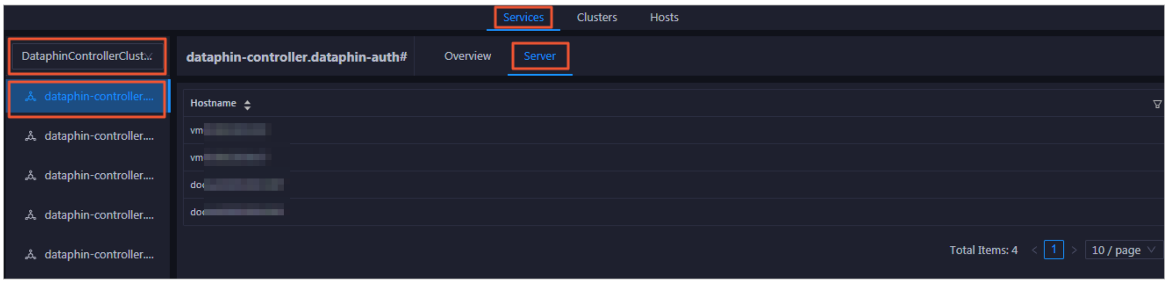


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the selected service in the specified period.

11.11.4.2. Service hosts

The Server tab allows you to view the host list of each Dataphin service so that you can understand the service deployment on hosts.

1. At the top of the **O&M** page, click **Services**.
2. On the **Services** page, search for a cluster in the search box above the left-side service list, and then select a service in the service list.
3. Click the **Server** tab to go to the **Server** tab for the service.



Hostname
vm[redacted]
vm[redacted]
do[redacted]
do[redacted]

Total Items: 4 1 10 / page

On the **Server** tab, you can view the hosts where the selected service is run.

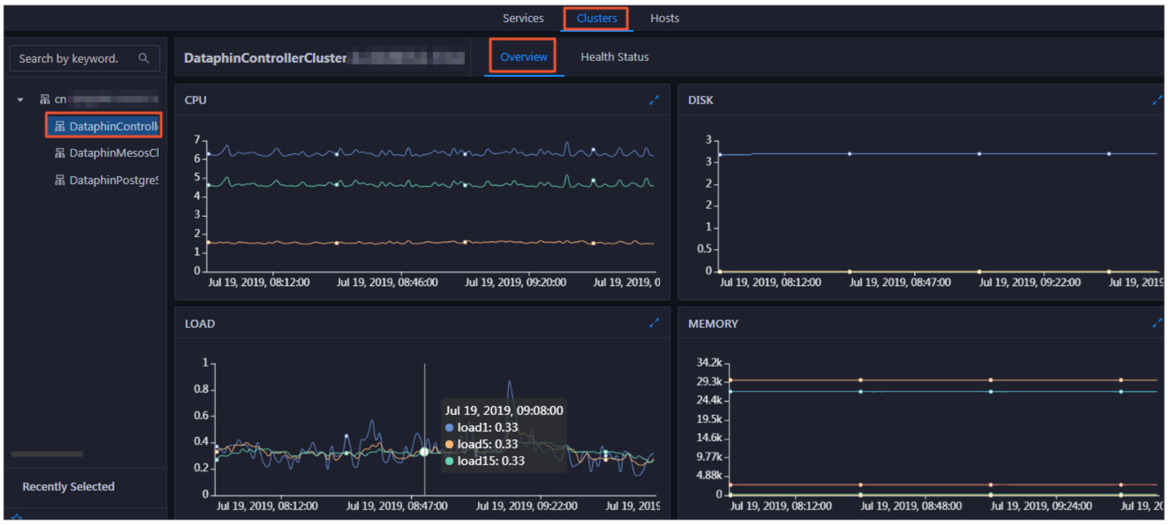
11.11.5. Cluster O&M

11.11.5.1. Cluster overview

The Overview tab displays the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for a cluster.

Entry

1. At the top of the **O&M** page, click **Clusters**.
2. On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Overview** tab.

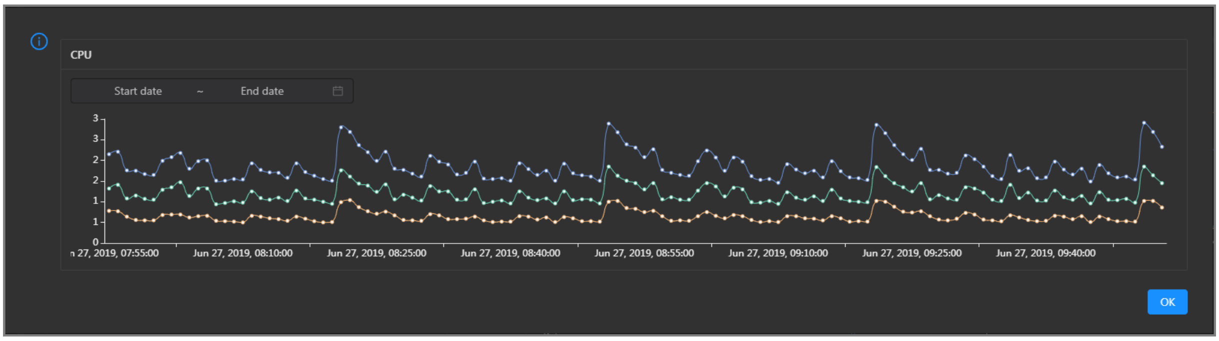


CPU

This chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

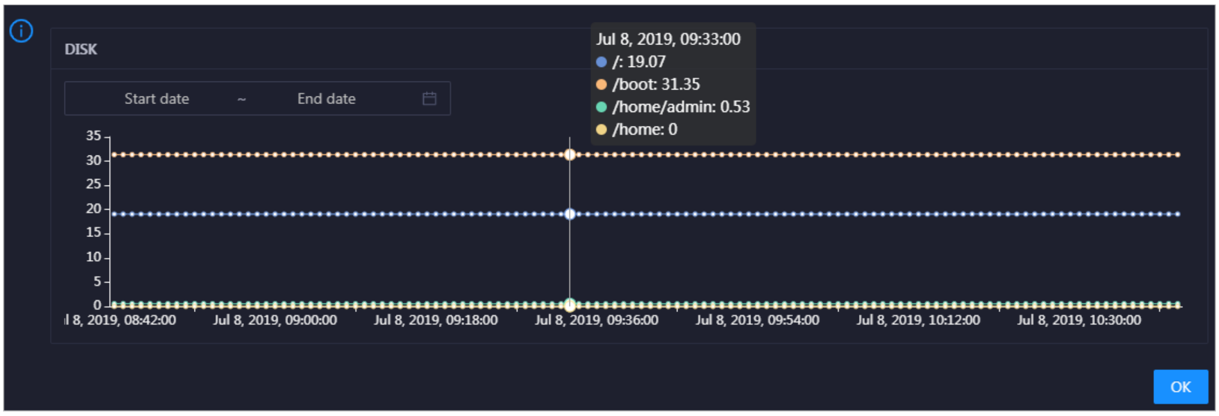
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the cluster in the specified period.



DISK

This chart shows the trend lines of the storage usage on the */*, */boot*, */home/admin*, and */home* directories for the cluster over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

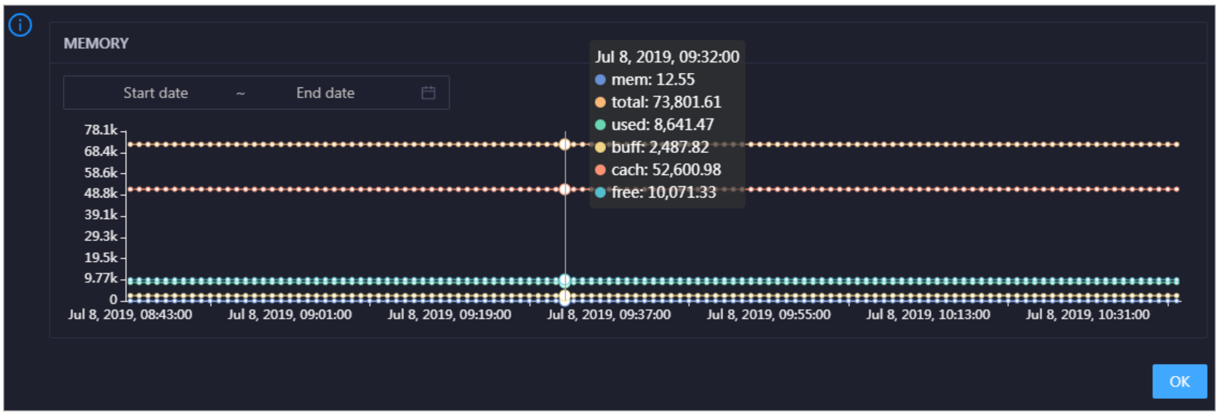


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

MEMORY

This chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

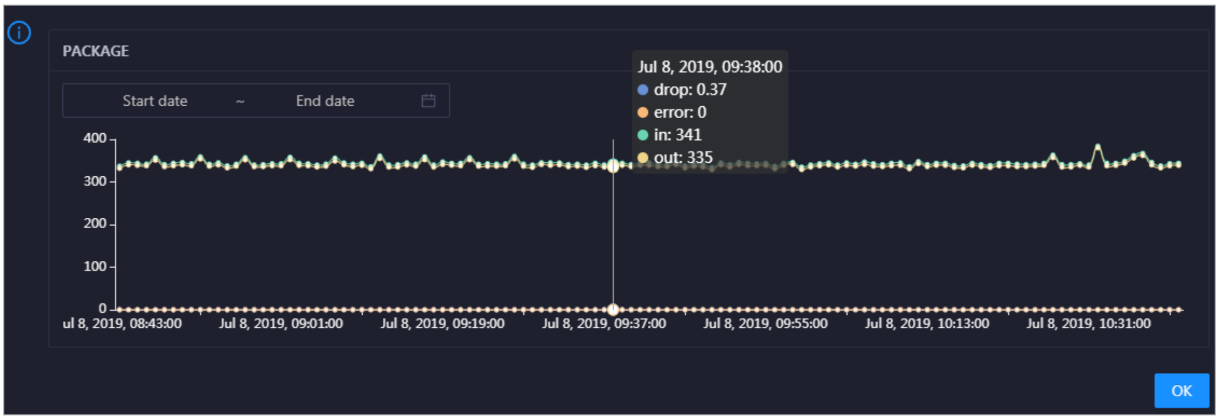


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the cluster in the specified period.

PACKAGE

This chart shows the trend lines of the numbers of dropped packets (drop), error packets (error), received packets (in), and sent packets (out) for the cluster in different colors. These trend lines reflect the data transmission status of the cluster.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

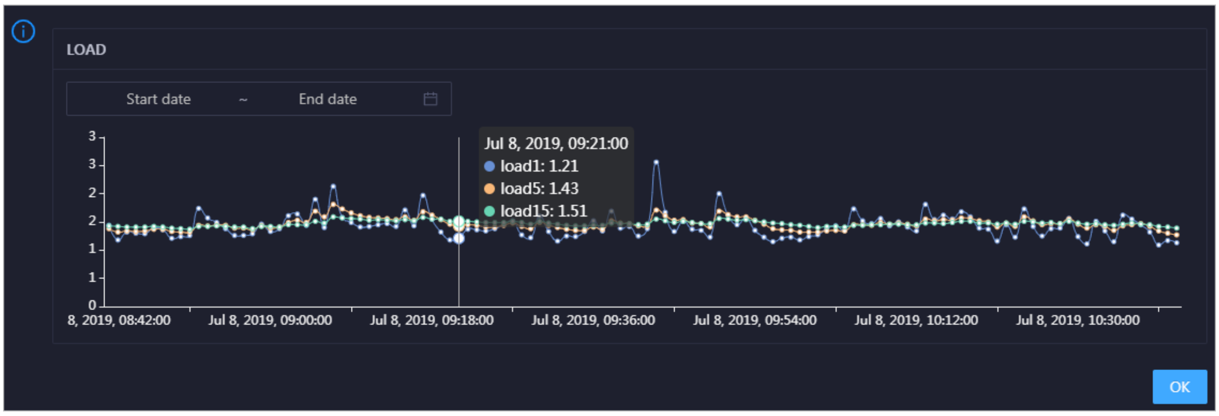


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the cluster in the specified period.

LOAD

This chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



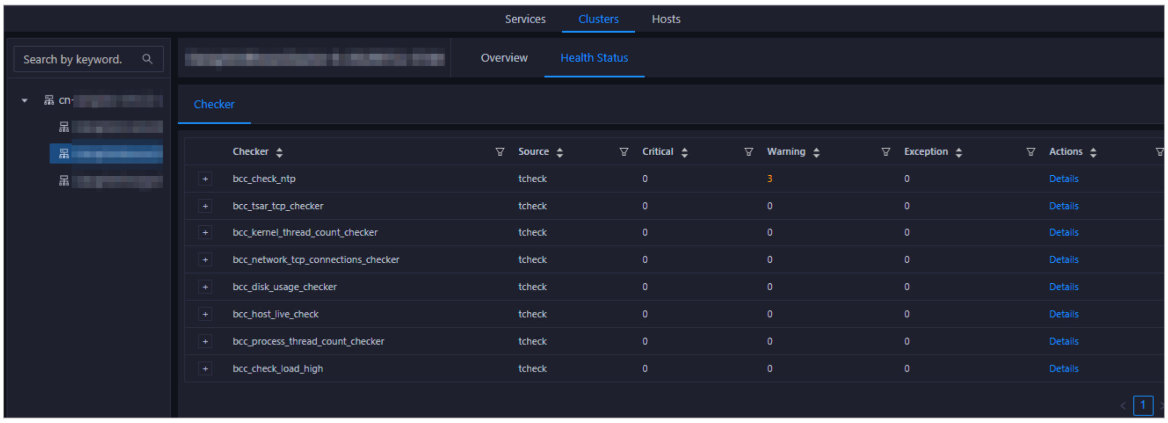
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the cluster in the specified period.

11.11.5.2. Cluster health

On the Health Status tab, you can view all checkers of a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts. In addition, you can log on to a host and perform manual checks on the host.

Entry

1. At the top of the **O&M** page, click **Clusters**.
2. On the **Clusters** page, select a cluster in the left-side navigation pane, and then click the **Health Status** tab.

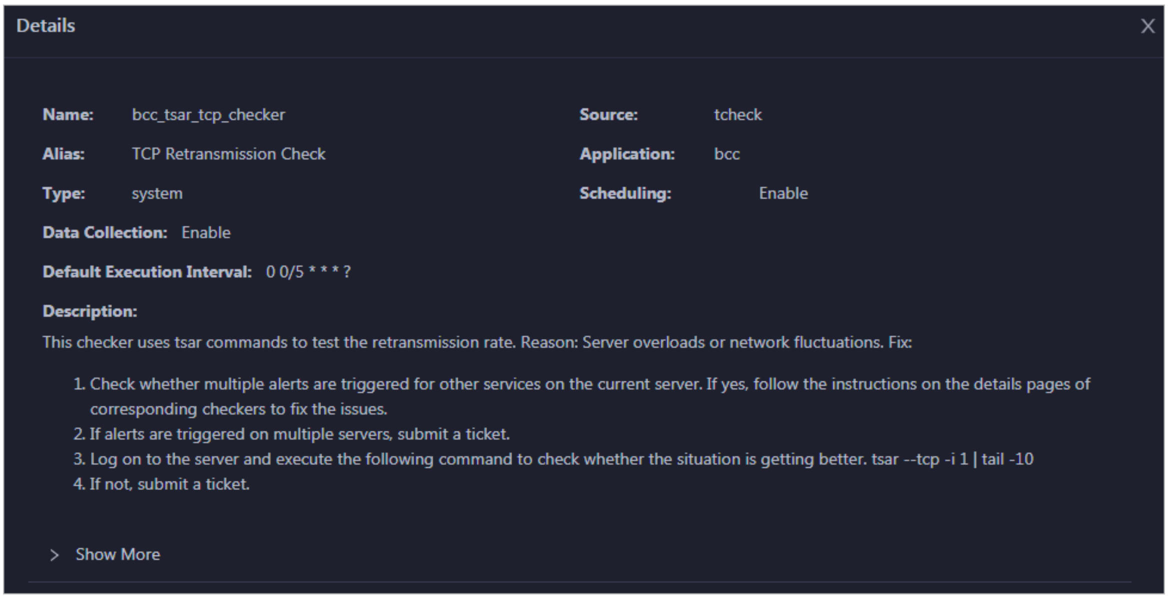


	Checker	Source	Critical	Warning	Exception	Actions
+	bcc_check_ntp	tcheck	0	3	0	Details
+	bcc_tsar_tcp_checker	tcheck	0	0	0	Details
+	bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
+	bcc_network_tcp_connections_checker	tcheck	0	0	0	Details
+	bcc_disk_usage_checker	tcheck	0	0	0	Details
+	bcc_host_live_check	tcheck	0	0	0	Details
+	bcc_process_thread_count_checker	tcheck	0	0	0	Details
+	bcc_check_load_high	tcheck	0	0	0	Details

On the **Health Status** tab, you can view all checkers for the cluster and the check results for the hosts in the cluster. The following alerts may be reported on a host: **CRITICAL**, **WARNING**, and **EXCEPTION**. The alerts are represented in different colors. You must handle the alerts in a timely manner, especially the **CRITICAL** and **WARNING** alerts.

View checker details

1. On the Health Status tab, click **Details** in the Actions column of a checker. On the Details page, view checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

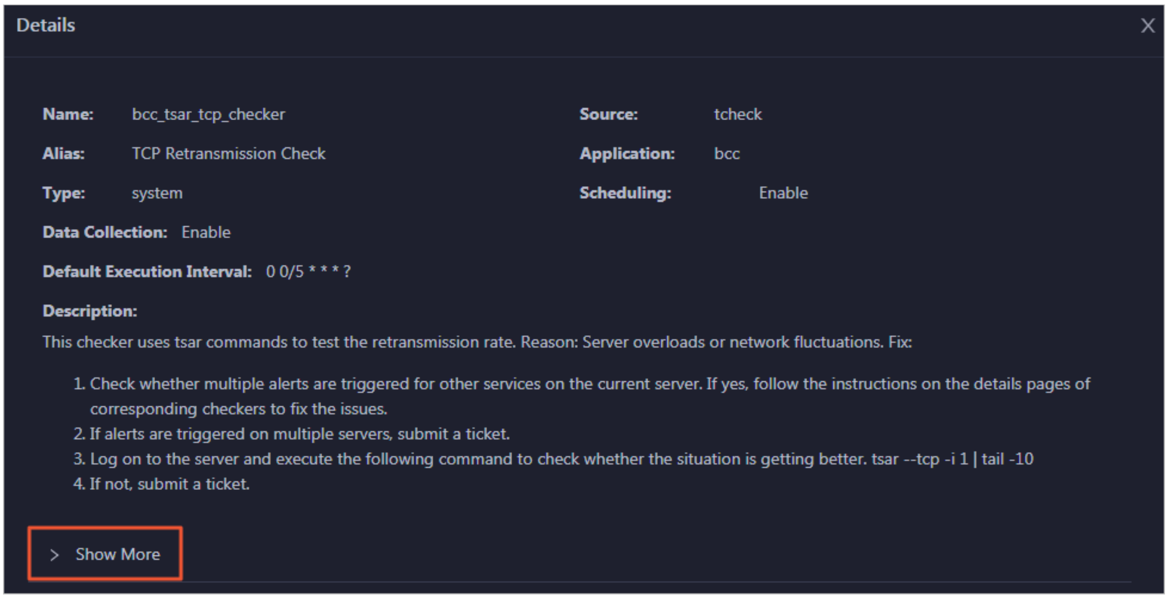
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include **Name**, **Source**, **Alias**, **Application**, **Type**, **Scheduling**, **Data Collection**, **Default Execution Interval**, and **Description**. The schemes to clear alerts are provided in the description.

2. Click **Show More** to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

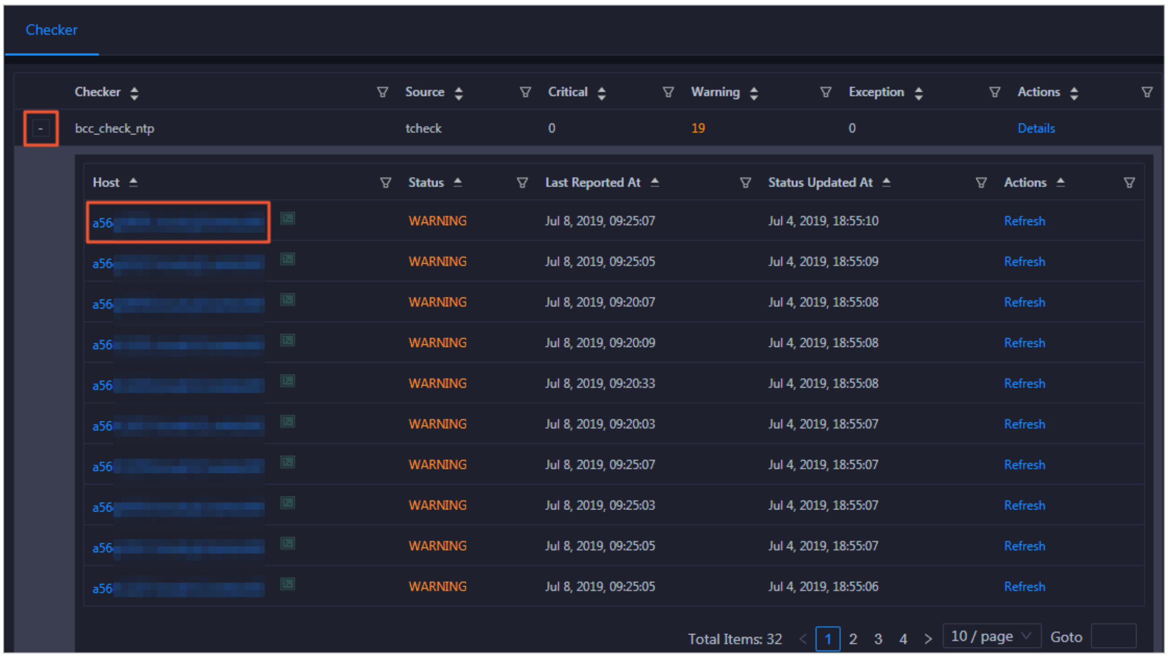
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about **Script**, **Target (TianJi)**, **Default Threshold**, and **Mount Point**.

View the hosts for which alerts are reported and causes for the alerts

You can view the check history and check results of a checker on a host.

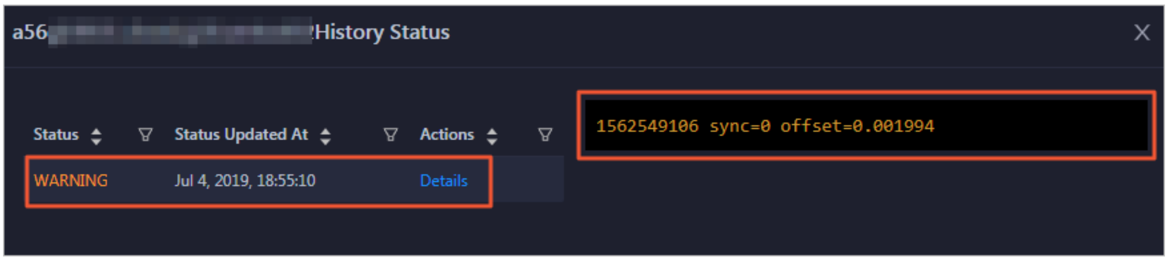
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported. You can view all hosts where the checker is run.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:06	Refresh

2. Click a hostname. In the panel that appears, click **Details** in the Actions column of a check result to view the cause of the alert.



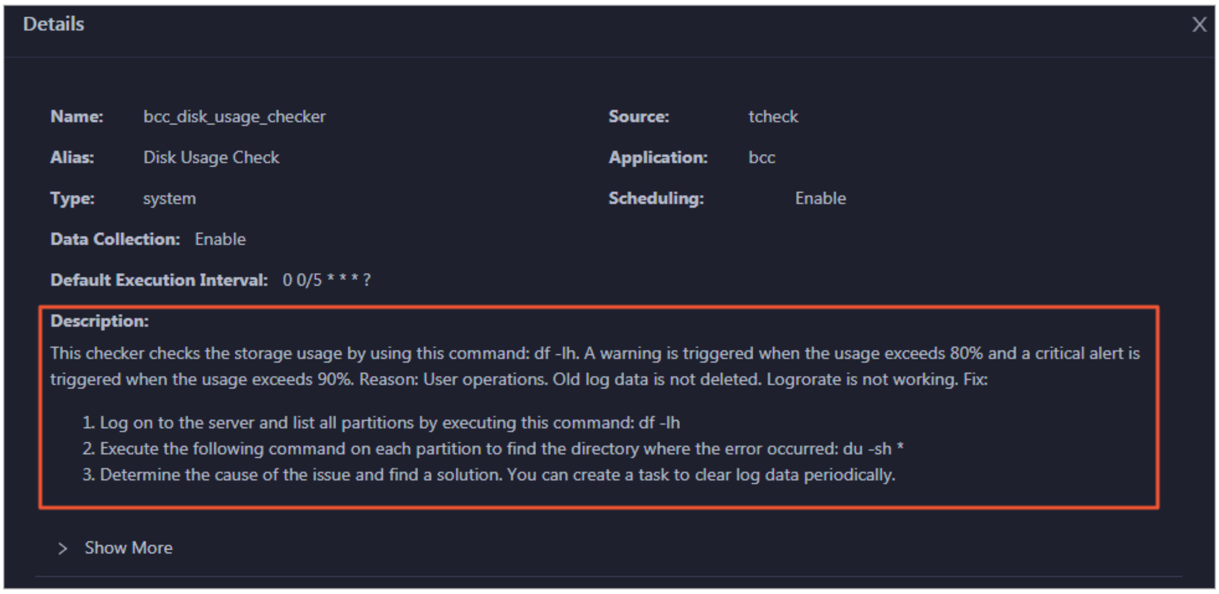
a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status tab, click **Details** in the Actions column of a checker for which alerts are reported. On the Details page, view the schemes to clear alerts.



Details

Name: bcc_disk_usage_checker

Alias: Disk Usage Check

Type: system

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Source: tcheck

Application: bcc

Scheduling: Enable

Description:

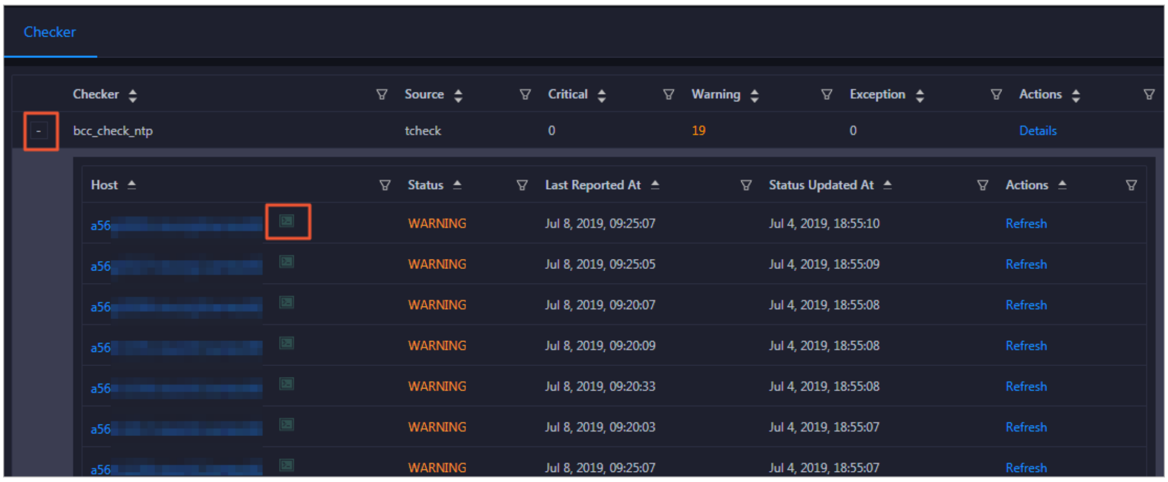
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

You may need to log on to a host to handle alerts or other issues that occurred on the host.

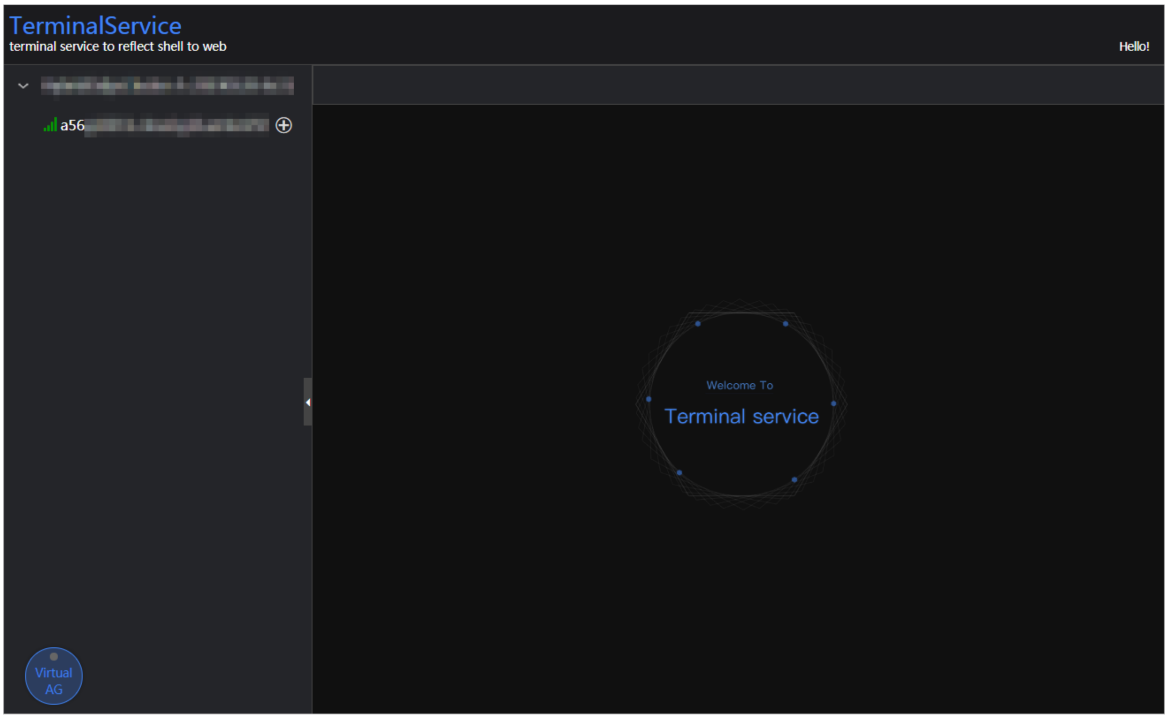
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported.



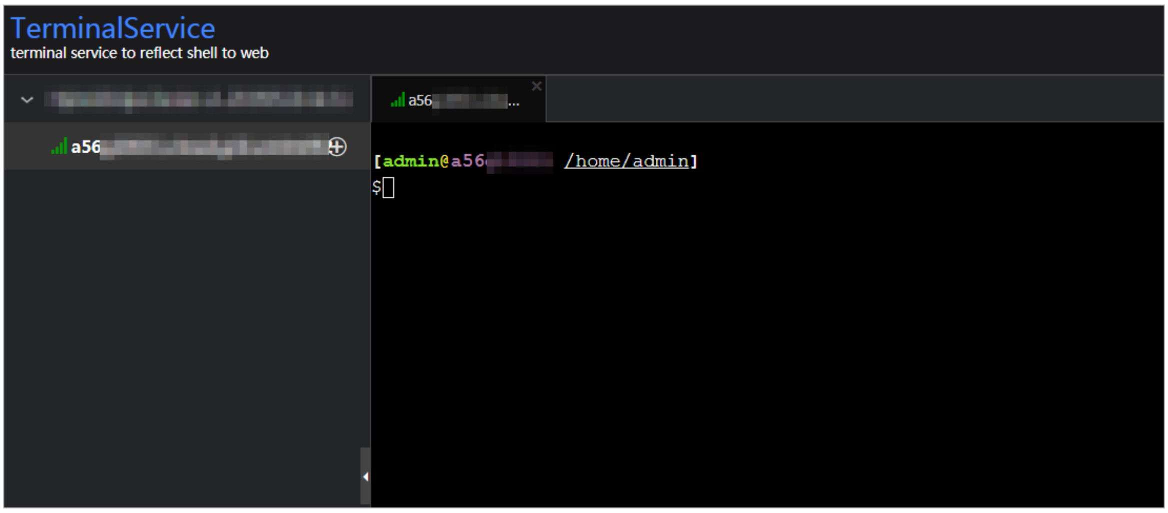
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

2. Click the **Login in** icon of a host. The **TerminalService** page appears.



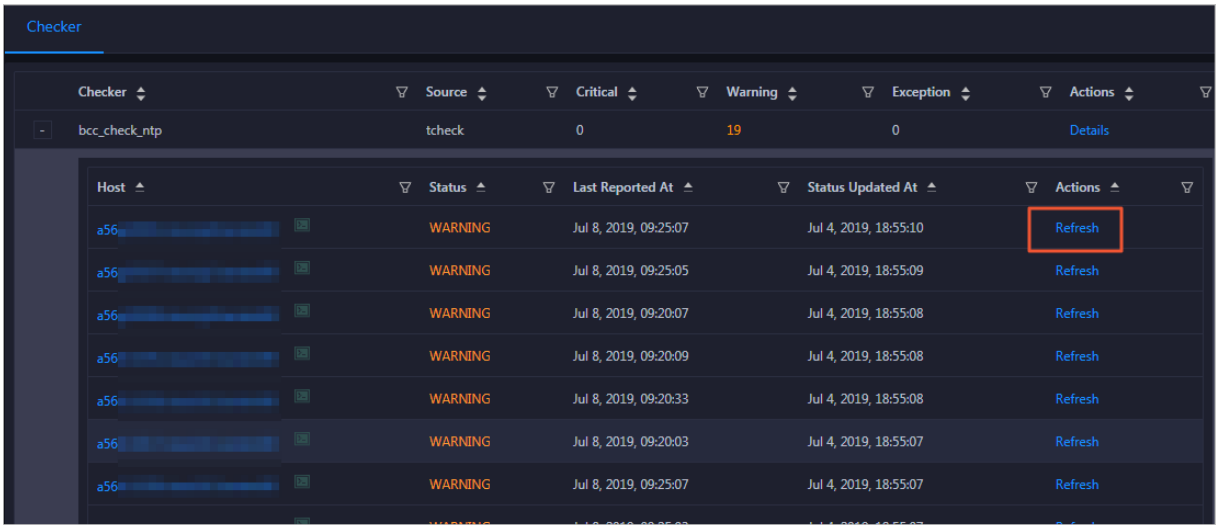
3. On the **TerminalService** page, click the hostname in the left-side navigation pane to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. This way, you can check whether the alert is cleared.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

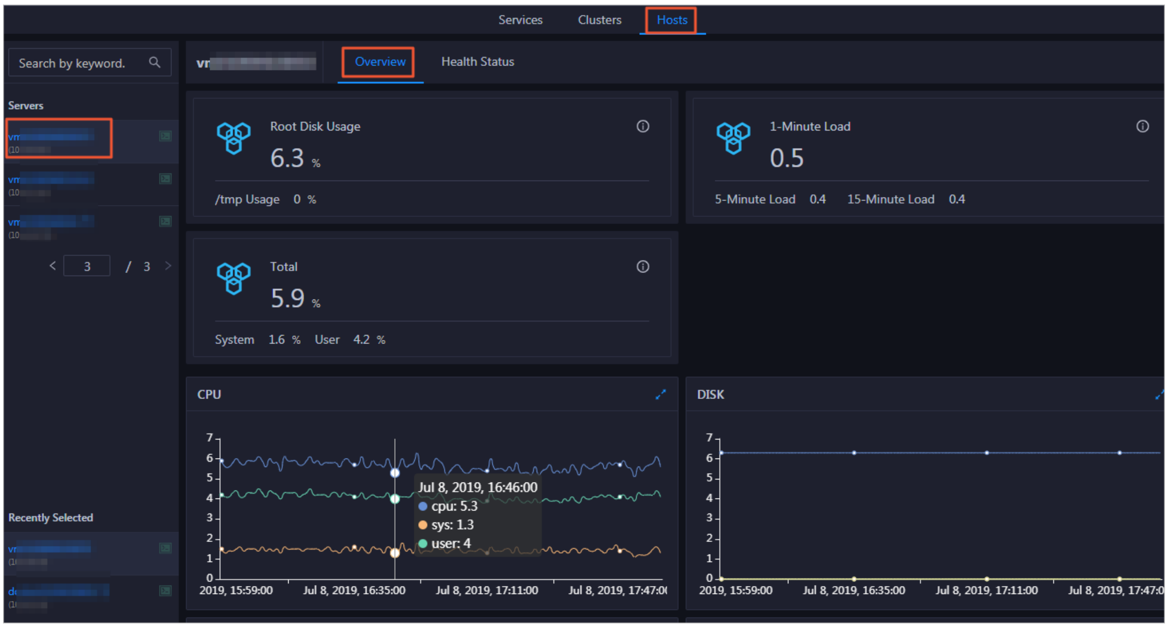
11.11.6. Host O&M

11.11.6.1. Host overview

The Overview tab displays the overall running and health check information about a host in a Dataphin cluster. On this page, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.

Entry

1. At the top of the **O&M** page, click **Hosts**.
2. On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Overview** tab.



Root Disk Usage 6.3 %

/tmp Usage 0 %

1-Minute Load 0.5

5-Minute Load 0.4 15-Minute Load 0.4

Total 5.9 %

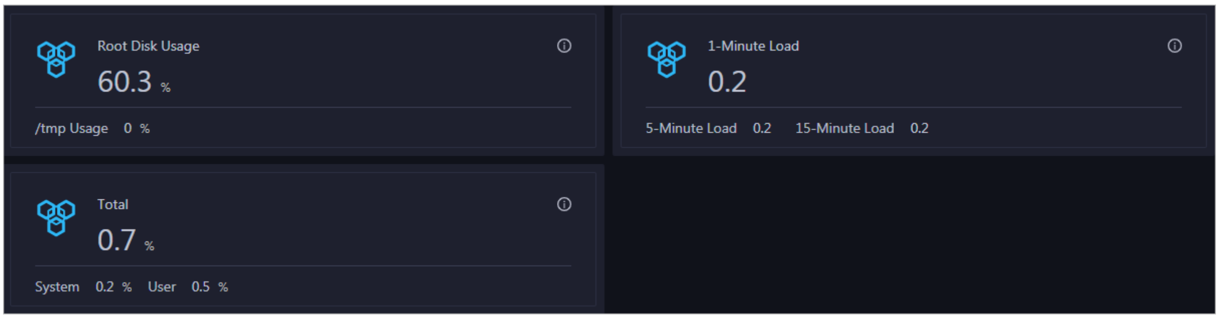
System 1.6 % User 4.2 %

Jul 8, 2019, 16:46:00
cpu: 5.3
sys: 1.3
user: 4

On the **Overview** tab, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the host.

Root Disk Usage, Total, and 1-Minute Load

These sections display the root disk usage, total usage, and 1-minute load for the selected host. The Root Disk Usage section provides the usage of the */tmp* directory. The Total section provides the system usage and user usage. The 1-Minute Load section provides the 1-minute, 5-minute, and 15-minute load averages.



Root Disk Usage
60.3 %
/tmp Usage 0 %

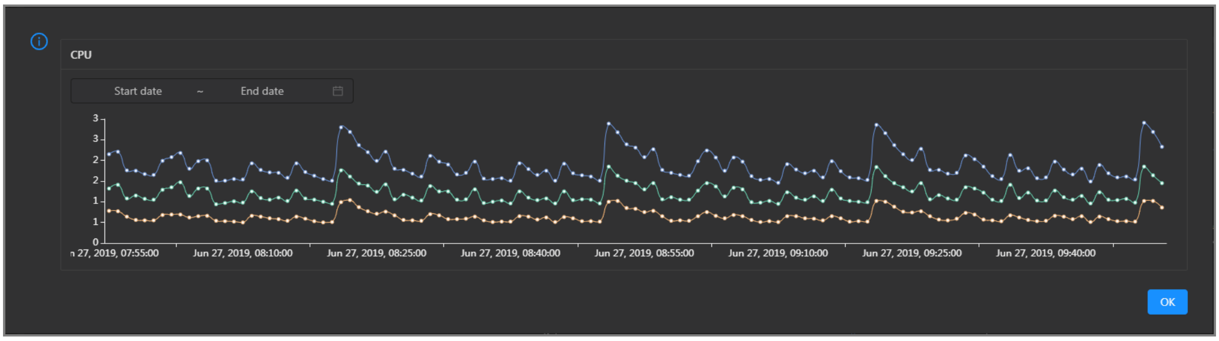
1-Minute Load
0.2
5-Minute Load 0.2 15-Minute Load 0.2

Total
0.7 %
System 0.2 % User 0.5 %

CPU

The CPU chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) of the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

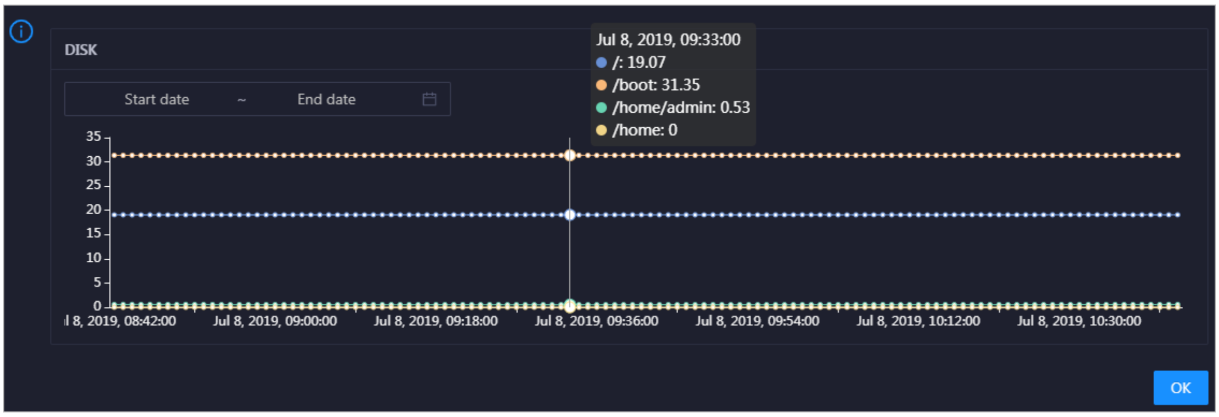


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the host in the specified period.

DISK

The DISK chart shows the trend lines of the storage usage in the */*, */boot*, */home/admin*, and */home* directories for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

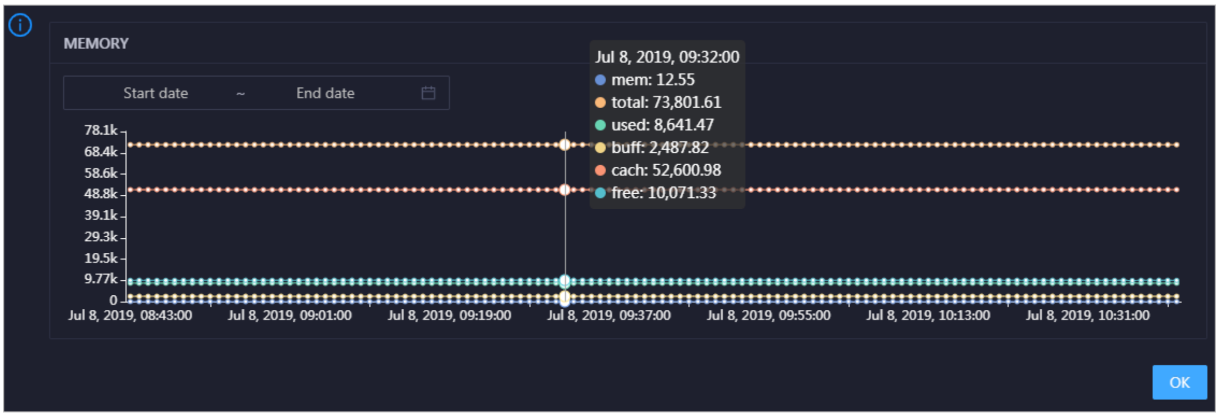


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the host in the specified period.

MEMORY

The MEMORY chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

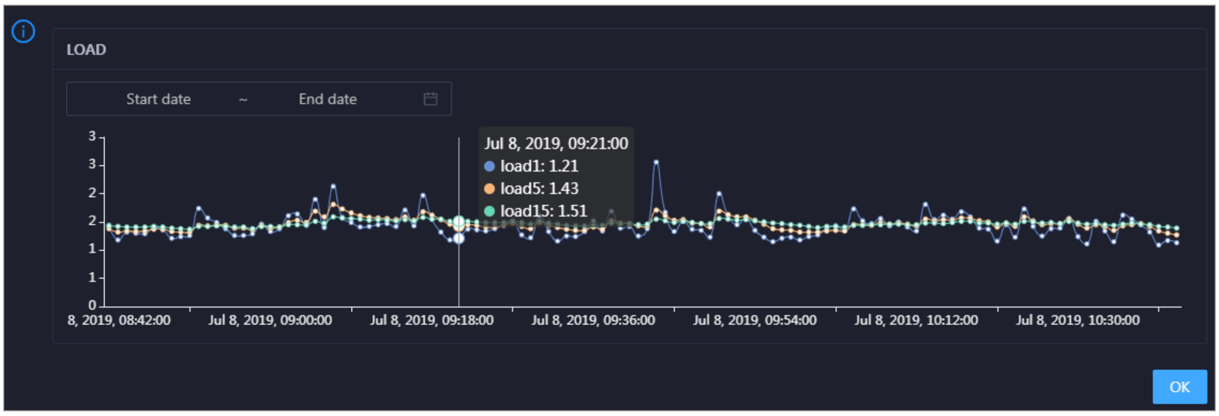


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the host in the specified period.

LOAD

The LOAD chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

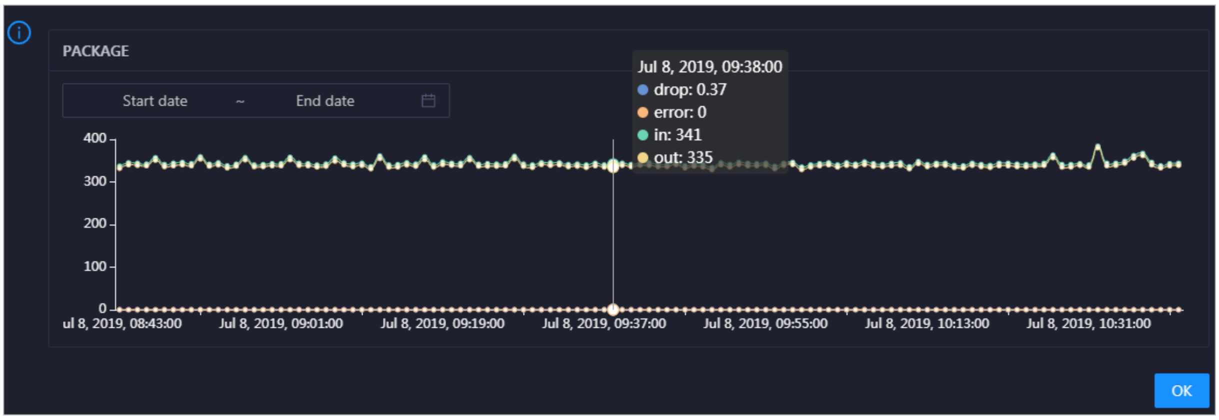


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the host in the specified period.

PACKAGE

The PACKAGE chart shows the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the host over time in different colors. These trend lines reflect the data transmission status of the host.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

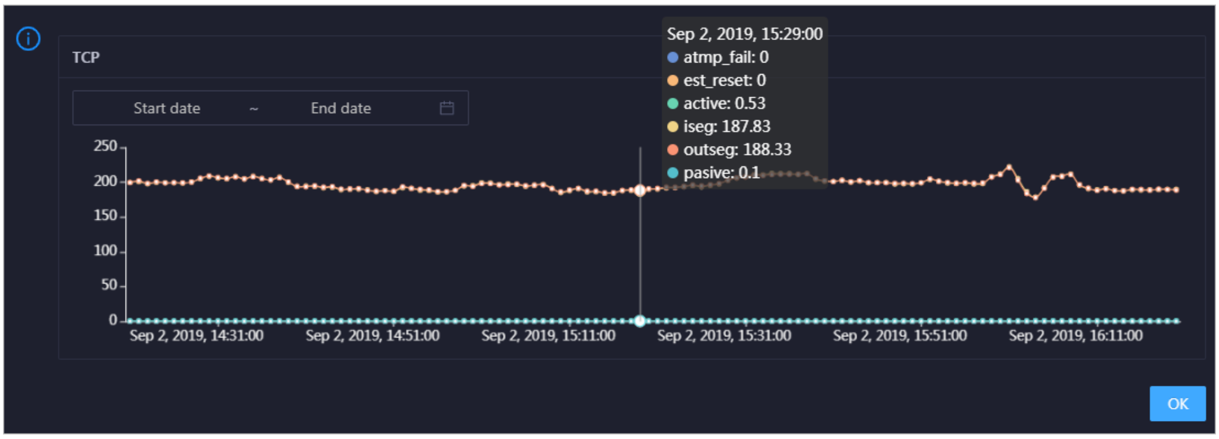


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the host in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the host over time in different colors. These trend lines reflect the TCP connection status of the host.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

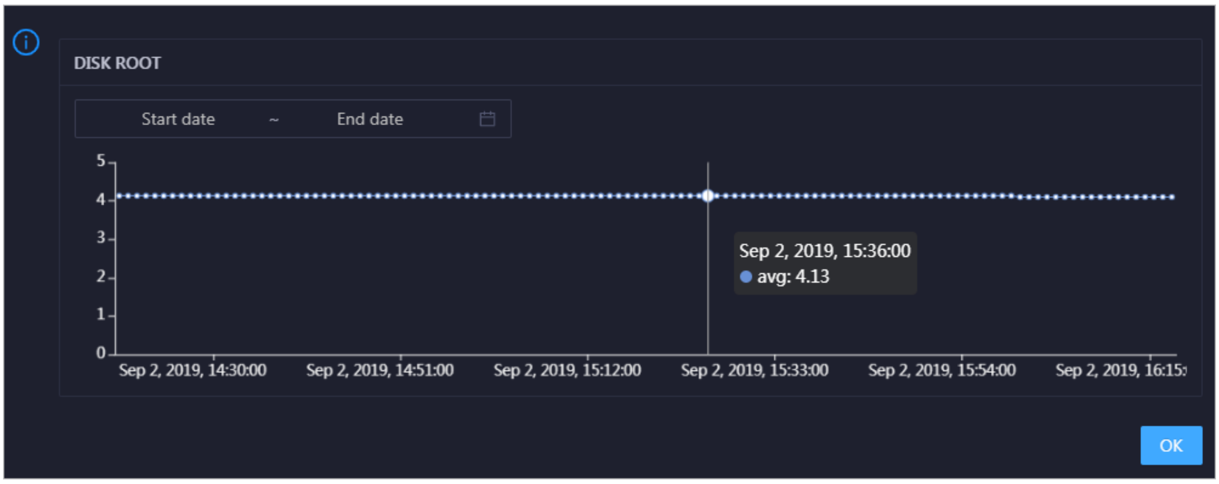


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the host in the specified period.

DISK ROOT

This chart displays the trend line of the average usage of the root disk (/) for the host over time.

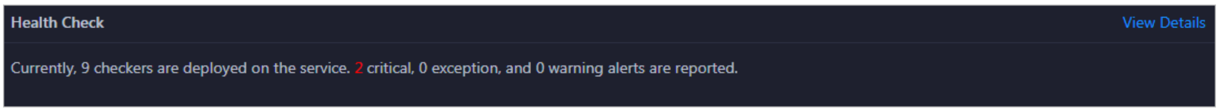
Click ⤢ in the upper-right corner of the chart to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the host in the specified period.

Health Check

This section displays the number of checkers deployed for the host and the respective number of Critical, Warning, and Exception alerts.


Health Check

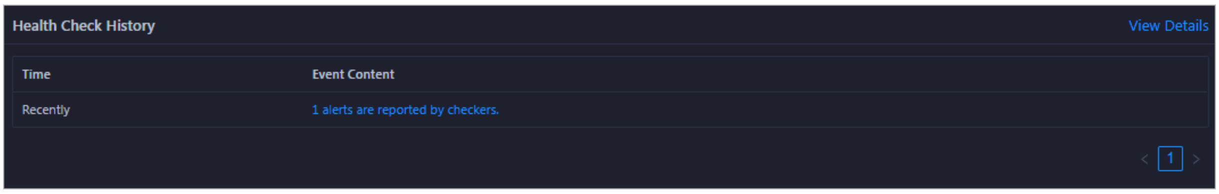
View Details

Currently, 9 checkers are deployed on the service. 2 critical, 0 exception, and 0 warning alerts are reported.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Host health.

Health Check History

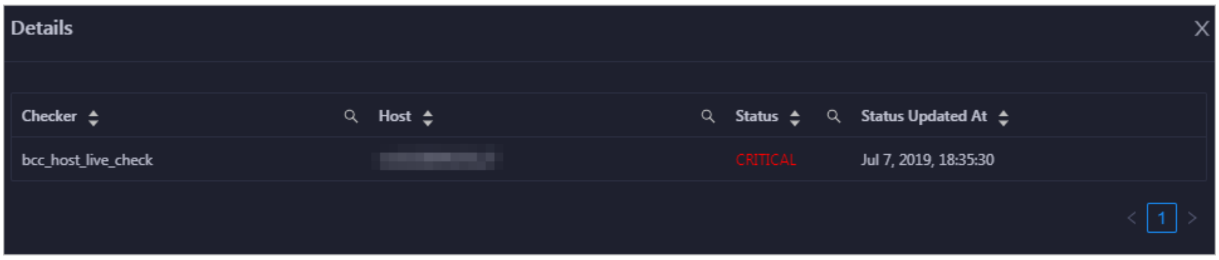
This section displays a record of the health checks performed on the host.


Health Check History

Time	Event Content
Recently	1 alerts are reported by checkers.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Host health.

You can click the event content of a check to view the exception items.


Details

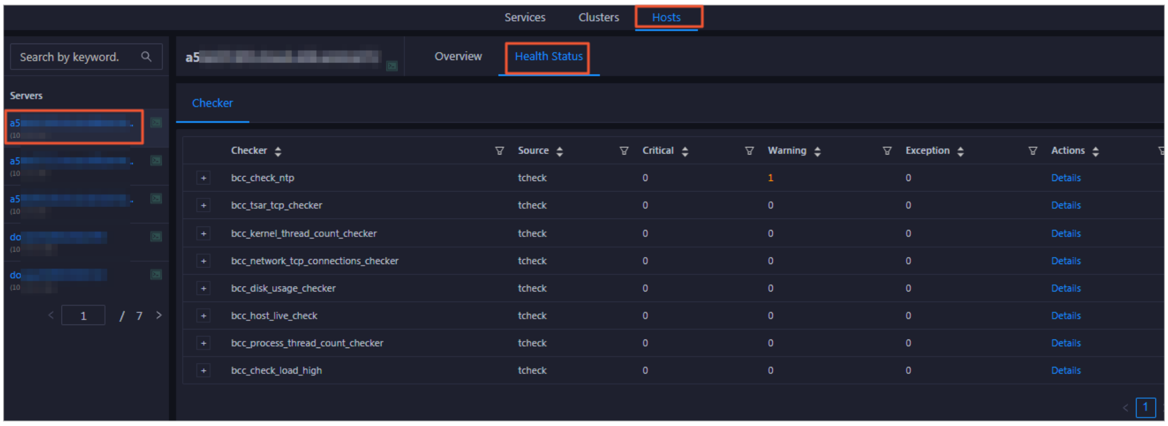
Checker	Host	Status	Status Updated At
bcc_host_live_check	[redacted]	CRITICAL	Jul 7, 2019, 18:35:30

11.11.6.2. Host health

On the Health Status tab, you can view the checkers of the selected host, including the checker details, check results, and schemes to clear alerts. In addition, you can log on to the host and perform manual checks on the host.

Entry

1. At the top of the **O&M** page, click **Hosts**.
2. On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Health Status** tab.

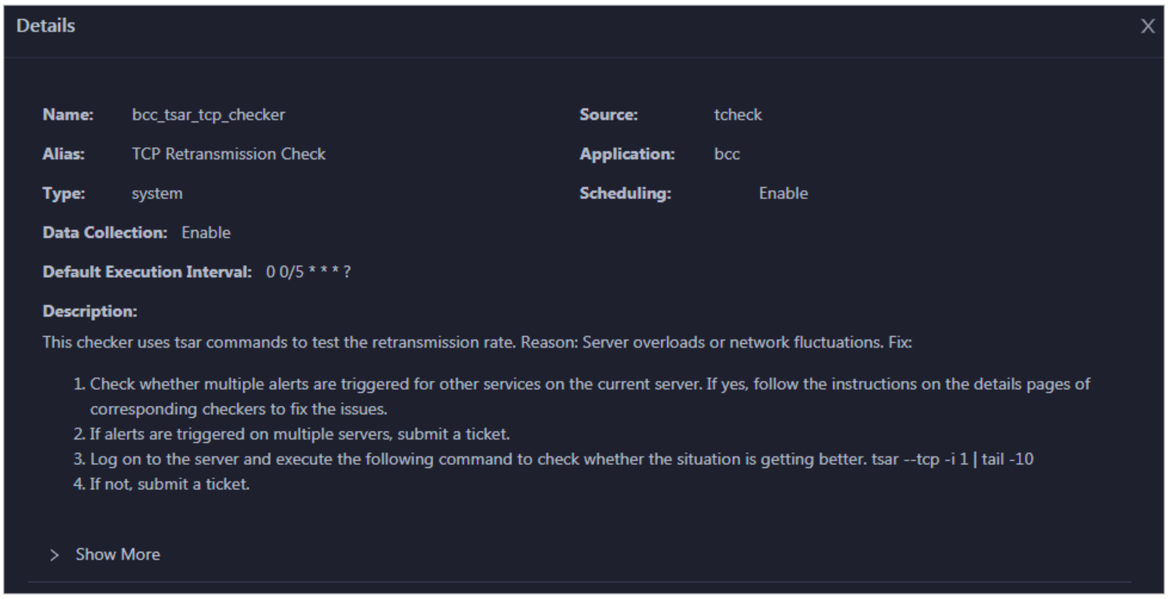


	Checker	Source	Critical	Warning	Exception	Actions
+	bcc_check_ntp	tcheck	0	1	0	Details
+	bcc_tsar_tcp_checker	tcheck	0	0	0	Details
+	bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
+	bcc_network_tcp_connections_checker	tcheck	0	0	0	Details
+	bcc_disk_usage_checker	tcheck	0	0	0	Details
+	bcc_host_live_check	tcheck	0	0	0	Details
+	bcc_process_thread_count_checker	tcheck	0	0	0	Details
+	bcc_check_load_high	tcheck	0	0	0	Details

On the **Health Status** page, you can view all checkers and the check results for the host. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

View checker details

1. On the Health Status page, click **Details** in the Actions column of a checker. In the dialog box that appears, view the checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

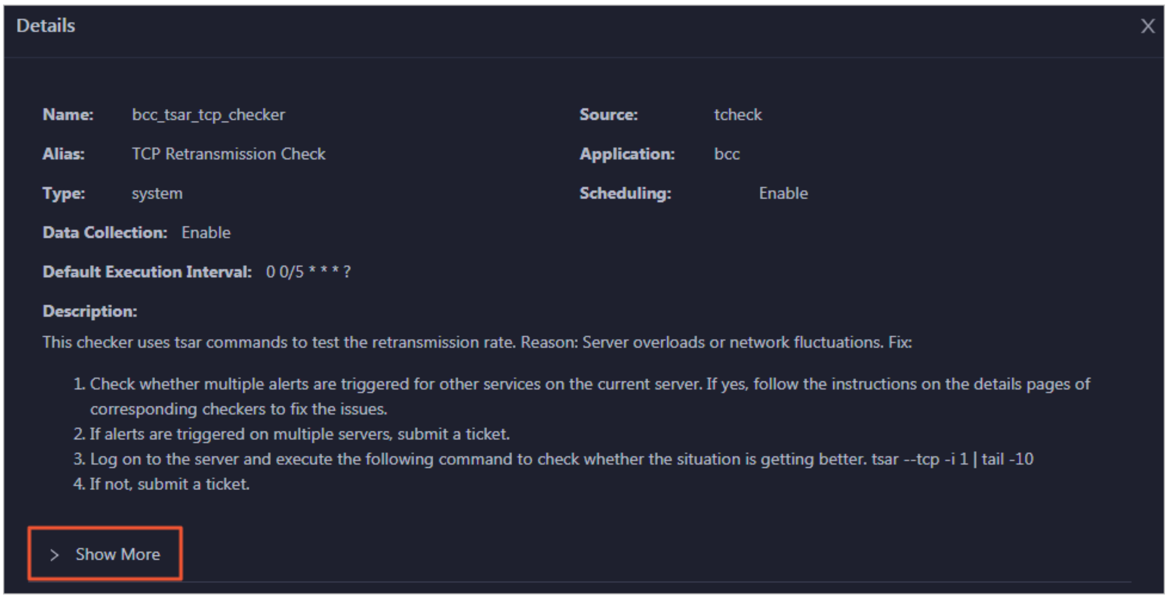
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include the name, source, alias, application, type, default execution interval, and description of the checker, whether scheduling is enabled, and whether data collection is enabled. The schemes to clear alerts are provided in the description.

2. Click **Show More** at the bottom to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

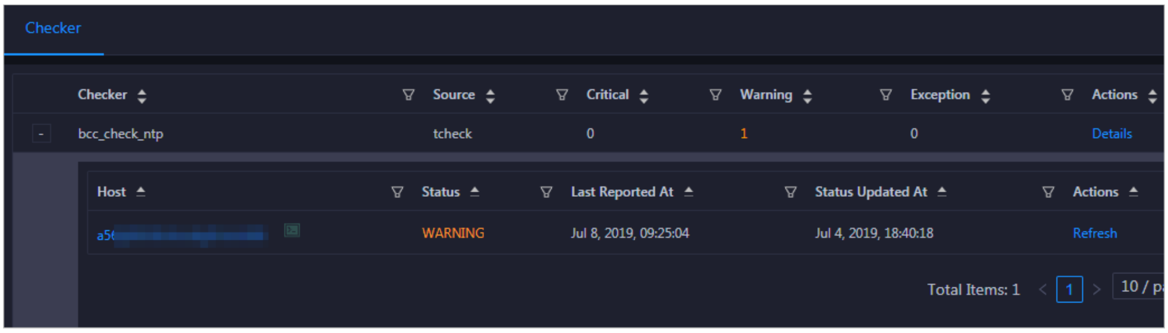
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about the execution script, execution target, default threshold, and mount point for data collection.

View alert causes

You can view the check history and check results of a checker.

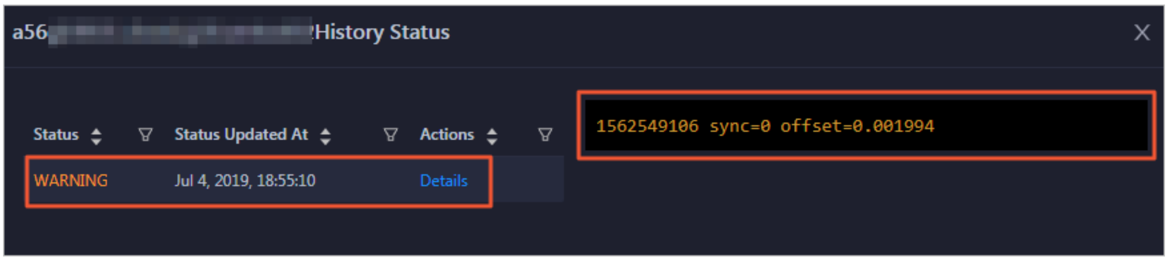
1. On the Health Status page, click **+** to expand a checker with alerts.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

2. Click the hostname. In the dialog box that appears, click **Details** in the Actions column of a check result to view the alert causes.

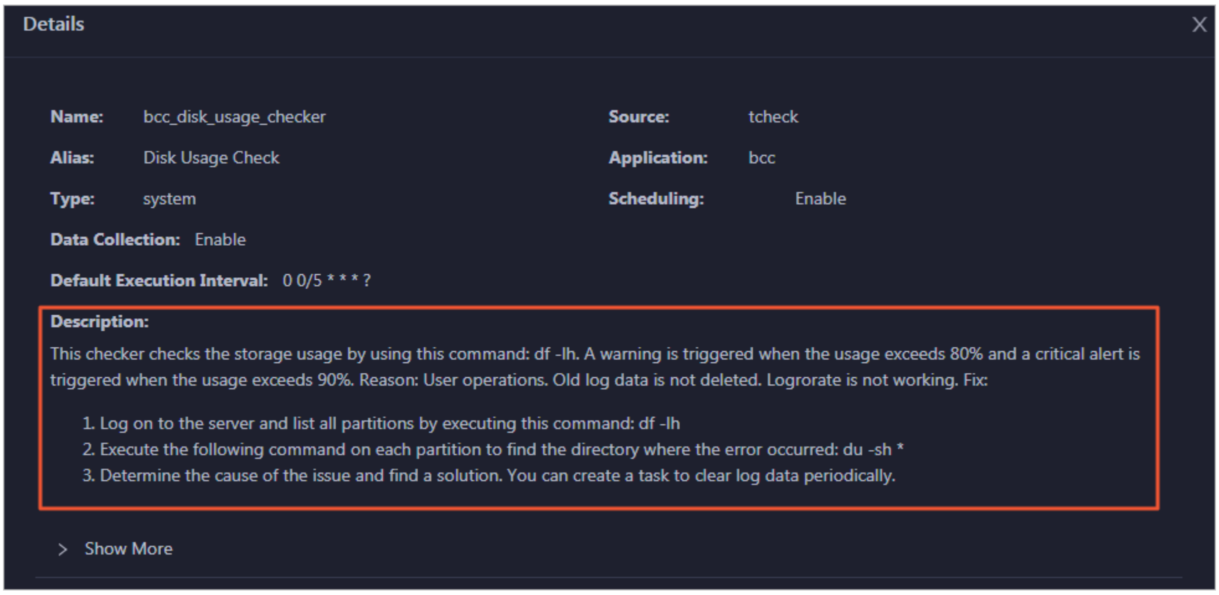


Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status page, click **Details** in the Actions column of a checker with alerts. In the dialog box that appears, view the schemes to clear alerts.



Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

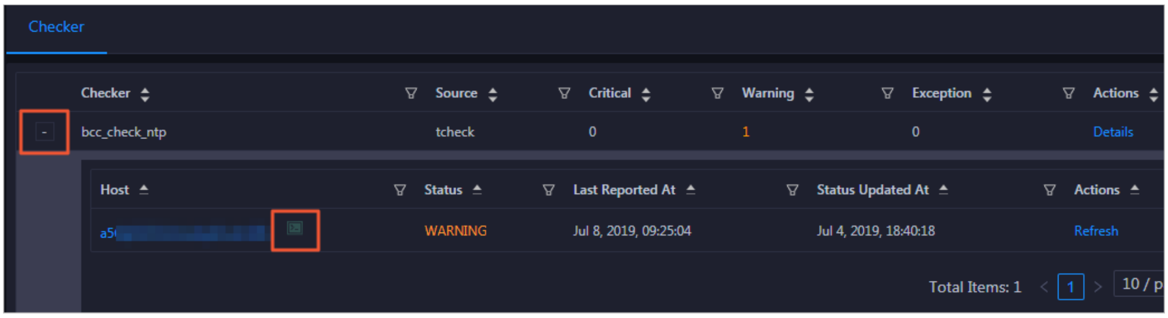
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

To log on to a host to clear alerts or perform other operations, follow these steps:

1. On the Health Status page, click **+** to expand a checker with alerts.

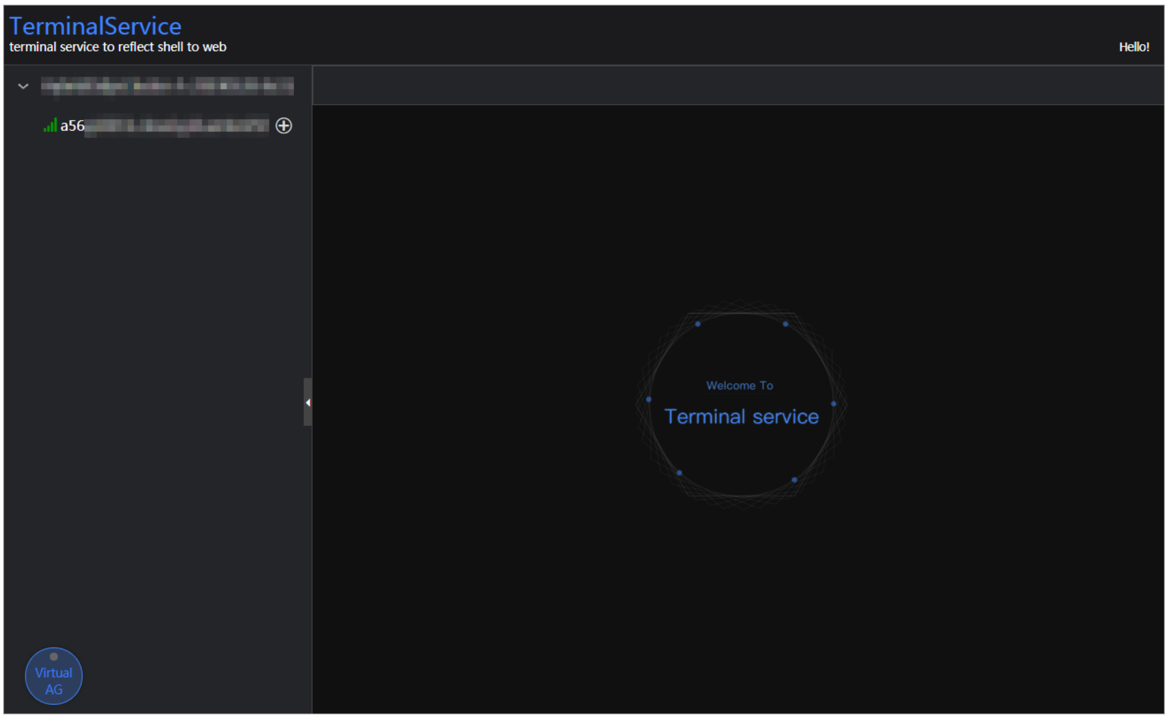


Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	1	0	Details

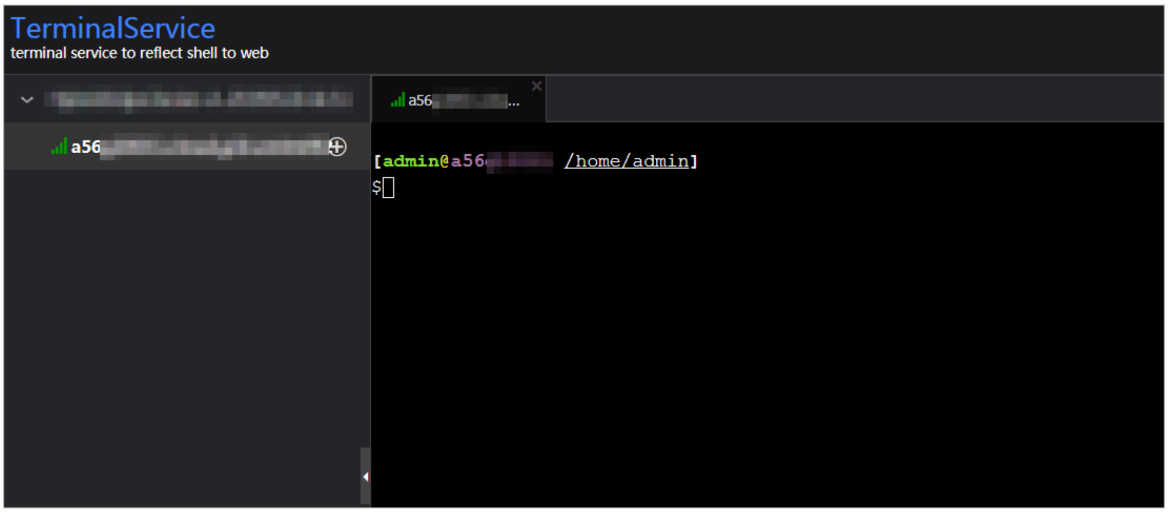
Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

2. Click the **Log On** icon of a host. The **TerminalService** page appears.



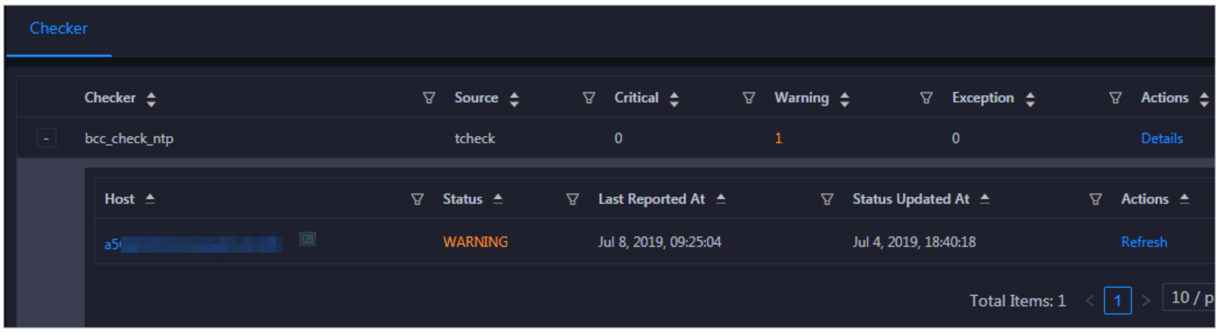
3. On the **TerminalService** page, click the hostname on the left to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. In this way, you can check whether the alert is cleared.



Checker

Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

11.12. Elasticsearch (on ECS)

11.12.1. What is Apsara Big Data Manager?

Apsara Big Data Manager (ABM) is an operations and maintenance (O&M) platform designed for big data products. You can use ABM to perform O&M on Apsara Stack Elasticsearch from the perspectives of business, services, clusters, and hosts. You can also update patches, customize alerting configurations, and view O&M history for Elasticsearch in ABM.

ABM helps on-site Apsara Stack engineers manage Elasticsearch. For example, the engineers can view resource usage, view and handle alerts, and modify configurations.

11.12.2. Log on to the ABM console

This topic describes how to log on to the Apsara Big Data Manager (ABM) console.

Prerequisites

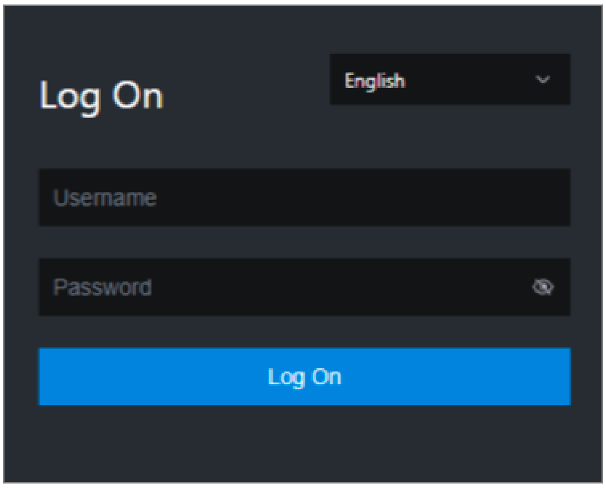
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.


Log On

English

Username

Password

Log On

Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

   When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   For security reasons, your password must meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password must be 10 to 20 characters in length.

4. Click **Log On**.
5. In the top navigation bar of the Apsara Uni-manager Operations Console, click **O&M**.
6. In the left-side navigation pane, choose **Product Management** > **Products**.
7. In the **Big Data Services** section, choose **General-Purpose O&M** > **Apsara Big Data Manager**.

11.12.3. Elasticsearch O&M overview

This topic describes the features of Apsara Stack Elasticsearch O&M. It also provides information about how to navigate to the Elasticsearch O&M page.

Modules

Elasticsearch O&M contains four modules: Business, Services, Clusters, and Hosts. The following table describes these modules.

Module	Feature	Description
Business	Cluster Configuration	Allows you to view and modify the cluster configuration files in the **worker** and **kibana** lists for Elasticsearch.
	System Configuration	Allows you to view and modify the system configuration files for Elasticsearch.
Services	Overview	Displays all Elasticsearch services in a cluster. You can view the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for each service.
	Server	Displays all hosts where each Elasticsearch service is running. This allows you to quickly understand service deployment on hosts.
Clusters	Overview	Displays the overall running and health check information about a cluster. On this tab, you can view the host status, service status, health check result, and health check history of the cluster. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.
	Health Status	Displays all checkers for a cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts if any. In addition, you can log on to a host and perform manual checks on the host.
Hosts	Overview	Displays the overall running and health check information about a host. On this tab, you can view the root disk usage, total usage, 1-minute load, 5-minute load, 15-minute load, health check result, and health check history of the host. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.
	Charts	Displays the enlarged trend charts of CPU utilization, memory usage, disk usage, load, and packet transmission.
	Health Status	Displays the health check results of a host. A host has the following health states: CRITICAL, WARNING, EXCEPTION, and OK.
	Services	Displays information about service instances and service instance roles of a host.

Entry

1. Log on to Apsara Bigdata Manager.
2. Click the ⊞ icon in the upper-left corner and then **Elasticsearch**.
3. In the top navigation bar of the page that appears, click **O&M**. The **Business** page appears.

   O&M contains four modules: **Business**, **Services**, **Clusters**, and **Hosts**.

11.12.4. Business O&M

11.12.4.1. Cluster configuration

This topic describes how to view and modify the cluster configuration files in the worker and kibana lists for Elasticsearch in the Apsara Big Data Manager (ABM) console.

Entry

1. In the upper part of the page, click the **Business** tab.
2. In the left-side navigation pane of the **Business** tab, click **Cluster Configuration**.
3. In the **worker** or **kibana** list, click the cluster configuration file that you want to view. The details of the file appear on the right part of the page.

Modify a cluster configuration file

1. Click the cluster configuration file that you want to modify and click **Edit**. Then, modify the file based on your business requirements.
2. Click **Save**.
3. Click **Preview**.
   i. In the **Preview** dialog box, compare the differences before and after the file modification.
   ii. If the modification is correct, click **OK**.
4. Click **Submit** in the lower part of the page. The modification is complete.

   If you want to cancel the modification, click **Undo**.

Upload a plug-in

> **Notice** Custom plug-ins may affect the stability of your cluster. Make sure that the custom plug-in you want to upload is reliable, secure, and ready to use. Plug-ins are not automatically updated with Elasticsearch. To update a plug-in, you must manually upload a new version of the plug-in.

1. Select the cluster to which you want to upload a plug-in from the drop-down list. Click **Upload Plug-in**.
2. In the **Upload Plug-in** dialog box, click **Click here to select files for upload** to upload one or more files.

   To delete a file that is not required for the upload, click the x icon next to the file.

3. Select the check box in the dialog box and click **OK**.

11.12.4.2. System configuration

This topic describes how to view and modify the system configuration files for Elasticsearch in Apsara Big Data Manager (ABM).

Entry

1. In the upper part of the page, click the **Business** tab.
2. On the **Business** page, click **System Configuration** in the left-side navigation pane.
3. Click the configuration file that you want to view. The details of the file appear on the right.

Modify a system configuration file

1. Click the system configuration file that you want to modify and click **Edit**. Then, modify the file based on your business requirements.
2. Click **Save**.
3. Click **Preview**.
    i. In the **Preview** dialog box, compare the differences before and after the file modification.
    ii. If the modification is correct, click **OK**.
4. Click **Submit** in the lower part of the page. The modification is complete.

    If you want to cancel the modification, click **Undo**.

11.12.5. Service O&M

11.12.5.1. Service overview

The service overview page lists all Elasticsearch services in a cluster. You can view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for each service.

Entry

1. At the top of the **O&M** page, click the **Services** tab.
2. On the **Services** page that appears, select a service in the left-side navigation pane. Click the **Overview** tab.

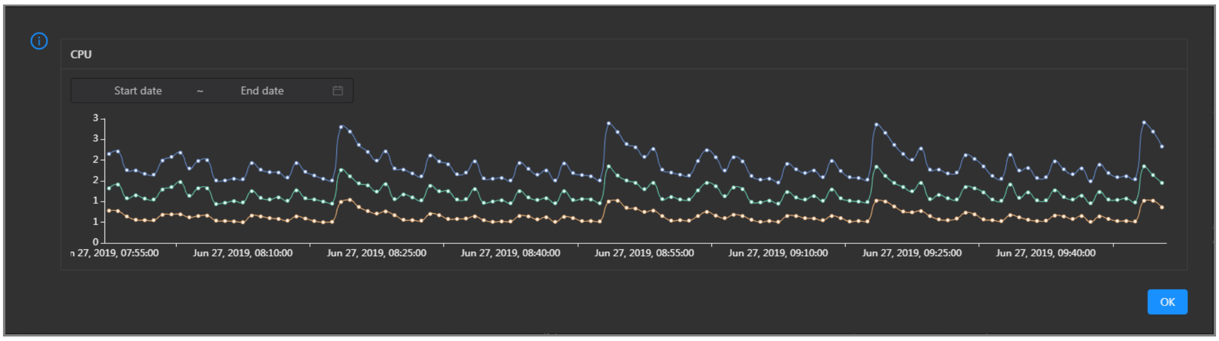
    On the Overview page that appears, you can view the trend charts of CPU usage, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage for the selected service.

CPU

This chart displays the trend lines of the total CPU usage (cpu), CPU usage for executing code in kernel space (sys), and CPU usage for executing code in user space (user) for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

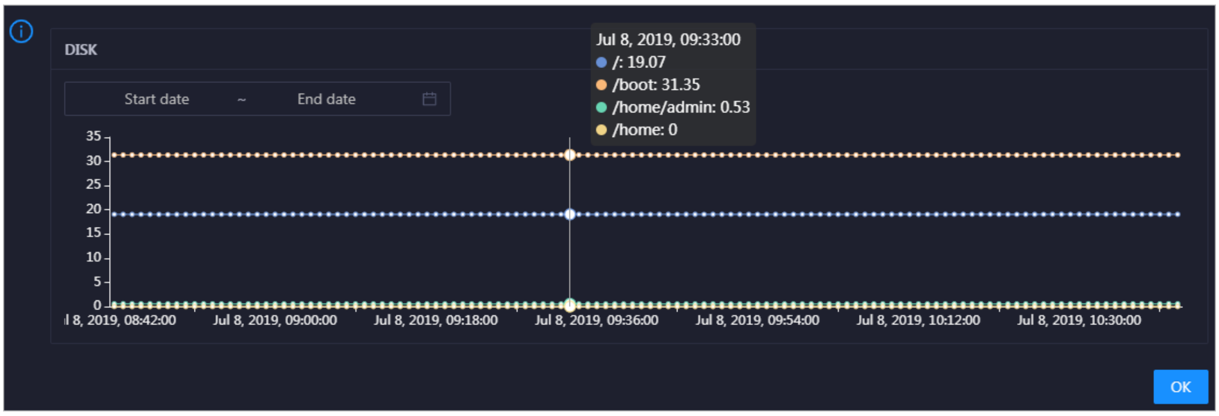
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU usage of the service in the specified period.



DISK

This chart displays the trend lines of the storage space usage on the */*, */boot*, */home/admin*, and */home* directories for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

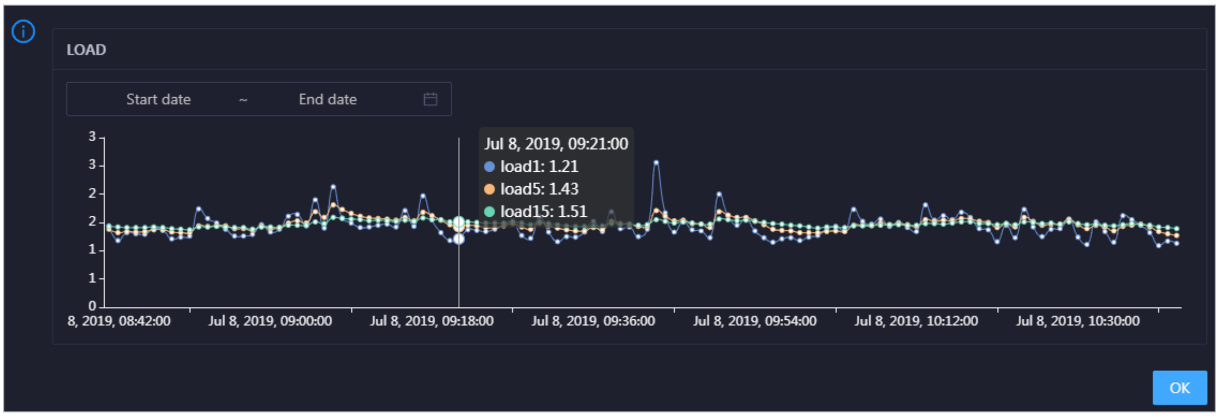


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage space usage of the service in the specified period.

LOAD

This chart displays the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

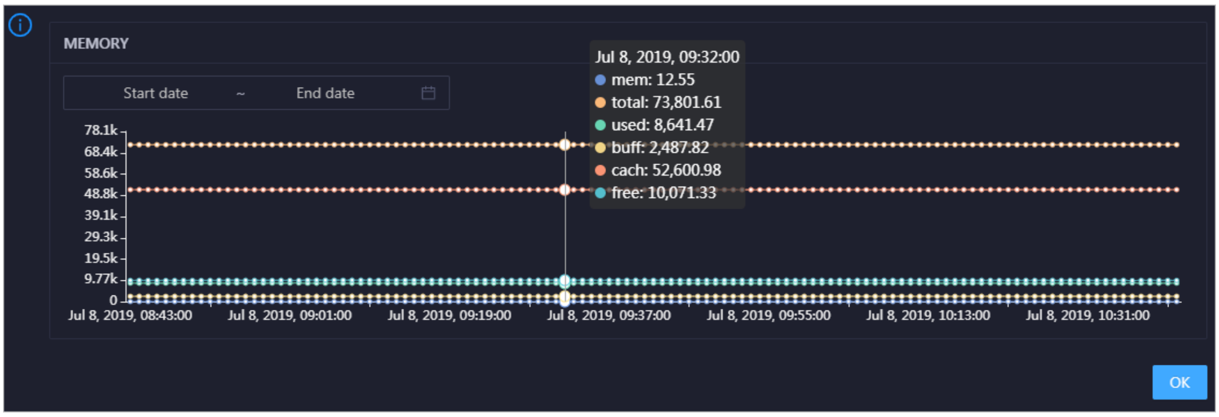


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the selected service in the specified period.

MEMORY

This chart displays the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the selected service over time in different colors.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

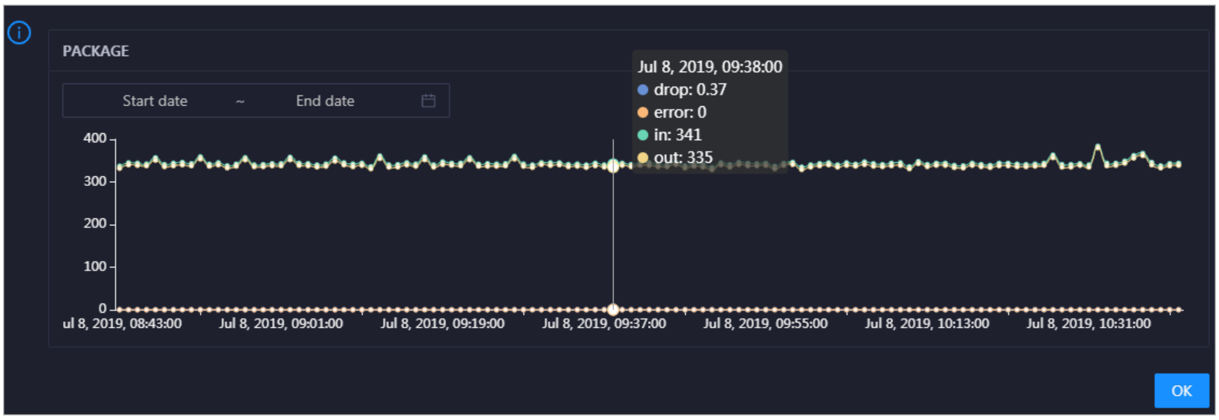


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the selected service in the specified period.

PACKAGE

This chart displays the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the selected service over time in different colors. These trend lines reflect the data transmission status of the service.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

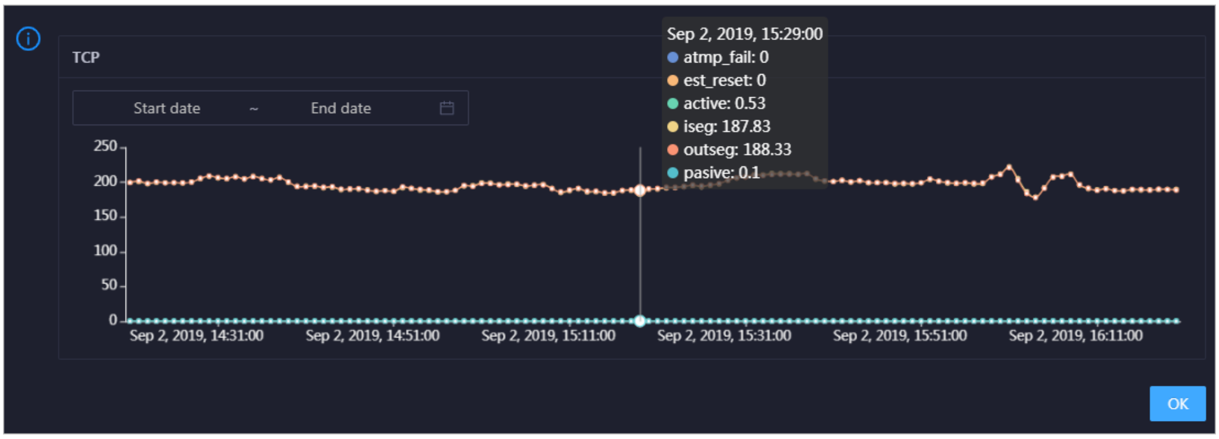


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the selected service in the specified period.

TCP

This chart displays the trend lines of the number of failed TCP connection attempts (atmp_fail), that of the times of resetting TCP connections in the ESTABLISHED state (est_reset), that of active TCP connections (active), that of passive TCP connections (pasive), that of received TCP packets (iseg), and that of sent TCP packets (outseg) for the selected service over time in different colors. These trend lines reflect the TCP connection status of the service.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.

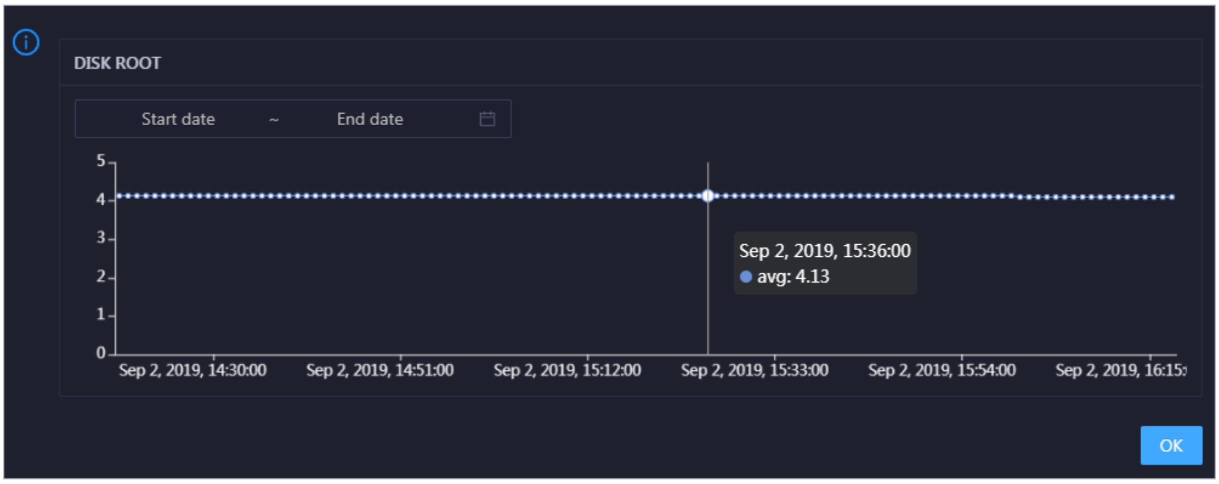


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the TCP connection status of the selected service in the specified period.

DISK ROOT

This chart displays the trend line of the average root disk usage (avg) for the selected service over time.

Click ⤢ in the upper-right corner of the chart to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the average root disk usage of the selected service in the specified period.

11.12.5.2. Service hosts

This topic describes how to view all hosts where each Elasticsearch service is run.

On the Server page, you can view the hosts where the selected service is run.

1. At the top of the **O&M** page, click the **Services** tab.
2. On the **Services** page that appears, select a service in the left-side navigation pane.
3. Click the **Server** tab. The **Server** page for the service appears.

   On the **Server** page, you can view the hosts where the selected service is run.

11.12.6. Cluster O&M

11.12.6.1. Cluster overview

The Overview tab of a cluster displays the overall running and health check information about the cluster. On this tab, you can view the host status, service status, health check result, and health check history of the cluster. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, packet transmission, TCP connection, and root disk usage.

Entry

1. In the upper part of the page, click the **Clusters** tab.
2. On the **Clusters** tab, select a cluster in the left-side navigation pane and click the **Overview** tab.

Hosts

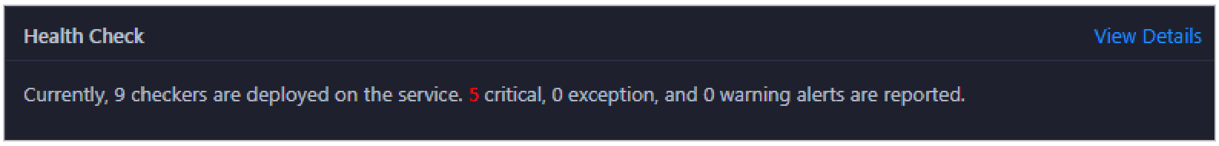
This section displays host states and the number of hosts in each state. The host states include **good** and **bad**.

Service Status

This section displays all the services that are deployed in the cluster. It also provides information about the numbers of available and unavailable services.

Health Check

This section displays the number of checkers for the cluster and the numbers of CRITICAL, WARNING, and EXCEPTION alerts.


Health Check

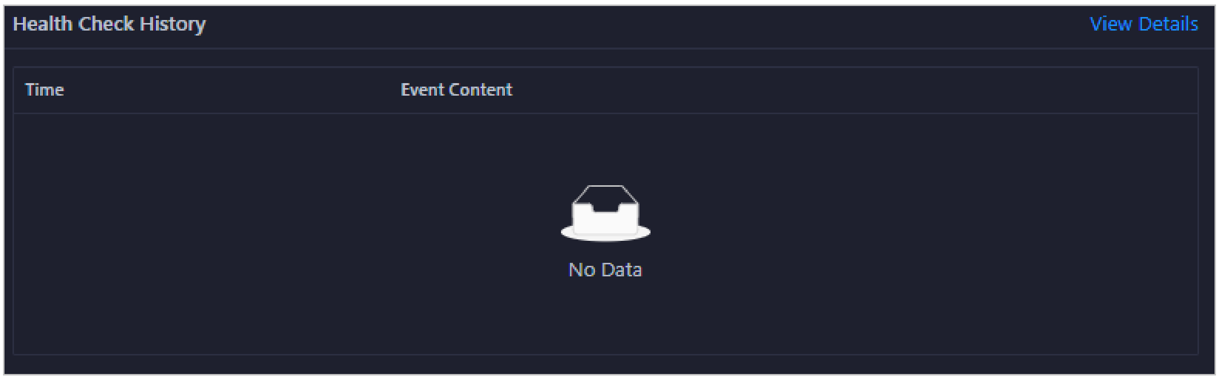
Currently, 9 checkers are deployed on the service. 5 critical, 0 exception, and 0 warning alerts are reported.

You can click **View Details** to go to the Health Status tab. On this tab, you can view the health check details.

Health Check History

This section displays the historical health checks that are performed on the cluster.

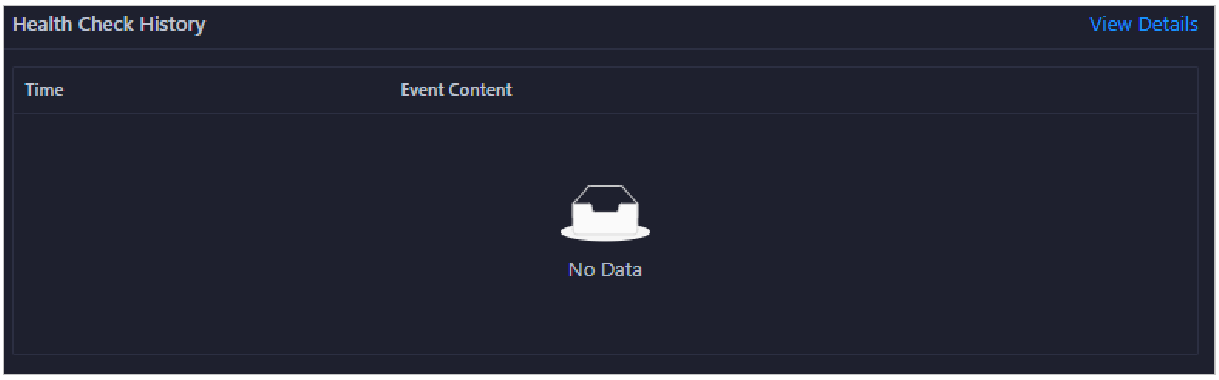
You can click **View Details** to go to the Health Status tab. On this tab, you can view the health check details.


Health Check History

Time	Event Content

No Data

You can click the event content of a check to view exception items.

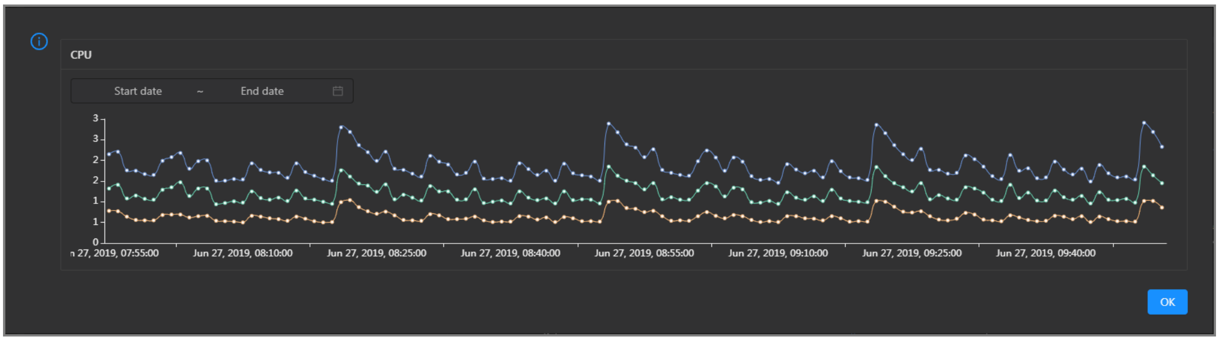


CPU

This chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

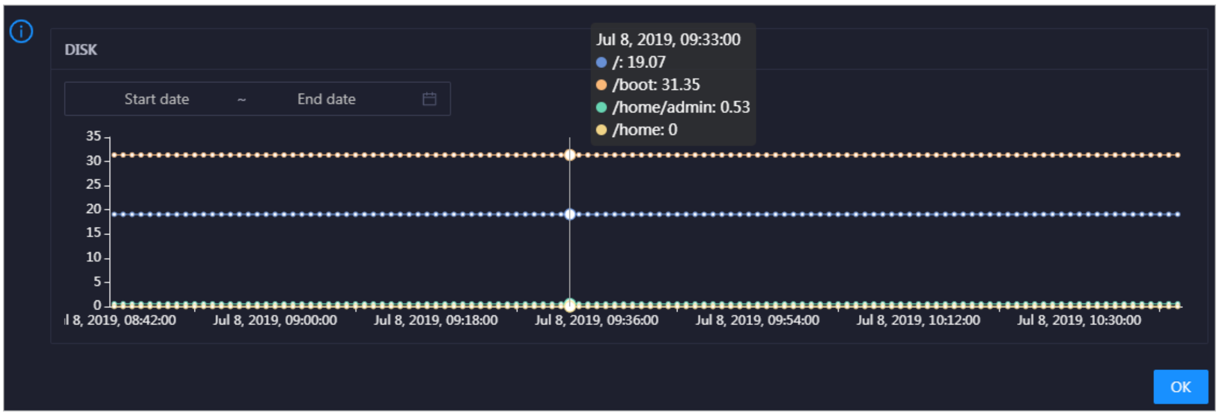
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the cluster in the specified period.



DISK

This chart shows the trend lines of the storage usage on the */*, */boot*, */home/admin*, and */home* directories for the cluster over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

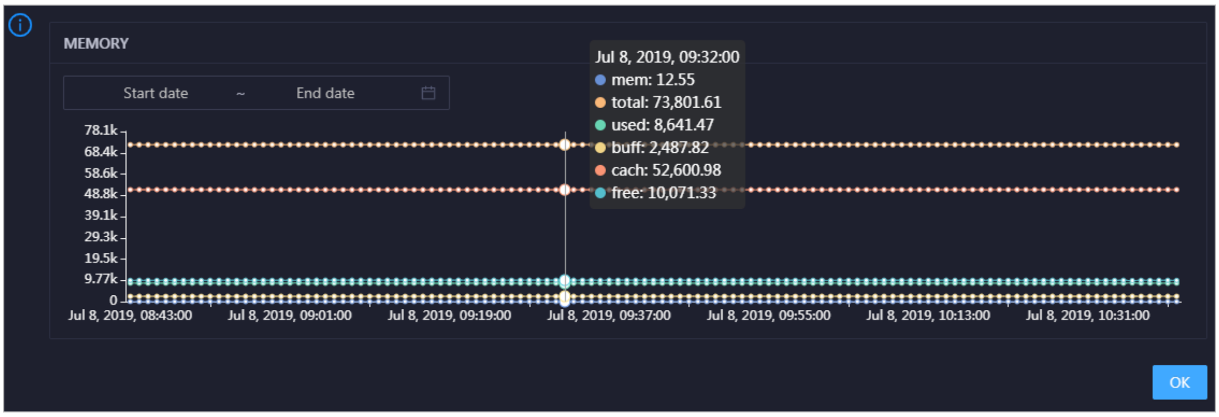


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the cluster in the specified period.

MEMORY

This chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

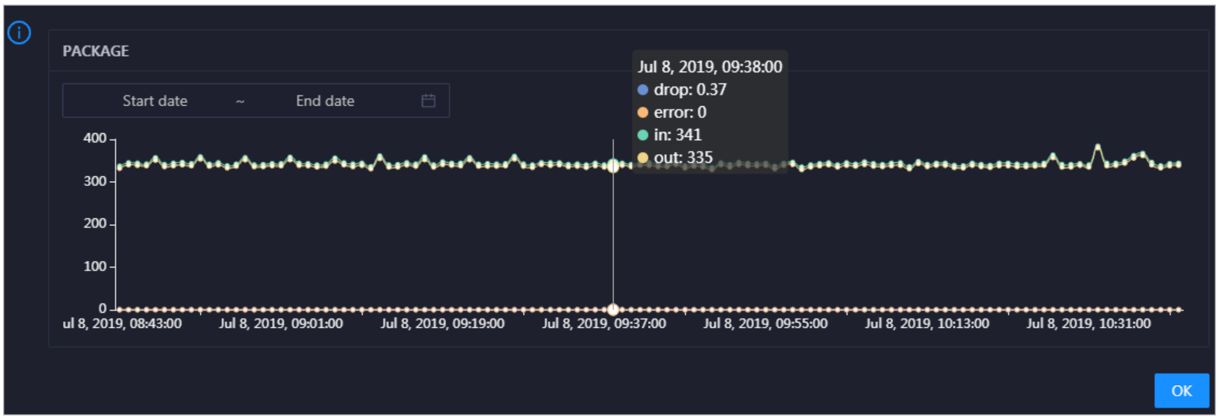


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the cluster in the specified period.

PACKAGE

This chart shows the trend lines of the numbers of dropped packets (drop), error packets (error), received packets (in), and sent packets (out) for the cluster in different colors. These trend lines reflect the data transmission status of the cluster.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

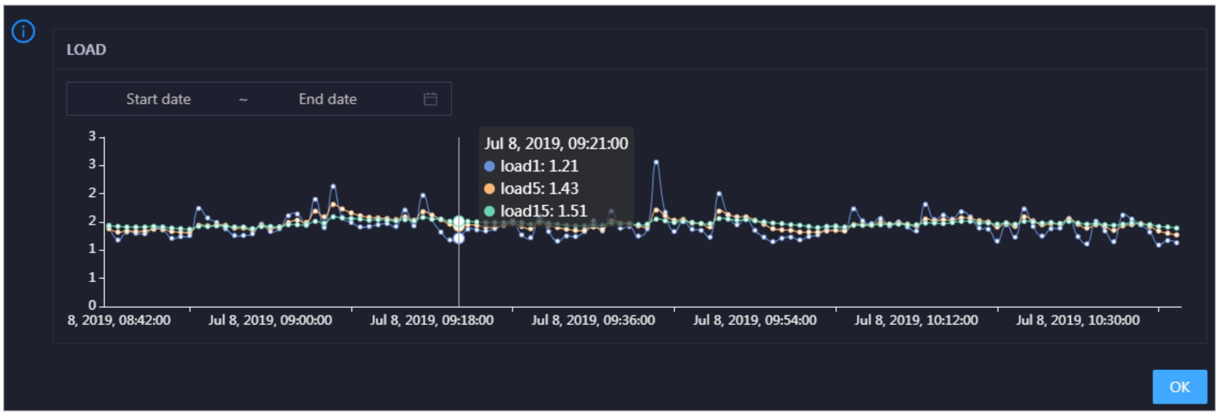


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the cluster in the specified period.

LOAD

This chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the cluster in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



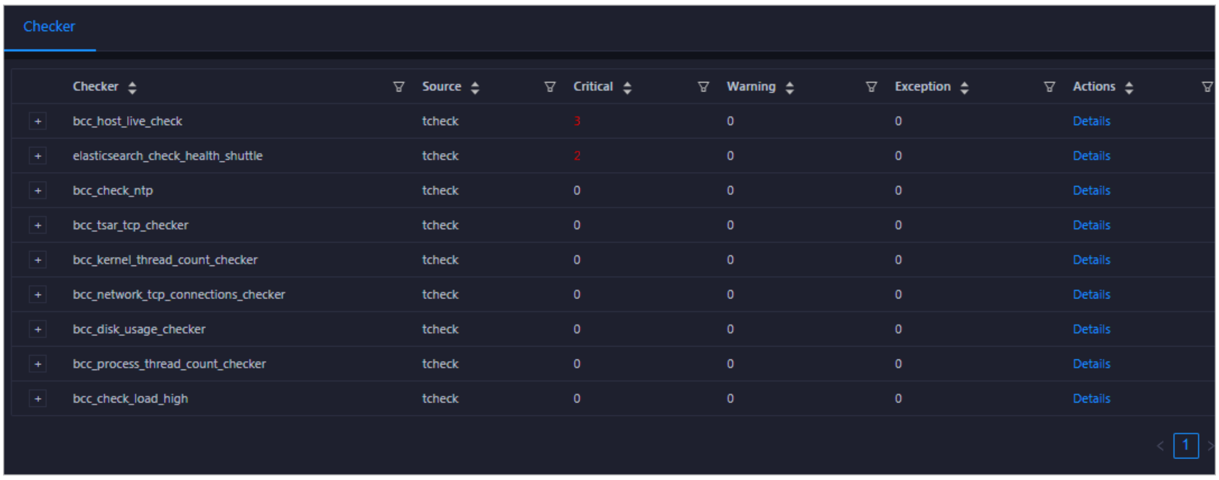
You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the cluster in the specified period.

11.12.6.2. Cluster health

On the Health Status tab of a cluster, you can view all checkers for the cluster, including the checker details, check results for the hosts in the cluster, and schemes to clear alerts if any. In addition, you can log on to a host and perform manual checks on the host.

Entry

In the upper part of the page, click the **Clusters** tab. Then, select a cluster in the left-side navigation pane and click the **Health Status** tab.

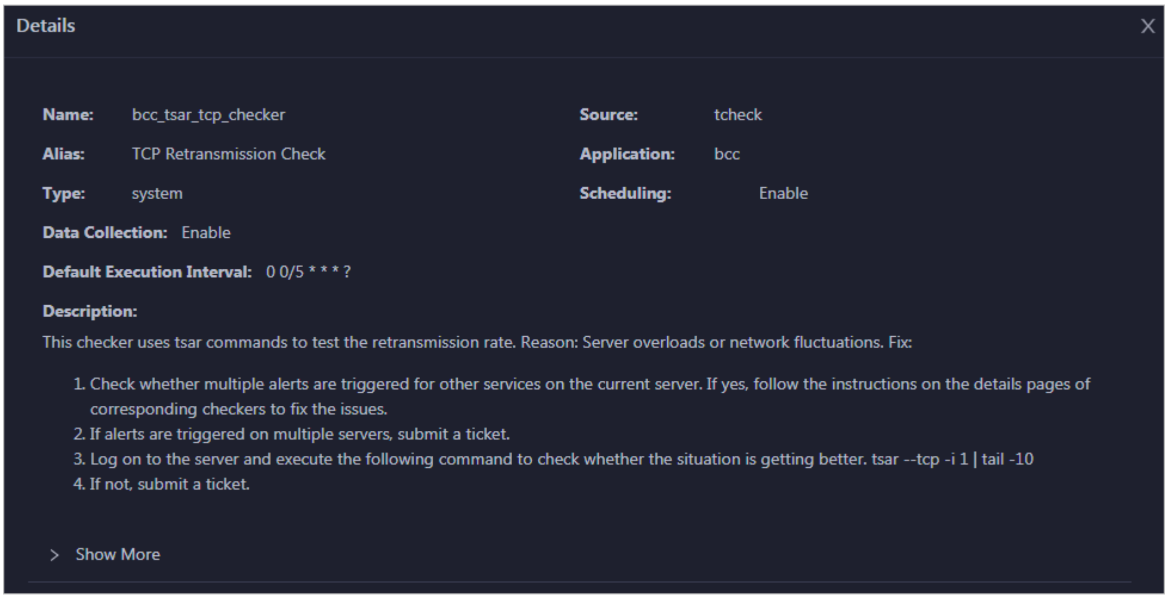


	Checker	Source	Critical	Warning	Exception	Actions
+	bcc_host_live_check	tcheck	3	0	0	Details
+	elasticsearch_check_health_shuttle	tcheck	2	0	0	Details
+	bcc_check_ntp	tcheck	0	0	0	Details
+	bcc_tsar_tcp_checker	tcheck	0	0	0	Details
+	bcc_kernel_thread_count_checker	tcheck	0	0	0	Details
+	bcc_network_tcp_connections_checker	tcheck	0	0	0	Details
+	bcc_disk_usage_checker	tcheck	0	0	0	Details
+	bcc_process_thread_count_checker	tcheck	0	0	0	Details
+	bcc_check_load_high	tcheck	0	0	0	Details

On the **Health Status** tab, you can view all checkers for the cluster and the check results for the hosts in the cluster. The following alerts may be reported on a host: **CRITICAL**, **WARNING**, and **EXCEPTION**. The alerts are represented in different colors. You must handle the alerts in a timely manner, especially the **CRITICAL** and **WARNING** alerts.

View checker details

1. On the Health Status tab, click **Details** in the Actions column of a checker. On the Details page, view checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

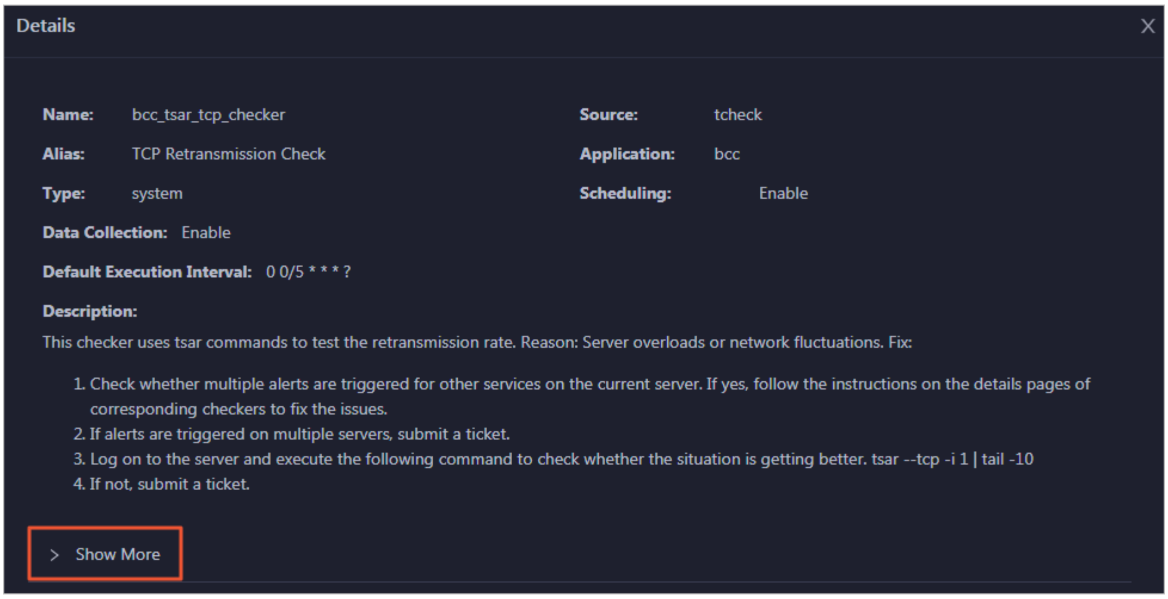
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include **Name**, **Source**, **Alias**, **Application**, **Type**, **Scheduling**, **Data Collection**, **Default Execution Interval**, and **Description**. The schemes to clear alerts are provided in the description.

2. Click **Show More** to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

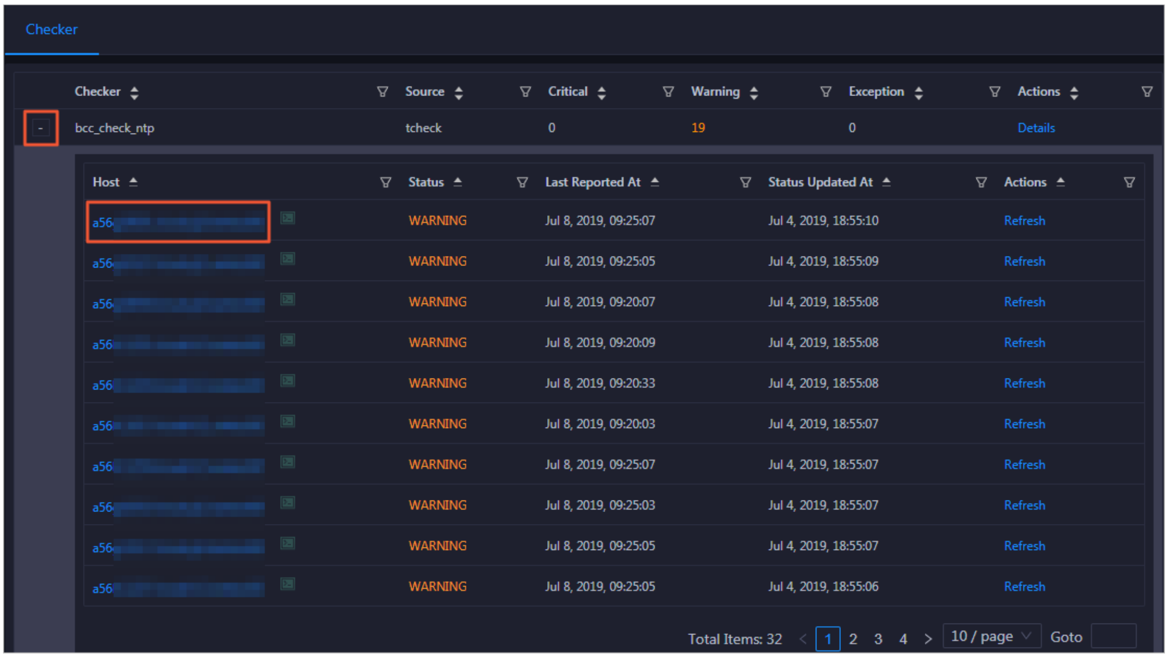
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about **Script**, **Target (TianJi)**, **Default Threshold**, and **Mount Point**.

View the hosts for which alerts are reported and causes for the alerts

You can view the check history and check results of a checker on a host.

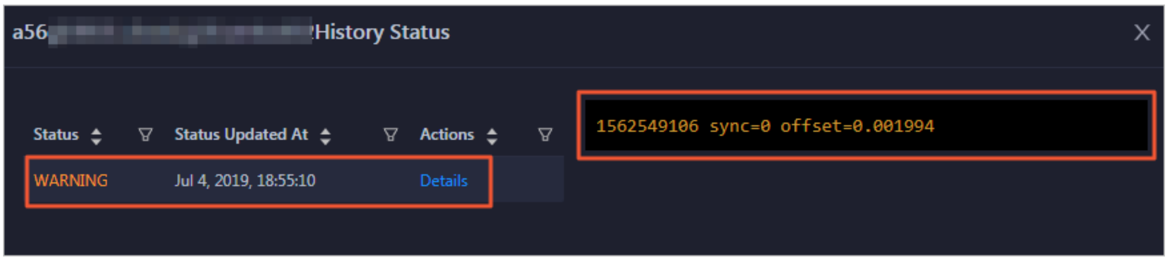
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported. You can view all hosts where the checker is run.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:06	Refresh

2. Click a hostname. In the panel that appears, click **Details** in the Actions column of a check result to view the cause of the alert.

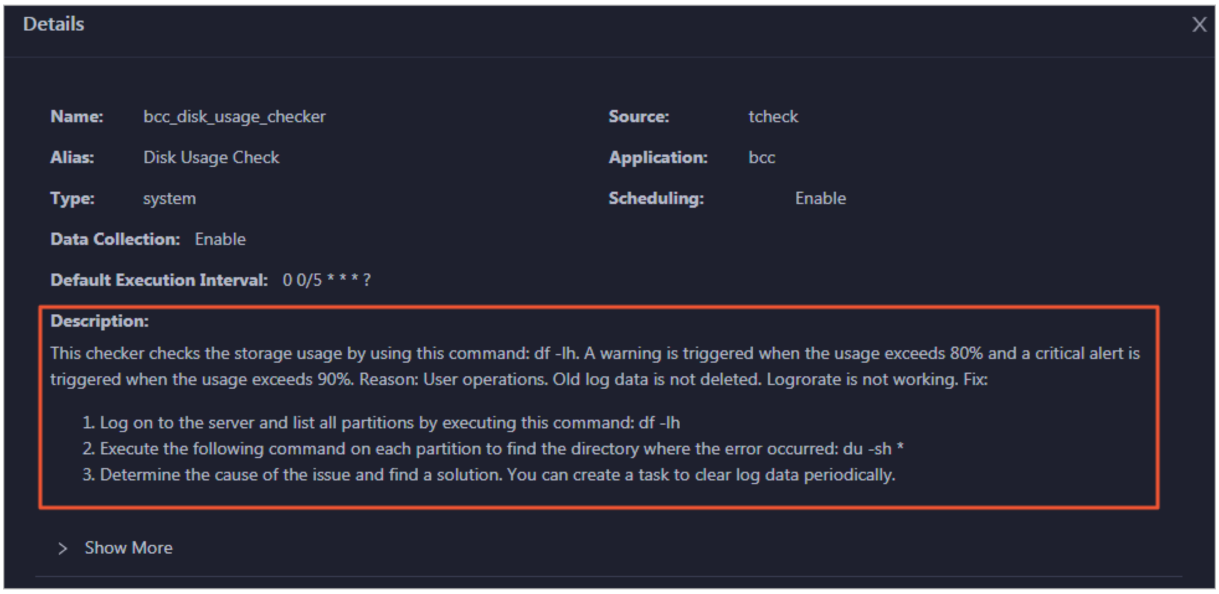


Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status tab, click **Details** in the Actions column of a checker for which alerts are reported. On the Details page, view the schemes to clear alerts.



Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

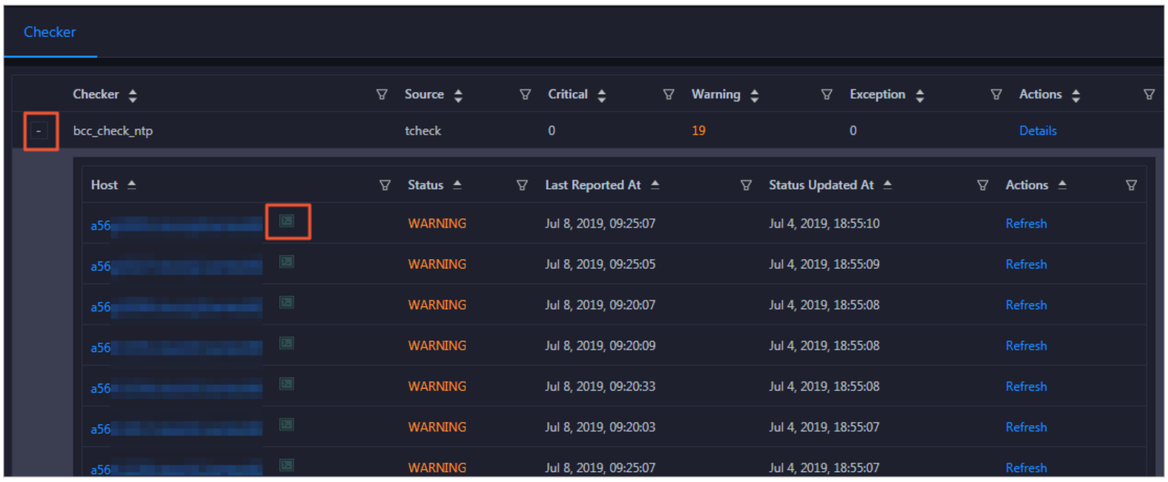
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

You may need to log on to a host to handle alerts or other issues that occurred on the host.

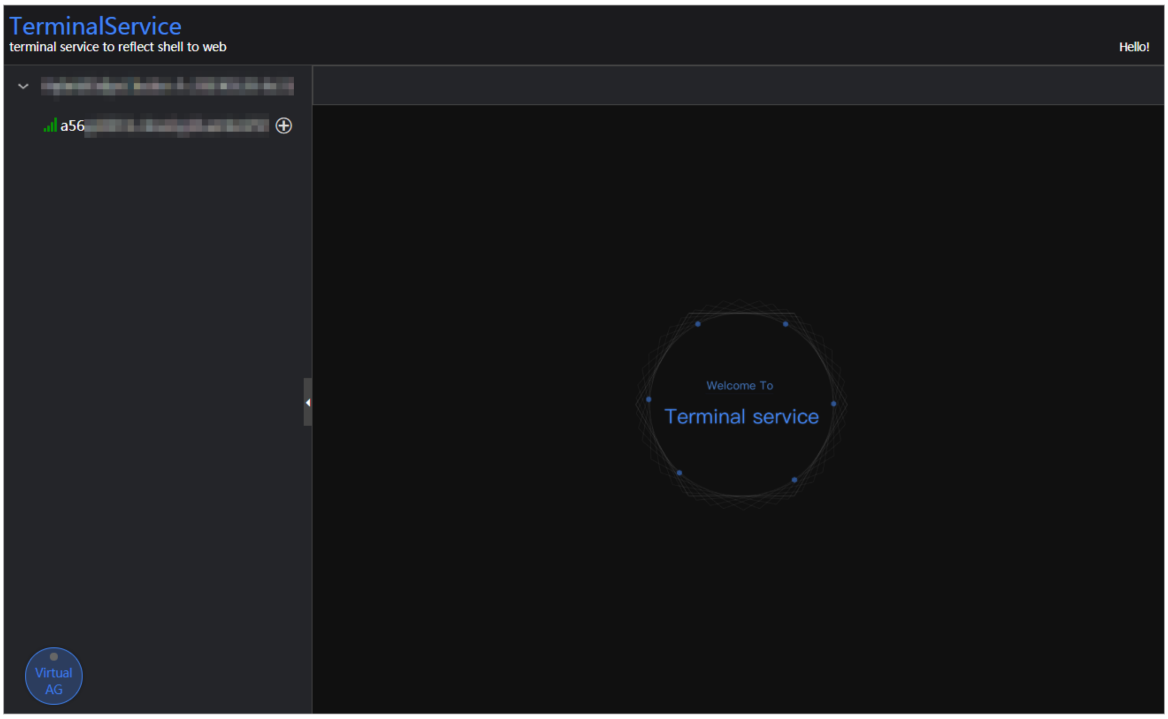
1. On the Health Status tab, click **+** to expand a checker for which alerts are reported.



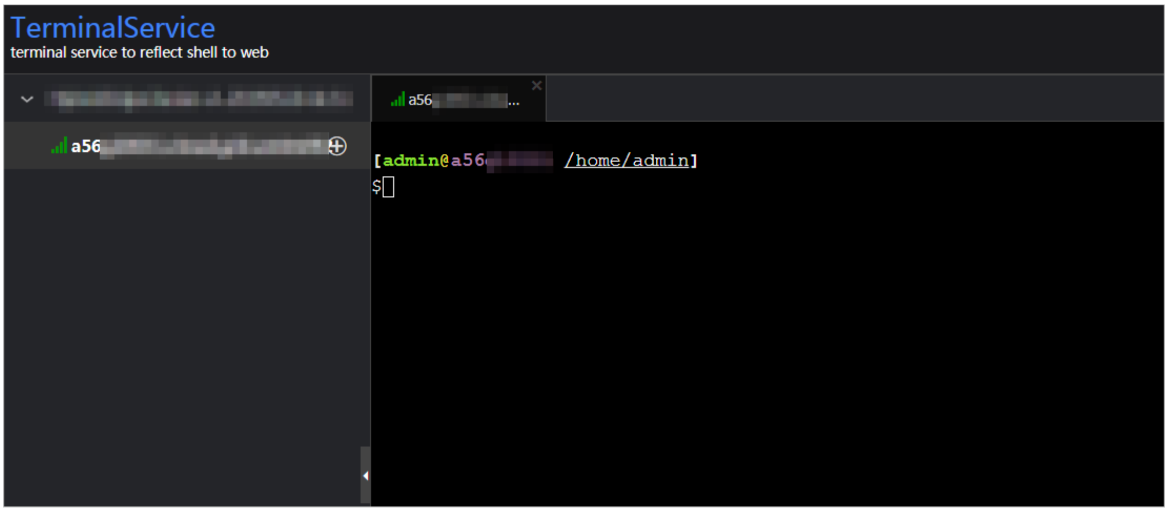
	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

2. Click the **Login in** icon of a host. The **TerminalService** page appears.



3. On the **TerminalService** page, click the hostname in the left-side navigation pane to log on to the host.

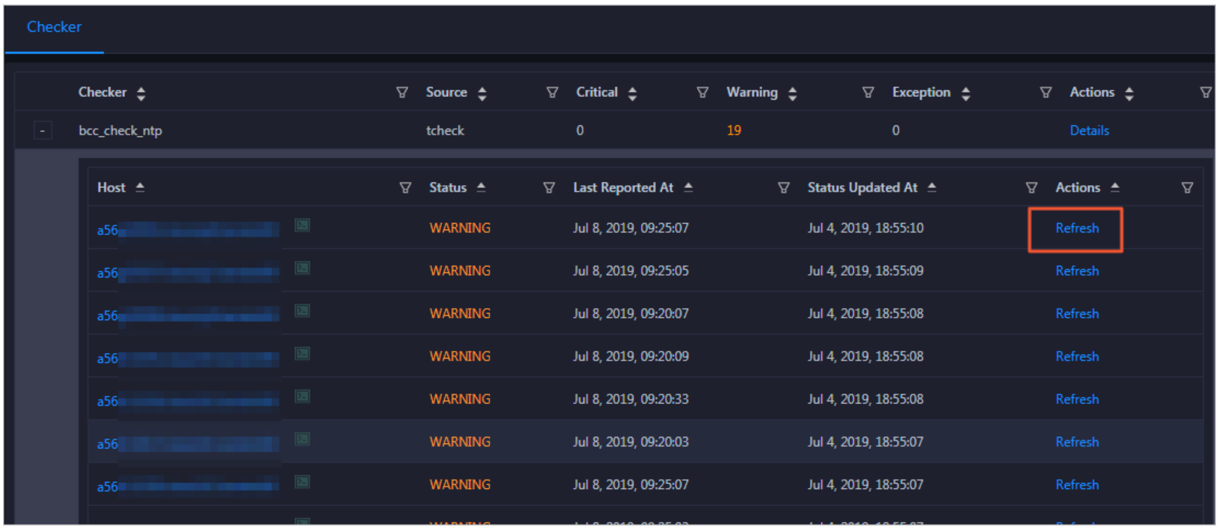


TerminalService
terminal service to reflect shell to web

```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. This way, you can check whether the alert is cleared.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	19	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:10	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:05	Jul 4, 2019, 18:55:09	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:07	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:09	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:33	Jul 4, 2019, 18:55:08	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:20:03	Jul 4, 2019, 18:55:07	Refresh
a56[redacted]	WARNING	Jul 8, 2019, 09:25:07	Jul 4, 2019, 18:55:07	Refresh

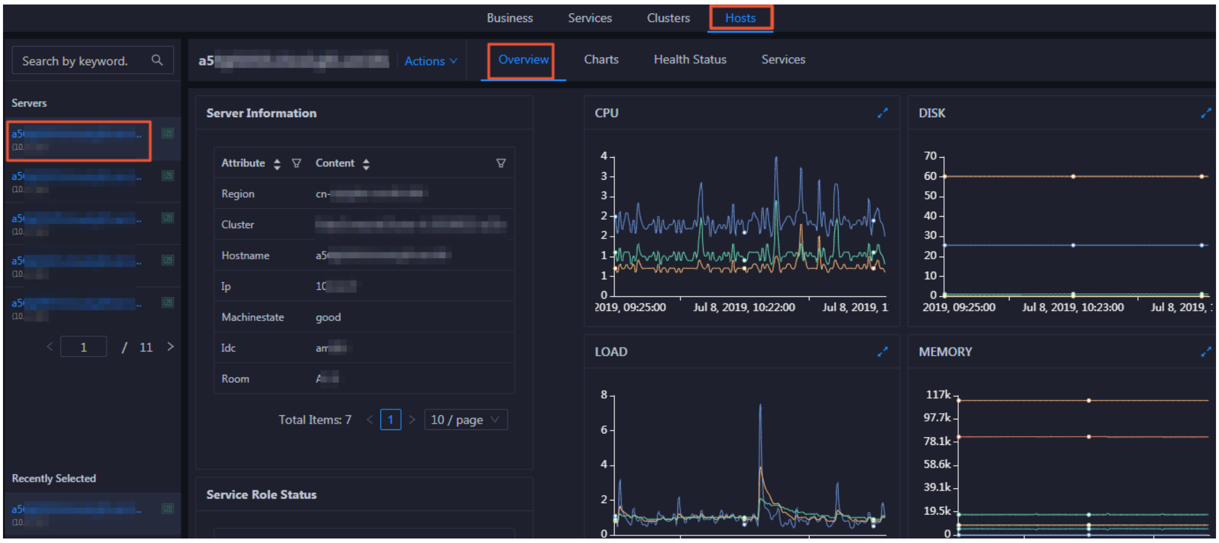
11.12.7. Host O&M

11.12.7.1. Host overview

The host overview page displays the overall running information about a host in an Elasticsearch cluster. On this page, you can view the information, service role status, health check result, and health check history of the host. You can also view the trend charts of CPU usage, disk usage, memory usage, load, and packet transmission.

Go to the Overview tab

In the left-side navigation pane of the **Hosts** tab, click a host. Then, click the **Overview** tab. The **Overview** tab for the host appears.



Server Information

Attribute	Content
Region	cn-[redacted]
Cluster	[redacted]
Hostname	a5[redacted]
Ip	10[redacted]
Machinestate	good
Idc	am[redacted]
Room	A[redacted]

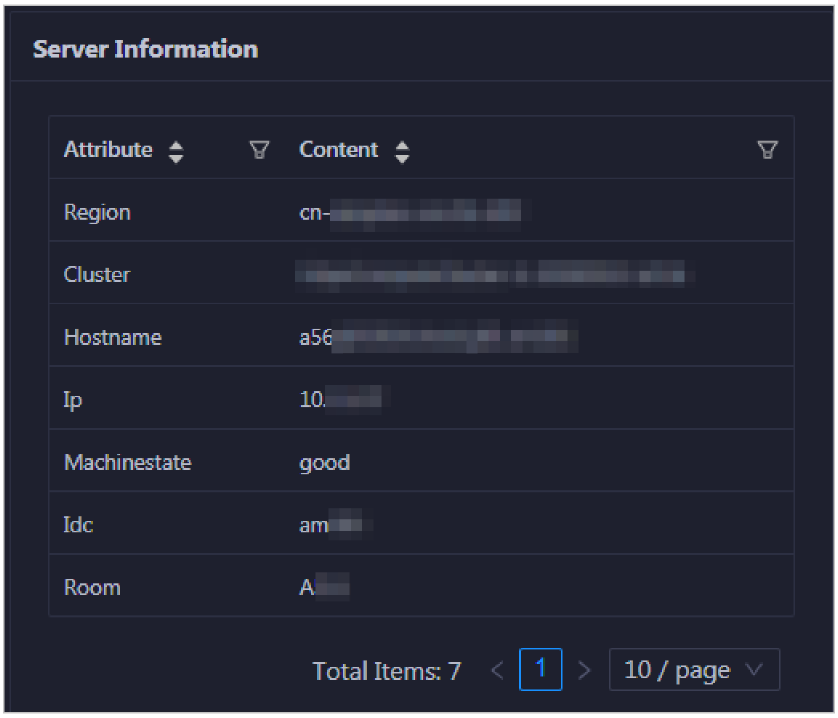
Total Items: 7 1 10 / page

Service Role Status

On the **Overview** tab, you can view server information, service role status, health check result, and health check history of the host. You can also view the trend charts of CPU utilization, disk usage, memory usage, load, and packet transmission for the host.

Server Information

The Server Information section shows information about the host. Server information includes the region, cluster, name, IP address, data center, and server room.



Server Information

Attribute	Content
Region	cn-[redacted]
Cluster	[redacted]
Hostname	a56[redacted]
Ip	10.[redacted]
Machinestate	good
Idc	am[redacted]
Room	A[redacted]

Total Items: 7 1 10 / page

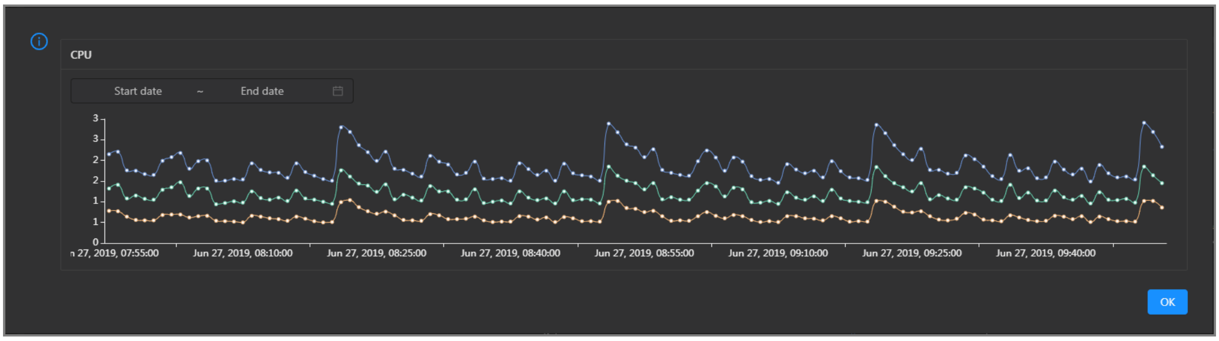
Service Role Status

This section displays the information about the services deployed on the host, including the roles, statuses, and number of services.

CPU

The CPU chart shows the trend lines of the total CPU utilization (cpu), CPU utilization for executing code in kernel space (sys), and CPU utilization for executing code in user space (user) of the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

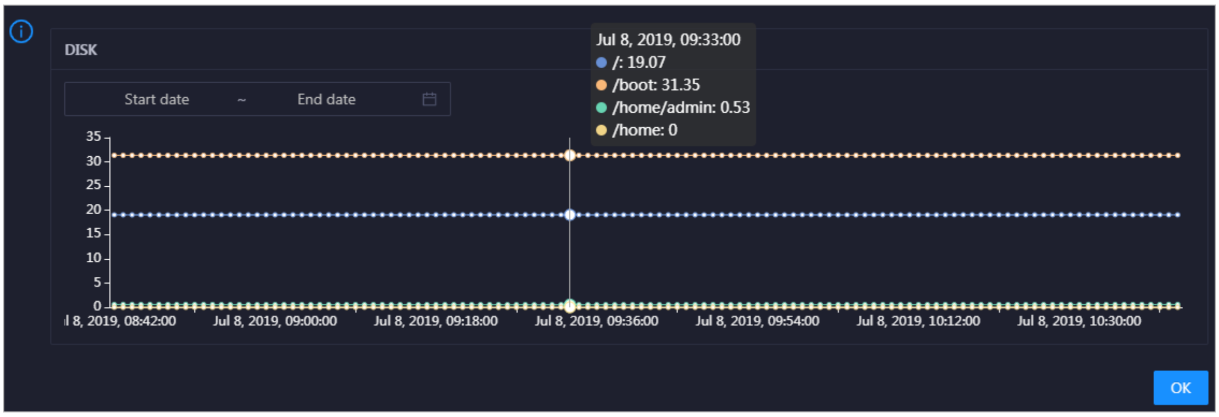


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the CPU utilization of the host in the specified period.

DISK

The DISK chart shows the trend lines of the storage usage in the*/*, */boot*, */home/admin*, and */home* directories for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

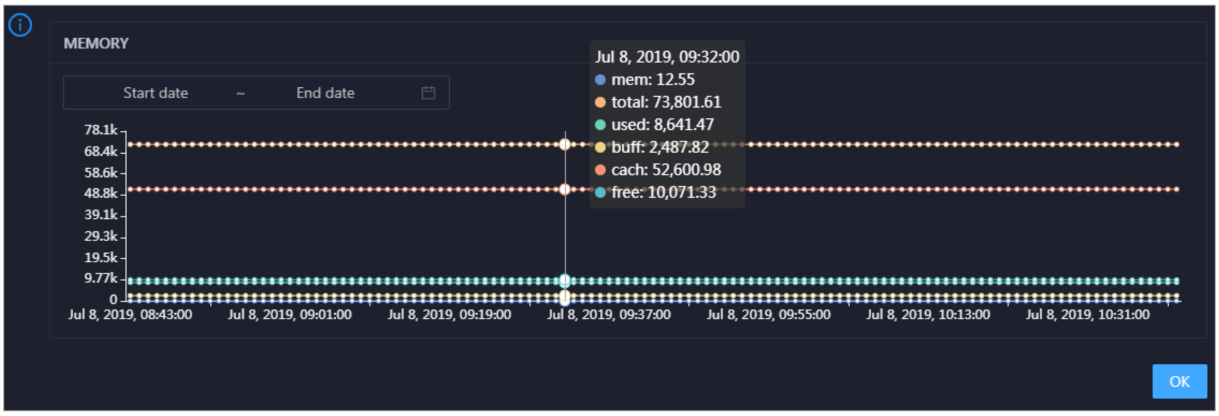


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the storage usage of the host in the specified period.

MEMORY

The MEMORY chart shows the trend lines of the memory usage (mem), total memory size (total), used memory size (used), size of memory used by kernel buffers (buff), size of memory used by the page cache (cach), and available memory size (free) for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

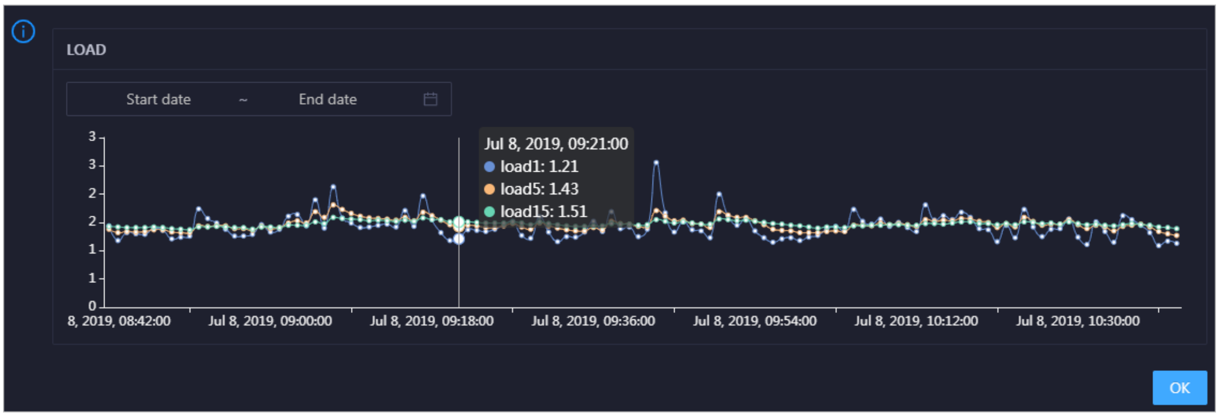


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the memory usage of the host in the specified period.

LOAD

The LOAD chart shows the trend lines of the 1-minute, 5-minute, and 15-minute load averages for the host over time in different colors.

In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.

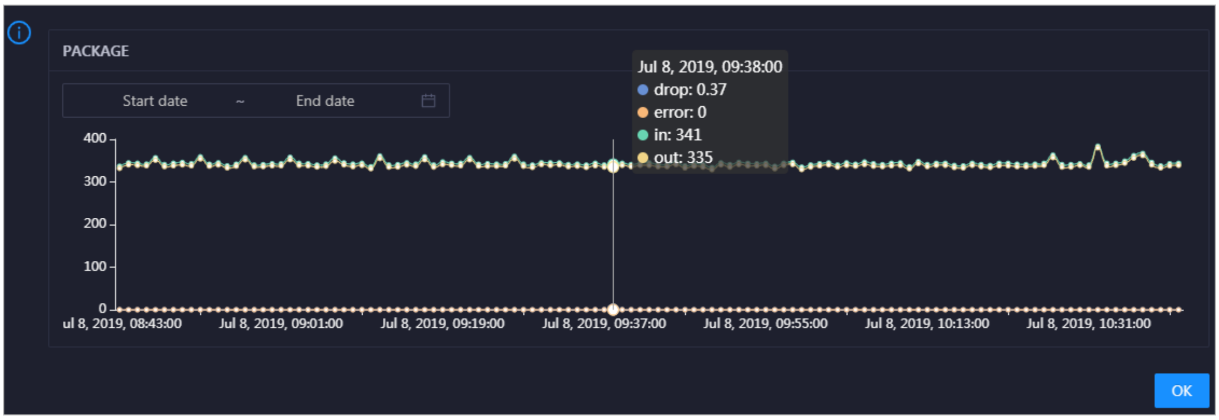


You can specify the start time and end time in the upper-left corner of the enlarged chart to view the 1-minute, 5-minute, and 15-minute load averages of the host in the specified period.

PACKAGE

The PACKAGE chart shows the trend lines of the number of dropped packets (drop), that of error packets (error), that of received packets (in), and that of sent packets (out) for the host over time in different colors. These trend lines reflect the data transmission status of the host.

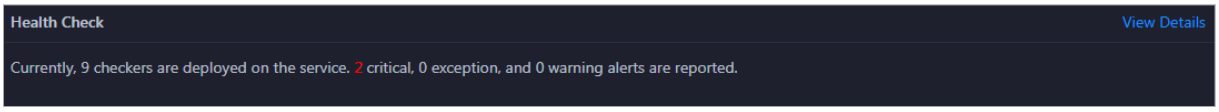
In the upper-right corner of the chart, click the ⤢ icon to zoom in the chart.



You can specify the start time and end time in the upper-left corner of the enlarged chart to view the data transmission status of the host in the specified period.

Health Check

This section displays the number of checkers deployed for the host and the respective number of Critical, Warning, and Exception alerts.

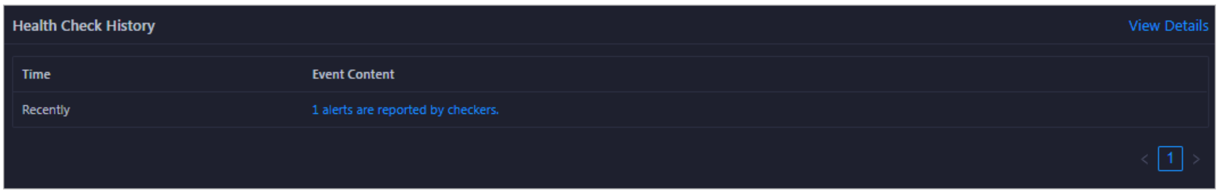


Currently, 9 checkers are deployed on the service. 2 critical, 0 exception, and 0 warning alerts are reported.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Host health.

Health Check History

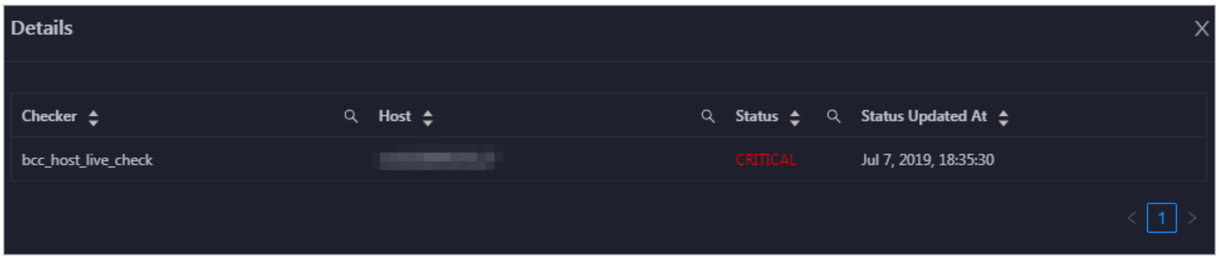
This section displays a record of the health checks performed on the host.



Time	Event Content
Recently	1 alerts are reported by checkers.

Click **View Details** to go to the Health Status page. On this page, you can view the health check details. For more information, see Host health.

You can click the event content of a check to view the exception items.

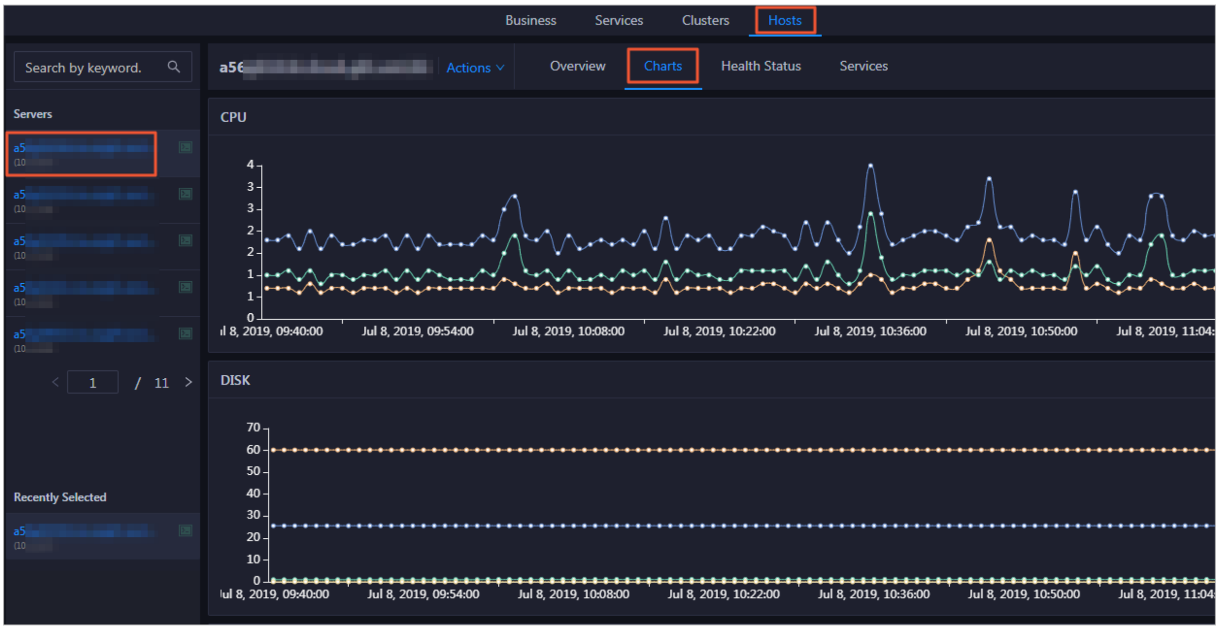


Checker	Host	Status	Status Updated At
bcc_host_live_check	[redacted]	CRITICAL	Jul 7, 2019, 18:35:30

11.12.7.2. Host charts

On the host chart page, you can view the enlarged trend charts of CPU usage, memory usage, storage usage, load, and packet transmission.

On the **Hosts** tab, select a host in the left-side navigation pane and click the **Charts** tab. The **Charts** tab for the host appears.



The **Charts** tab displays the trend charts of CPU utilization, disk usage, memory usage, load, and packet transmission for the host. For more information, see Host overview.

11.12.7.3. Host health

On the Health Status tab of a host, you can view the checkers for the selected host, including the checker details, check results, check history, and schemes to clear alerts if any. In addition, you can log on to a host and perform manual checks on the host.

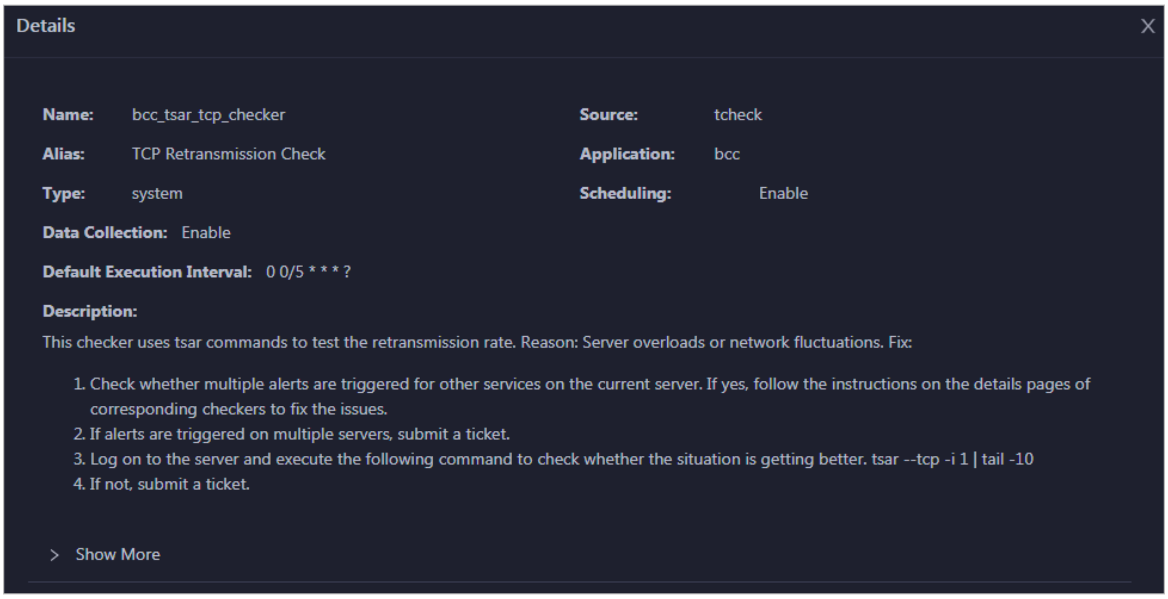
Entry

In the upper part of the page, click the **Hosts** tab. Then, select a cluster in the left-side navigation pane and click the **Health Status** tab.

On the **Health Status** page, you can view all checkers and the check results for the host. The check results are divided into **Critical**, **Warning**, and **Exception**. They are displayed in different colors. Pay attention to the check results, especially the **Critical** and **Warning** results, and handle them in a timely manner.

View checker details

1. On the Health Status page, click **Details** in the Actions column of a checker. In the dialog box that appears, view the checker details.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

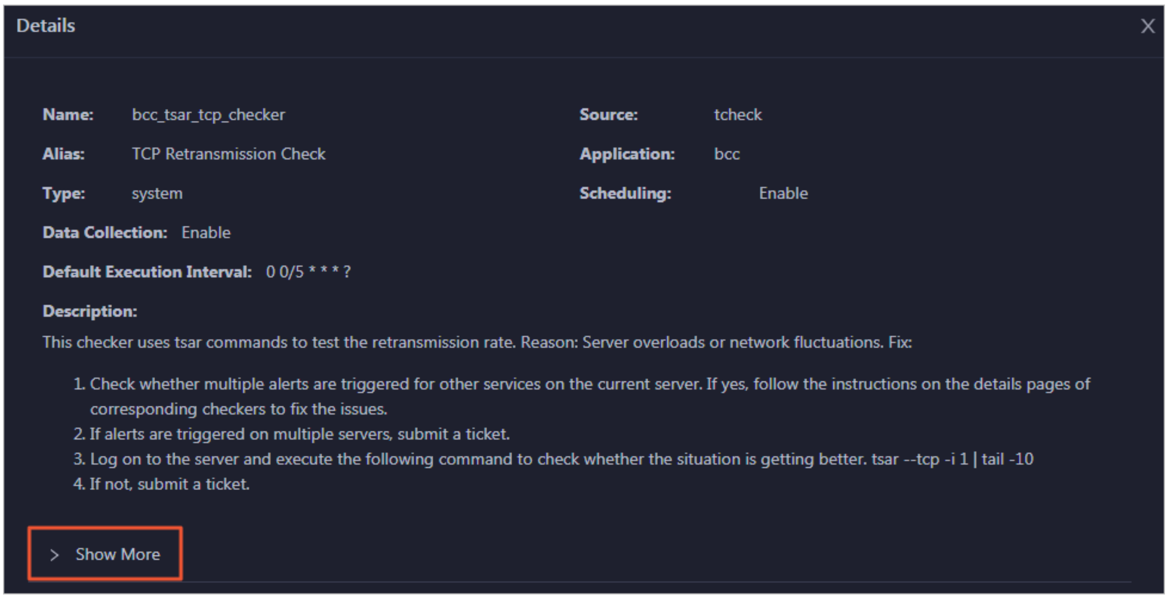
Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

The checker details include the name, source, alias, application, type, default execution interval, and description of the checker, whether scheduling is enabled, and whether data collection is enabled. The schemes to clear alerts are provided in the description.

2. Click **Show More** at the bottom to view more information about the checker.



Details

Name: bcc_tsar_tcp_checker

Source: tcheck

Alias: TCP Retransmission Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

This checker uses tsar commands to test the retransmission rate. Reason: Server overloads or network fluctuations. Fix:

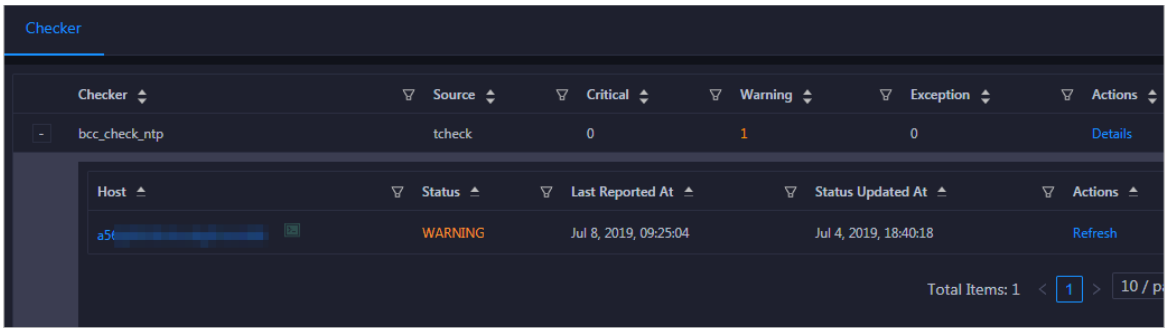
1. Check whether multiple alerts are triggered for other services on the current server. If yes, follow the instructions on the details pages of corresponding checkers to fix the issues.
2. If alerts are triggered on multiple servers, submit a ticket.
3. Log on to the server and execute the following command to check whether the situation is getting better. tsar --tcp -i 1 | tail -10
4. If not, submit a ticket.

You can view information about the execution script, execution target, default threshold, and mount point for data collection.

View alert causes

You can view the check history and check results of a checker.

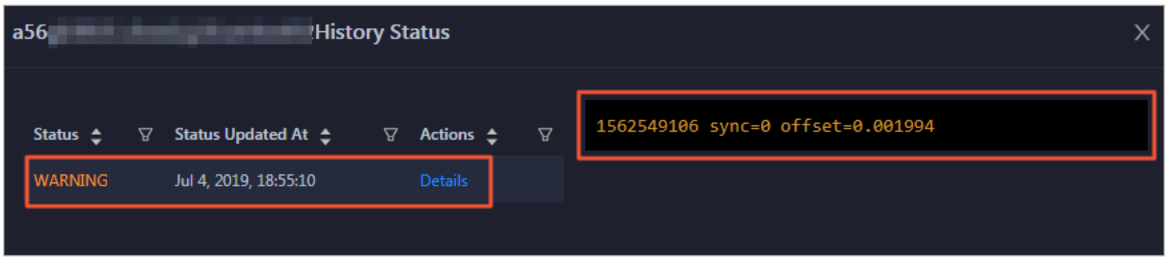
1. On the Health Status page, click **+** to expand a checker with alerts.



	Checker	Source	Critical	Warning	Exception	Actions
-	bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a56[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

2. Click the hostname. In the dialog box that appears, click **Details** in the Actions column of a check result to view the alert causes.

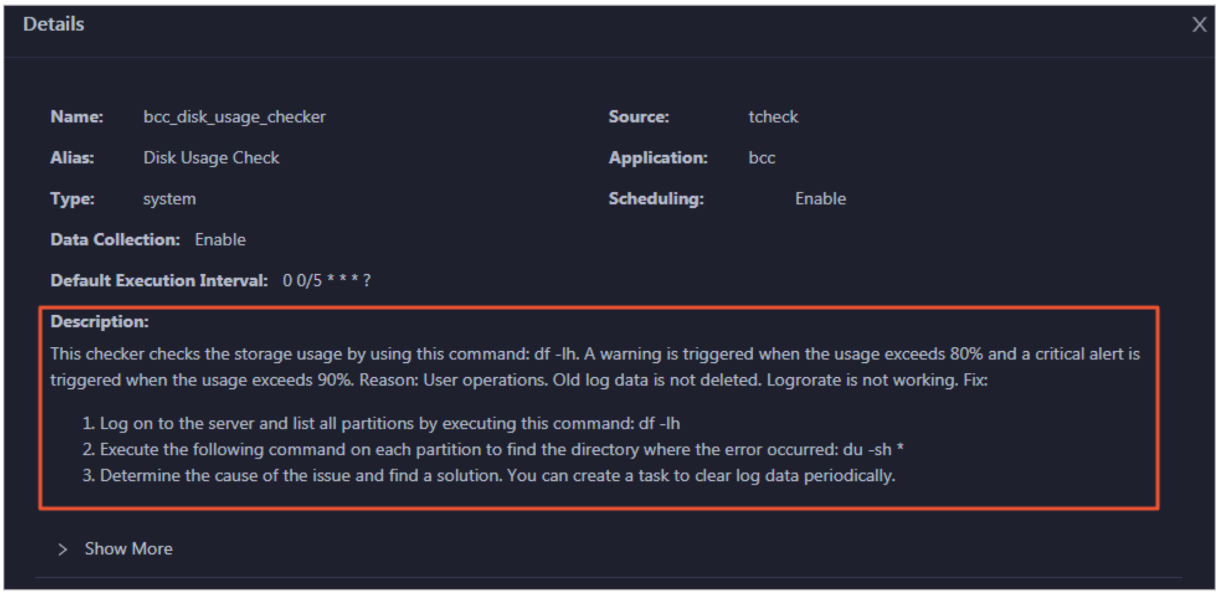

a56[redacted]History Status

Status	Status Updated At	Actions
WARNING	Jul 4, 2019, 18:55:10	Details

```
1562549106 sync=0 offset=0.001994
```

Clear alerts

On the Health Status page, click **Details** in the Actions column of a checker with alerts. In the dialog box that appears, view the schemes to clear alerts.


Details

Name: bcc_disk_usage_checker

Source: tcheck

Alias: Disk Usage Check

Application: bcc

Type: system

Scheduling: Enable

Data Collection: Enable

Default Execution Interval: 0 0/5 * * * ?

Description:

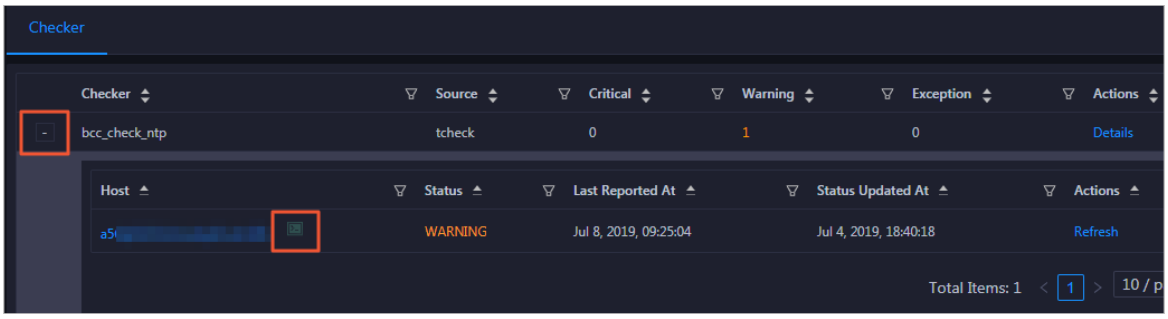
This checker checks the storage usage by using this command: df -lh. A warning is triggered when the usage exceeds 80% and a critical alert is triggered when the usage exceeds 90%. Reason: User operations. Old log data is not deleted. Logrorate is not working. Fix:

1. Log on to the server and list all partitions by executing this command: df -lh
2. Execute the following command on each partition to find the directory where the error occurred: du -sh *
3. Determine the cause of the issue and find a solution. You can create a task to clear log data periodically.

Log on to a host

To log on to a host to clear alerts or perform other operations, follow these steps:

1. On the Health Status page, click **+** to expand a checker with alerts.

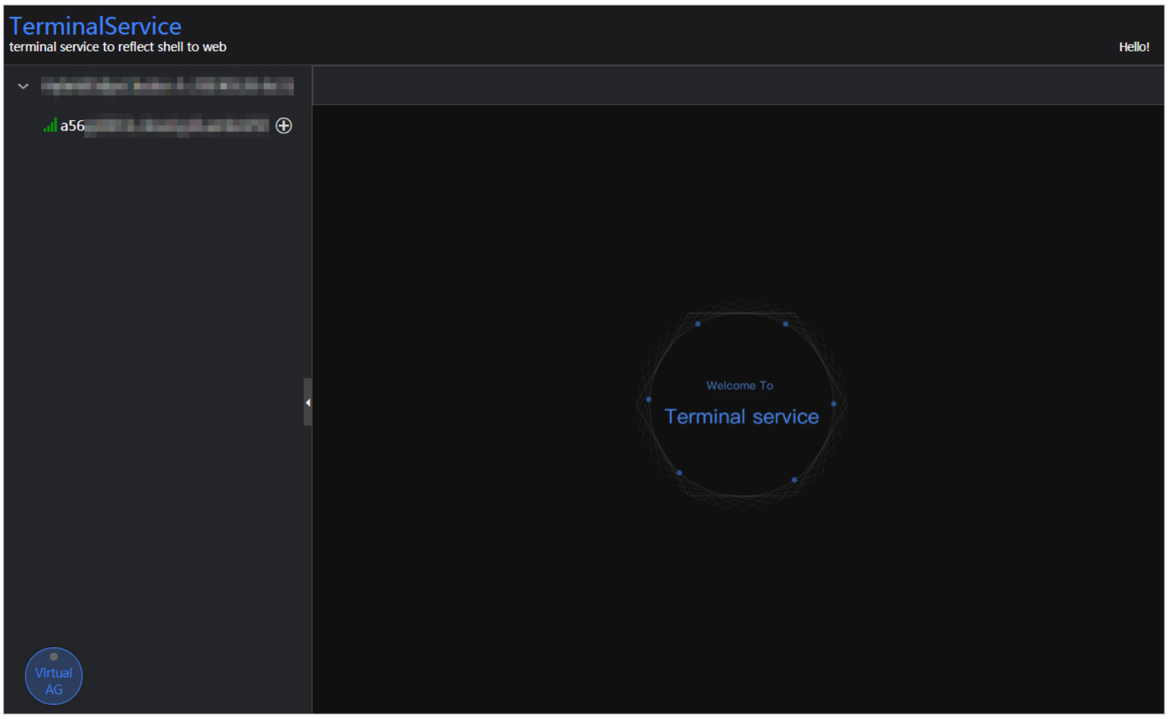


Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	1	0	Details

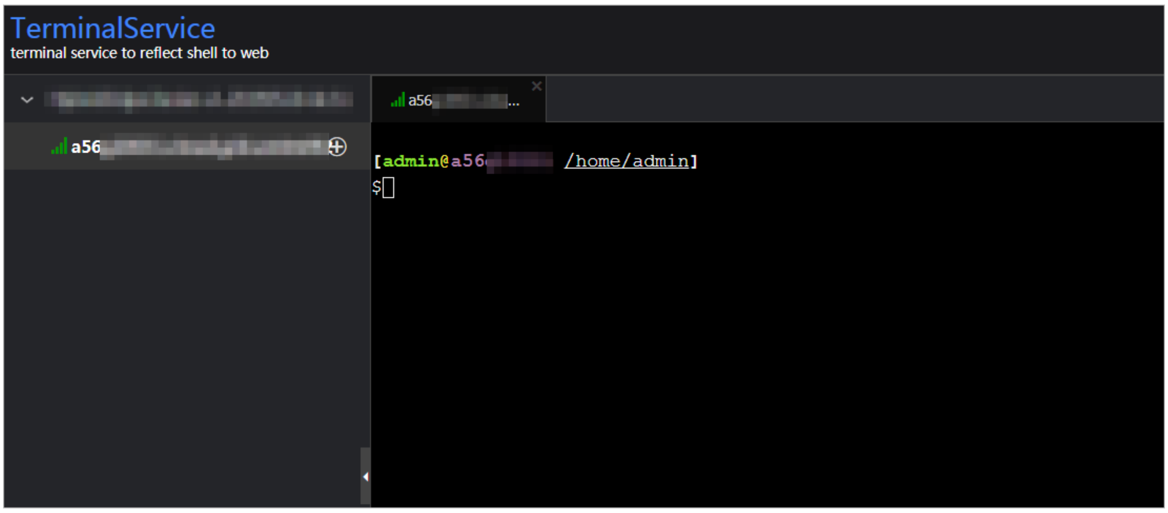
Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

2. Click the **Log On** icon of a host. The **TerminalService** page appears.



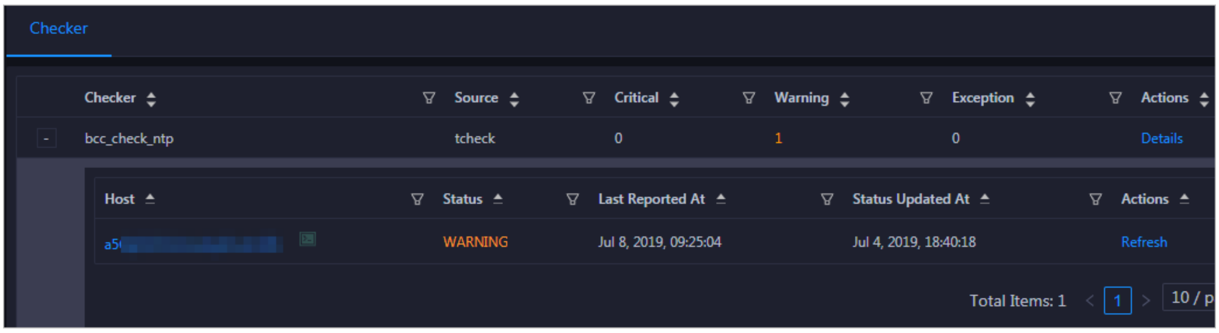
3. On the **TerminalService** page, click the hostname on the left to log on to the host.



```
[admin@a56[redacted] /home/admin]
$
```

Run a checker again

After you clear an alert for a host, click **Refresh** in the Actions column of the host to run the checker again for the host. In this way, you can check whether the alert is cleared.



Checker	Source	Critical	Warning	Exception	Actions
bcc_check_ntp	tcheck	0	1	0	Details

Host	Status	Last Reported At	Status Updated At	Actions
a5[redacted]	WARNING	Jul 8, 2019, 09:25:04	Jul 4, 2019, 18:40:18	Refresh

Total Items: 1 < 1 > 10 / p

11.12.7.4. Host services

On the Services page, you can view information about service instances and service instance roles of a host.

On the **Hosts** page, select a host in the left-side navigation pane, and then click the **Services** tab. The **Services** page for the host appears.

On the **Services** page, you can view the cluster, service instances, and service instance roles of the host.

11.12.8. Online O&M

11.12.8.1. Cluster health

You can view the statistical information of Elasticsearch clusters. The cluster health information is the most important. An Elasticsearch cluster has three health states: red, yellow, and green. This topic describes how to view the health status of an Elasticsearch cluster. It also provides more information about the preceding states.

You can run the following command to view the health status of a cluster:

```
curl -u Username:Password http://domain:9200/_cluster/health
```

State	Description	Remarks
red	Not all of the shards are available.	One or more indexes have unassigned shards.
yellow	All shards are available, but not all of the replicas are available.	One or more indexes have unassigned replicas.
green	All shards and replicas are available.	All indexes in the cluster are healthy and do not have unassigned shards or replicas.

Notice To ensure that the health state of your Elasticsearch cluster is green, all shards and replicas must be available at all times. We recommend that the number of replicas be less than or equal to amount_Node minus one. amount_Node represents the number of nodes. This ensures that the health state of your Elasticsearch cluster is green after it is restarted when dedicated master nodes are used.

11.12.9. Common failure troubleshooting

11.12.9.1. Resolve the issue that the health state of an Elasticsearch cluster is yellow

If the health state of your Elasticsearch is yellow, operations such as password resets and cluster upgrades are time-consuming. We recommend that you perform these operations when the health state of the cluster is green.

Cause: Some replicas are unassigned. You must check which indexes in the cluster have unassigned replicas.

11.12.9.2. Query index status

This topic describes how to view the status of an index in an Elasticsearch cluster.

You can run the following command to check which indexes have unassigned replicas:

```
curl -u Username:Password http://domain:9200/_cat/indices
```

If the cause of the issue is that the number of replicas is greater than amount_Node minus one, you must change the number of replicas for those indexes.

11.12.9.3. Recover an index

If your Elasticsearch cluster has three nodes and one or more indexes have three replicas, the health state of the cluster is yellow. This topic describes how to recover the indexes.

You can run the following command to set the number of replicas to 2:

```
curl -XPUT -u Username:Password http://domain:9200/Name of the index with unassigned replicas/_settings
-H 'Content-Type:
application/json' -d '{"index":{"number_of_replicas":(amount_Node - 1)}'
```

> **Note** After you perform operations such as restart, scale-out, and configuration modification, set an appropriate number of replicas based on the number of nodes. This improves the reliability and stability of your Elasticsearch cluster.

12.Appendix

12.1. Operation Access Manager (OAM)

12.1.1. Introduction to OAM

This topic describes the features and permission model of Operation Administrator Manager (OAM).

Overview

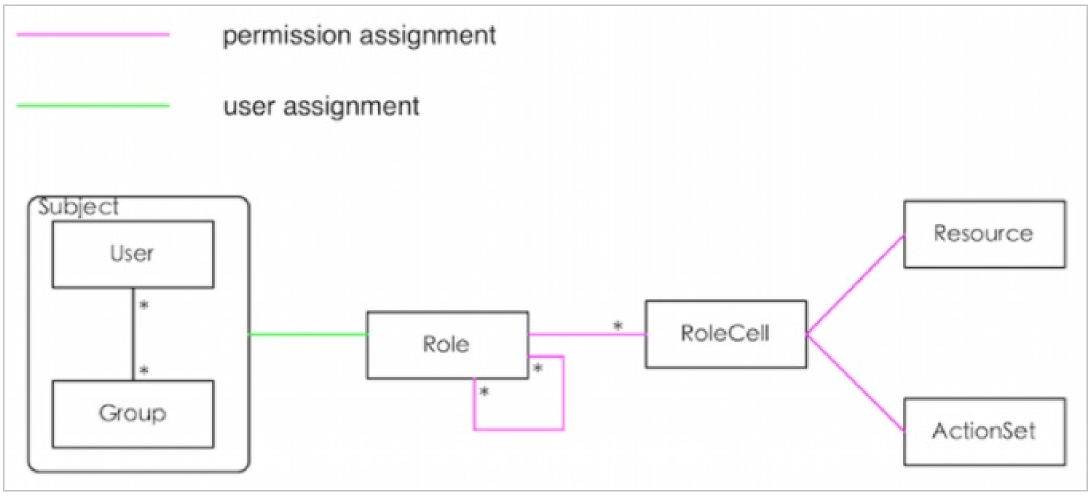
OAM is a centralized permission management platform in the Apsara Uni-manager Operations Console. OAM uses a simplified role-based access control (RBAC) model. Administrators can use OAM to assign roles to O&M personnel who are then granted the corresponding operation permissions on O&M systems.

OAM permission model

In RBAC, administrators do not directly grant system operation permissions to users. Instead, they create a role set that can be associated with sets of users and permissions. Each role has a set of permissions. When a role is assigned to a user, the user is granted all the operation permissions of that role. This way, administrators only need to assign a role to the user when they create the user, eliminating the need to grant permissions to the user. In addition, changes in role permissions occur less often than changes in user permissions, which leads to simplified user permission management and reduced system overheads.

The following figure shows the OAM permission model.

OAM permission model



12.1.2. Usage instructions

Before you use OAM, you must understand the following basic terms about permission management.

subject

The operators of the access control system. OAM has two types of subjects: user and group.

user

The administrators and operators of O&M systems.

group

A collection of users.

role

The core of the role-based access control (RBAC) system.

Typically, a role can be regarded as a collection of permissions. One role can include multiple role cells or roles.

role hierarchy

In OAM, one role can include other roles to form role hierarchy.

role cell

The specific description of a permission. A role cell consists of resources, action sets, and grant options.

resource

The description of an authorized object. For more information about the resources of O&M platforms, see **Operation permissions on O&M platforms**.

action set

The description of authorized actions. An action set can include multiple actions. For more information about the actions of O&M platforms, see **Operation permissions on O&M platforms**.

grant option

The maximum number of grants in the cascaded grant, which is an integer greater than or equal to zero. If the value is not zero, the permission can be granted. If the value is zero, the permission cannot be granted.

For example, if Administrator A sets Grant Option to 5 when Administrator A grants a permission to Administrator B, the permission can be granted another five times at most. When Administrator B grants the permission to Administrator C, the value of Grant Option cannot be greater than 4. If Grant Option is set to 0 when Administrator B grants the permission to Operator D, Operator D can only use the permission but cannot grant it to others.

> **Note** OAM does not support the cascaded revocation for cascaded grant. Therefore, Administrator C and Operator D still have the permission even if the permission is revoked for Administrator B.

12.1.3. Quick Start

By completing the steps in this guide, you will learn how to create and assign roles for O&M.

12.1.3.1. Log on to OAM

This topic describes how to log on to OAM.

Prerequisites

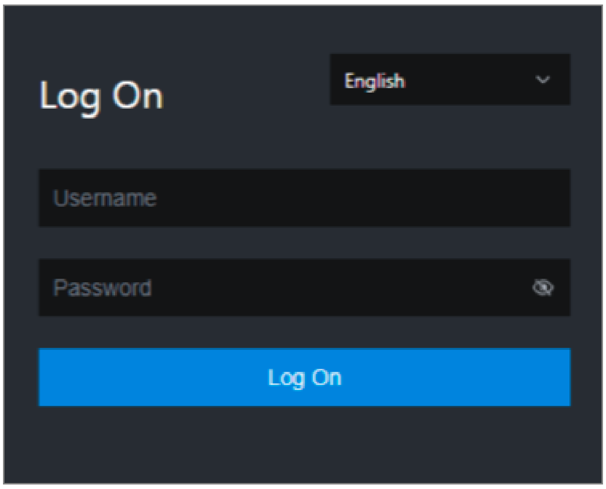
- The endpoint of the Apsara Uni-manager Operations Console and the username and password used to log on to the console are obtained from the deployment personnel or an administrator.

  The URL of the Apsara Uni-manager Operations Console is in the following format: *ops*.asconsole.*intranet-domain-id*.com.

- A browser is available. We recommend that you use Google Chrome.

Procedure

1. Open your browser.
2. In the address bar, enter the URL (*ops*.asconsole.*intranet-domain-id*.com). Then, press the Enter key.

   Note You can select a language from the drop-down list in the upper-right corner of the page.

3. Enter your username and password.

   Note Obtain the username and password used to log on to the Apsara Uni-manager Operations Console from the deployment personnel or an administrator.

   When you log on to the Apsara Uni-manager Operations Console for the first time, you must change the password of your username.

   For security reasons, your password must meet the following requirements:

   - The password contains uppercase and lowercase letters.
   - The password contains digits.
   - The password contains special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent signs (%).
   - The password must be 10 to 20 characters in length.

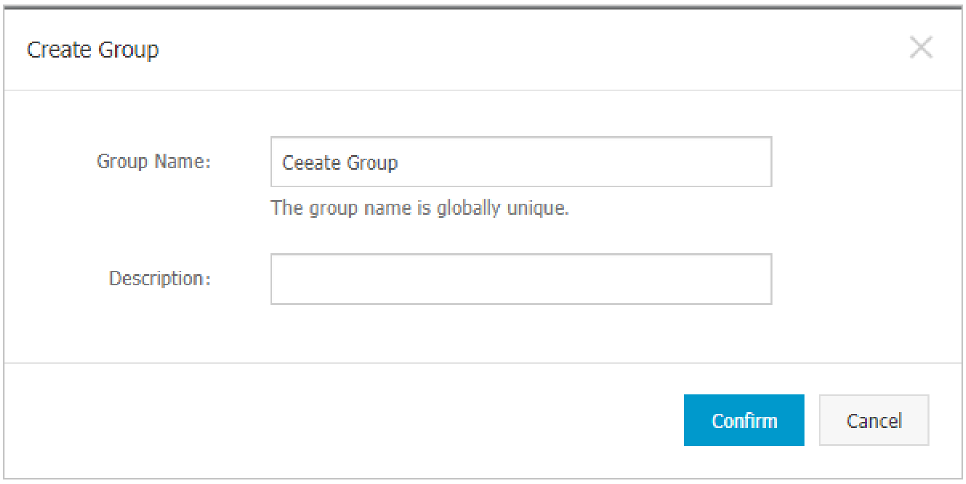
4. Click **Log On**.
5. In the top navigation bar, click **O&M**. In the left-side navigation pane, choose **Product Management > Products**. In the **Apsara Stack O&M** section, click **OAM**.

12.1.3.2. Create a group

You can create user groups for centralized management.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Group Management > Owned Groups**.
3. On the Owned Groups page, click **Create Group** in the upper-right corner. In the **Create Group** dialog box, set **Group Name** and **Description**.



Create Group

Group Name: Ceeate Group

The group name is globally unique.

Description:

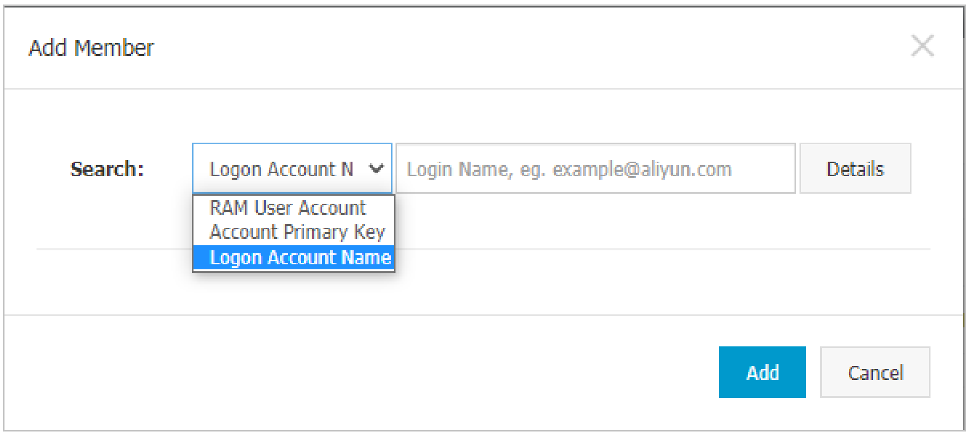
4. Click **Confirm**.After the group is created, it is displayed on the **Owned Groups** page.

12.1.3.3. Add a group member

You can add members to an existing group to grant permissions to the group members in a centralized manner.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Group Management > Owned Groups**.
3. Find the group whose name and description you want to modify and click **Manage** in the **Actions** column.
4. In the **Group Member** section, click **Add Member** in the upper-right corner.



5. Select a search mode, enter the corresponding information, and then click **Details**. Details of the specified user are displayed.

   Three search modes are available:

   - **RAM User Account**: Enter a RAM user in the format of RAM user@Apsara Stack tenant account ID to search for the RAM user.
   - **Account Primary Key**: Search by using the unique ID of the Apsara Stack tenant account.
   - **Logon Account Name**: Search by using the logon name of the Apsara Stack tenant account.

6. Click **Add**.
7. You can repeat the preceding steps to add multiple group members.To remove a member from a group, click **Remove** in the **Actions** column corresponding to the member.

12.1.3.4. Add a group role

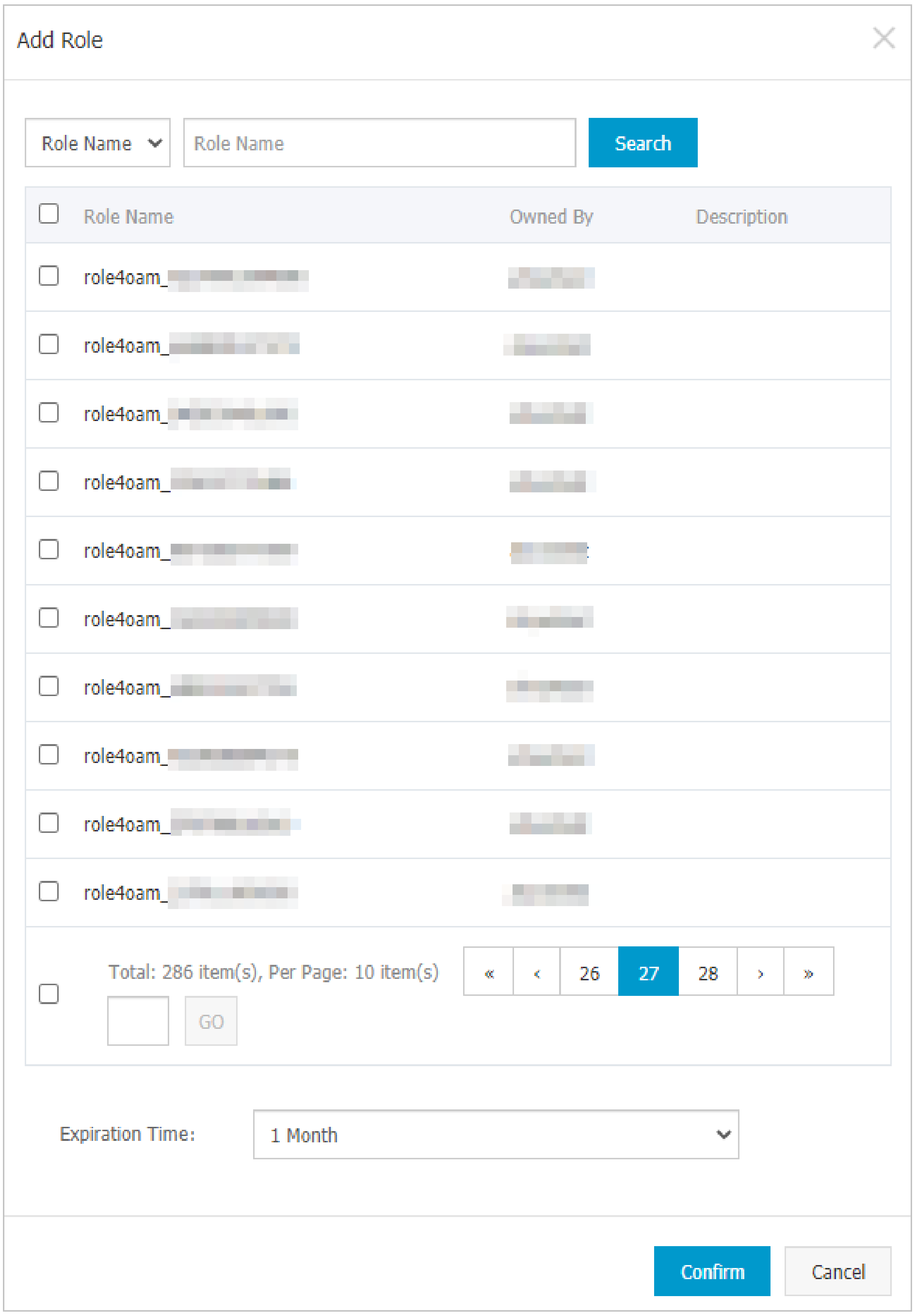
You can add roles to an existing group.

Prerequisites

- The role to be added is created. For more information, see Create a role.
- You are the owner of the group and the role.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Group Management > Owned Groups**.
3. Find the group whose name and description you want to modify and click **Manage** in the **Actions** column.
4. In the upper-right corner of the **Role List** section, click **Add Role**.



□	Role Name	Owned By	Description
□	role4oam_[redacted]	[redacted]	
□	role4oam_[redacted]	[redacted]	
□	role4oam_[redacted]	[redacted]	
□	role4oam_[redacted]	[redacted]	
□	role4oam_[redacted]	[redacted]	
□	role4oam_[redacted]	[redacted]	
□	role4oam_[redacted]	[redacted]	
□	role4oam_[redacted]	[redacted]	
□	role4oam_[redacted]	[redacted]	
□	role4oam_[redacted]	[redacted]	

□ Total: 286 item(s), Per Page: 10 item(s)

Expiration Time: 1 Month

5. Search for roles by **Role Name**. Select one or more roles and set Expiration Time.
6. Click **Confirm**.

   To remove a role from a group, find the role in **Role List** and click **Remove** in the **Actions** column.

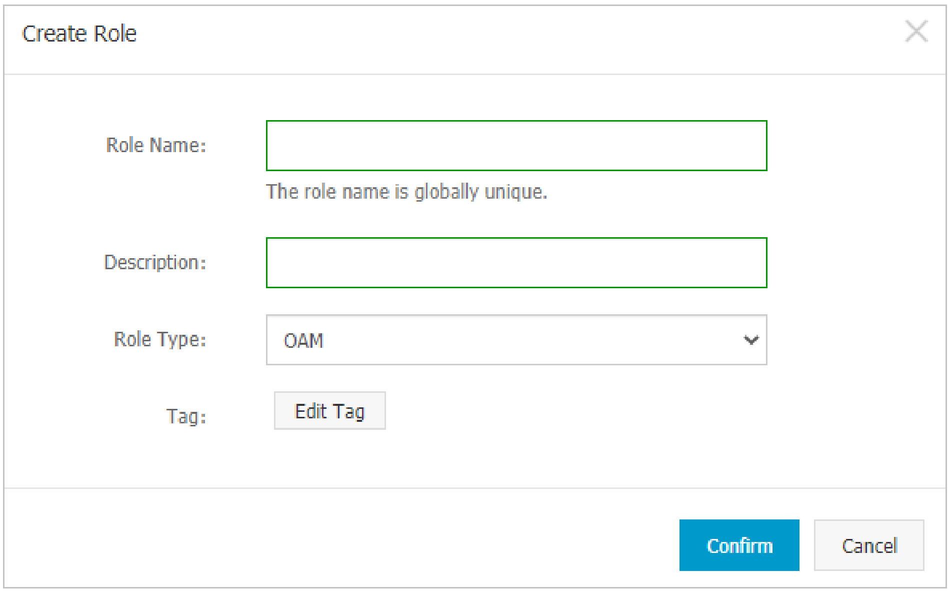
12.1.3.5. Create a role

This topic describes how to create a role.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > Owned Roles**.

3. On the **Owned Roles** page, click **Create Role** in the upper-right corner.



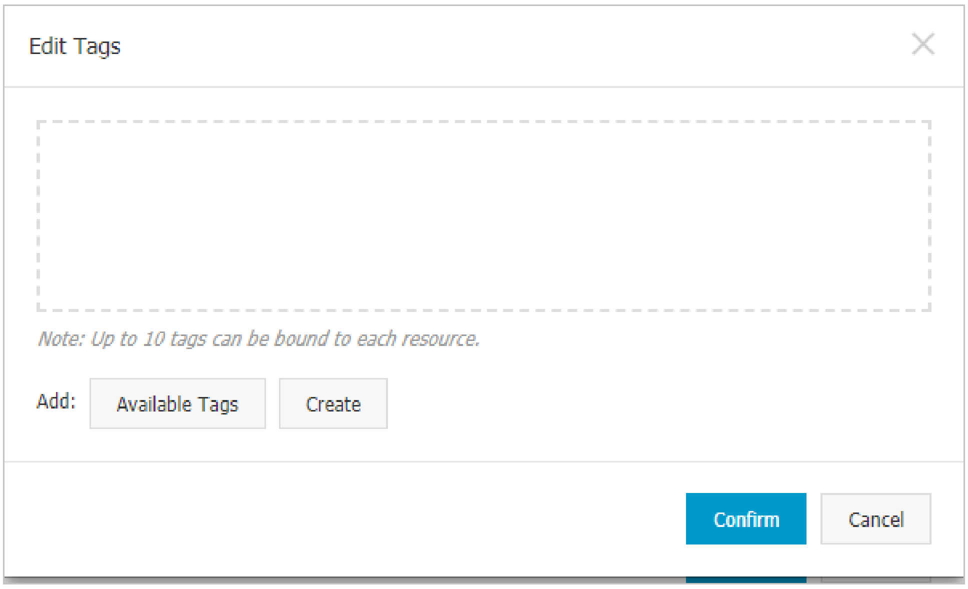
The role name is globally unique.

Role Type: OAM

4. In the Create Role dialog box, set **Role Name**, **Description**, and **Role Type**.

5. (Optional)Set tags for the role. Tags can be used to search for roles.

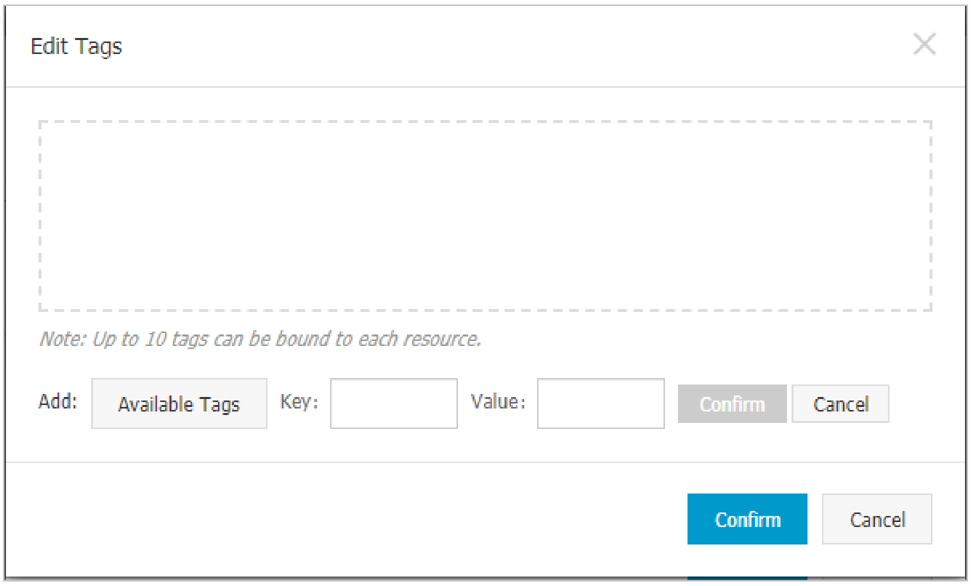
   i. Click **Edit Tag**.

   Note: Up to 10 tags can be bound to each resource.

   ii. In the **Edit Tags** dialog box, click **Create**.

iii. Set **Key** and **Value** for the tag and click **Confirm**.



Note: Up to 10 tags can be bound to each resource.

iv. Repeat the preceding step to create more tags.

The created tags are displayed inside the dotted box.

v. Click **Confirm** to create the tags and exit the **Edit Tags** dialog box.

6. Click **Confirm** to create the role.

12.1.3.6. Add an inherited role to a role

You can add inherited roles to a role to grant the permissions of the inherited roles to the role.

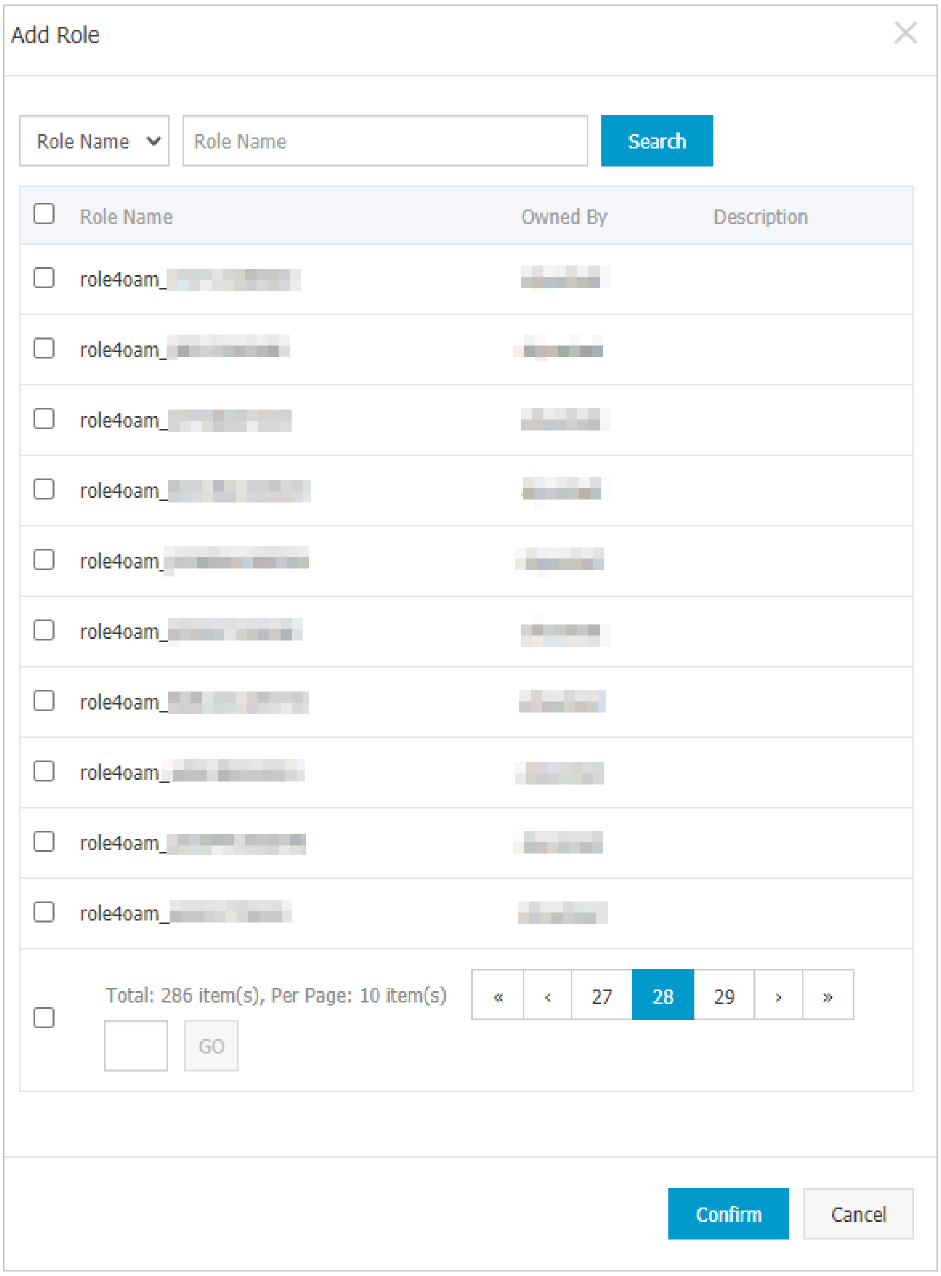
Prerequisites

You are the owner of the current role and the inherited role to be added.

For more information about how to query your owned roles, see Query roles.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > Owned Roles**.
3. Find the role to which you want to add an inherited role and click **Manage** in the **Actions** column.
4. On the Role Information page, click the **Inherited Role** tab.
5. Click **Add Role**. In the **Add Role** dialog box, search for roles by **Role Name**. Select one or more roles.



Add Role

☐	Role Name	Owned By	Description
☐	role4oam_[redacted]	[redacted]	
☐	role4oam_[redacted]	[redacted]	
☐	role4oam_[redacted]	[redacted]	
☐	role4oam_[redacted]	[redacted]	
☐	role4oam_[redacted]	[redacted]	
☐	role4oam_[redacted]	[redacted]	
☐	role4oam_[redacted]	[redacted]	
☐	role4oam_[redacted]	[redacted]	
☐	role4oam_[redacted]	[redacted]	
☐	role4oam_[redacted]	[redacted]	

☐ Total: 286 item(s), Per Page: 10 item(s)

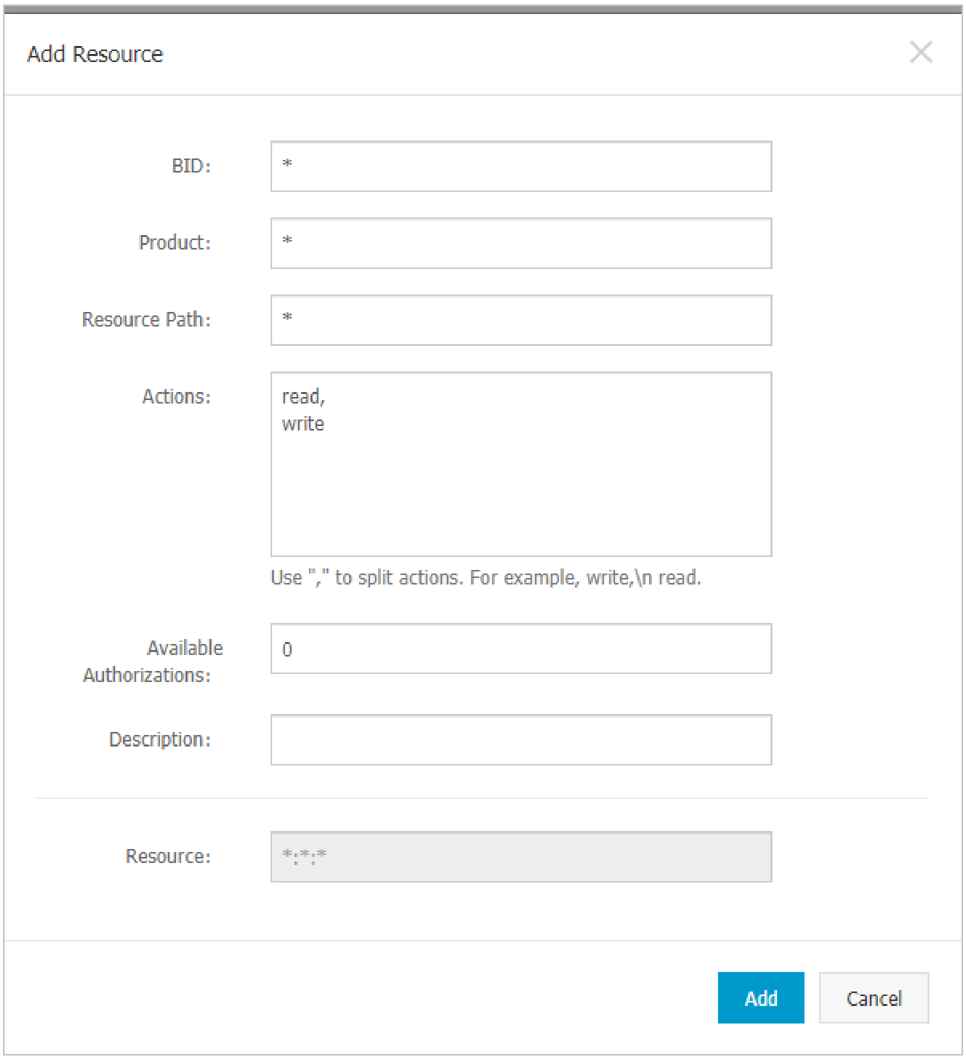
6. Click **Confirm**.

12.1.3.7. Add a resource to a role

You must add resources to a created role.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > Owned Roles**.
3. Find the role to which you want to add a resource and click **Manage** in the **Actions** column.
4. On the Role Information page, click the **Resource List** tab.
5. Click **Add Resource**.



Add Resource

BID: *

Product: *

Resource Path: *

Actions: read,
write

Use "," to split actions. For example, write,\n read.

Available Authorizations: 0

Description:

Resource: *:*:*

6. In the **Add Resource** dialog box, configure the parameters. For more information, see Parameters.Parameters

Parameter	Description
BID	The deployment region ID.
Product	The cloud service to be added. Example: rds. **Note** The cloud service name must be lowercase. For example, enter **rds** instead of **RDS**.
Resource Path	The resources of the cloud service. For more information about resources of the O&M platforms, see **Operation permissions on O&M platforms**.
Actions	An action set, which can contain multiple actions. For more information about actions on the O&M platforms, see **Operation permissions on O&M platforms**.

Parameter	Description
Available Authorizations	The maximum number of grants in cascaded grant, which must be an integer greater than or equal to zero. If the value is not zero, the permission can be granted. If the value is zero, the permission cannot be granted.
Description	The description of the resource.

7. Click **Add**.

12.1.3.8. Assign a role to authorized users

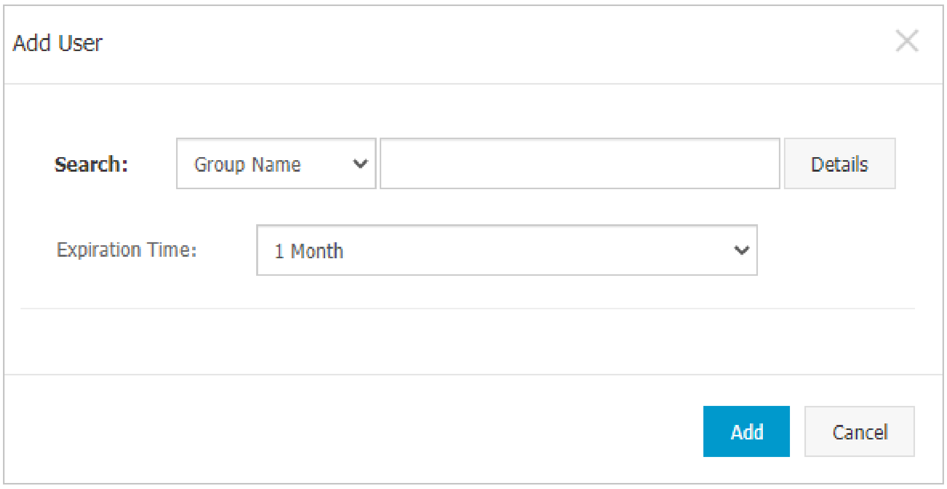
You can assign an existing role to users or user groups.

Prerequisites

The corresponding users or user groups are created. Users are created in the Apsara Uni-manager Operations Console. For more information about how to create a user group, see Create a group.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > Owned Roles**.
3. Find the role that you want to assign to a user and click **Manage** in the **Actions** column.
4. On the Role Information page, click the **Authorized Users** tab.
5. Click **Add User** in the upper-right corner.



6. Select a search mode and enter corresponding information to search for the user to which you want to assign the role.

   Four search modes are available:

   - **RAM User Account**: Enter a RAM user in the format of *RAM user@Apsara Stack tenant account ID* to search for the RAM user.
   - **Account Primary Key**: Search by using the unique ID of the Apsara Stack tenant account.
   - **Logon Account Name**: Search by using the logon name of the Apsara Stack tenant account.

- **Group Name**: Search by group name.

> ? **Note** You can search for a single user or user group. For more information about how to create a user group, see Create a group.

7. Set Expiration Time.When the specified expiration time is due, the user no longer has the permissions of the role. To grant permissions to the user again, click **Renew** in the Actions column corresponding to the authorized user on the **Authorized Users** tab to modify the expiration time.
8. Click **Add** to assign the role to the user.To cancel the authorization, click **Remove** in the Actions column corresponding to the authorized user on the **Authorized Users** tab.

12.1.4. Manage groups

Group management allows you to view, modify, and delete groups.

12.1.4.1. Modify group information

After you create a group, you can modify the group name and description on the Group Information page.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Group Management > Owned Groups**.
3. Find the group whose name and description you want to modify and click **Manage** in the **Actions** column.
4. On the Group Information page, click **Modify** in the upper-right corner.
5. In the **Modify Group** dialog box, modify the group name and description.
6. Click **Confirm**.

12.1.4.2. View group role details

You can view the information about inherited roles, resource list, and inheritance tree of a group role.

Prerequisites

A role is added to the group.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Group Management > Owned Groups**.
3. Find the group and click **Manage** in the **Actions** column.
4. In **Role List** section, click **Details** in the Actions column corresponding to the role.
5. On the **Role Information** page, perform the following operations:
   - Click the **Inherited Role** tab to view the information about the inherited roles of the role.

     To view the detailed information of an inherited role, click **Details** in the **Actions** column corresponding to the inherited role.

- Click the **Resource List** tab to view the resource information of the role.

  For information about how to add resources to this role, see Add a resource to a role.

- Click the **Inheritance Tree** tab to view the basic information and resource information of the role and its inherited roles by using the inheritance tree on the left.

12.1.4.3. Delete a group

You can delete a group that is no longer needed.

Prerequisites

The group to be deleted does not contain members.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Group Management** > **Owned Groups**.
3. Find the group that you want to delete and click **Remove** in the **Actions** column. In the message that appears, click **OK**.

12.1.4.4. View authorized groups

You can view the groups to which you are added on the Authorized Groups page.

Context

You can view only the groups to which you belong, but cannot view groups of other users.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Group Management** > **Authorized Groups**.
3. On the **Authorized Groups** page, view the name, owner, description, and modification time of the group to which you belong.

12.1.5. Manage roles

Role management allows you to view, modify, transfer, and delete roles.

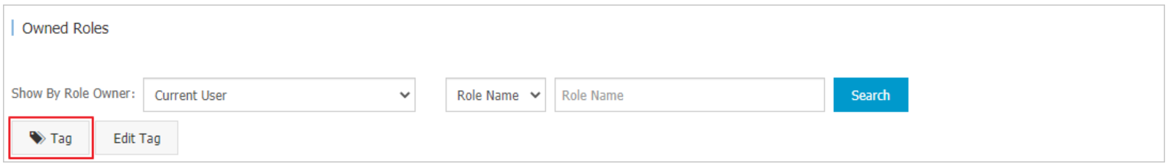
12.1.5.1. Query roles

You can view your owned roles on the Owned Roles page.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management** > **Owned Roles**.
3. Enter a role name in the **Role Name** search box and click **Search** to search for roles that meet the search condition.

> **Note** If the role that you want to search for has a tag, you can click **Tag** and select a tag key to search for the role based on the tag.



12.1.5.2. Modify role information

After you create a role, you can modify the role information.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > Owned Roles**.
3. Find the role whose information you want to modify and click **Manage** in the **Actions** column.
4. On the Role Information page, click **Modify** in the upper-right corner.
5. In the **Modify Role** dialog box, set **Role Name**, **Description**, **Role Type**, and **Tag**.
6. Click **Confirm**.

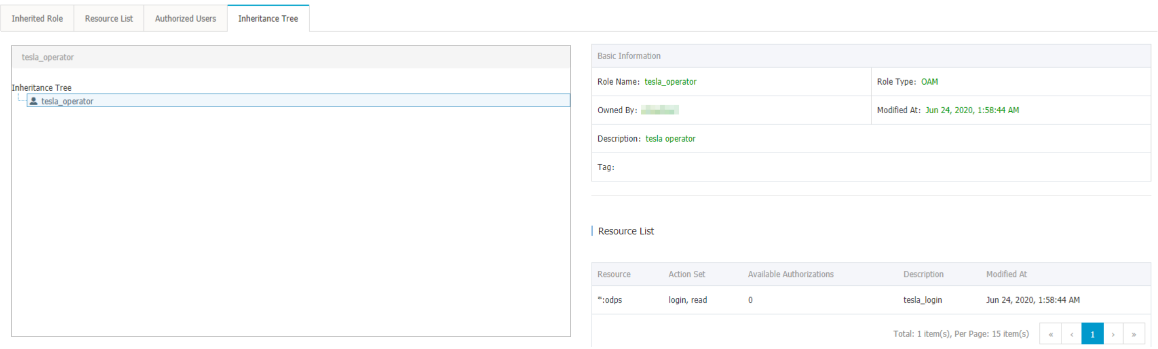
12.1.5.3. View the role inheritance tree

You can view the role inheritance tree to learn about the basic information and resource information of a role and its inherited roles.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > Owned Roles**.
3. Find the role whose information you want to modify and click **Manage** in the **Actions** column.
4. On the **Role Information** page, click the **Inheritance Tree** tab.

   View the basic information and resource information of the role and its inherited roles by using the inheritance tree on the left.



Role Name: tesla_operator
Role Type: OAM
Owned By: [redacted]
Modified At: Jun 24, 2020, 1:58:44 AM
Description: tesla operator
Tag:

Resource	Action Set	Available Authorizations	Description	Modified At
*:odps	login, read	0	tesla_login	Jun 24, 2020, 1:58:44 AM

Total: 1 item(s), Per Page: 15 item(s)

12.1.5.4. Transfer a role

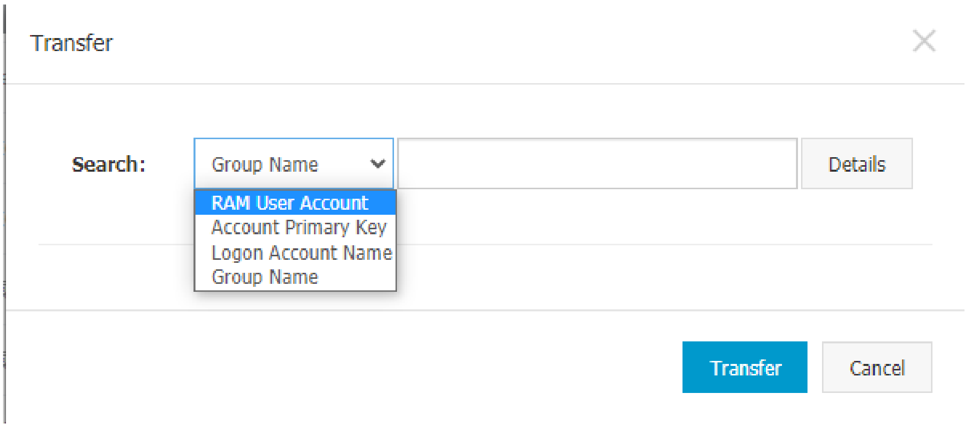
You can transfer a role to other users or groups based on your business requirements.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > Owned Roles**.
3. On the Owned Roles page, set the search conditions and search for the roles that you want to transfer.
4. Select one or more roles in the search results and click **Transfer** in the lower-left corner.
5. In the **Transfer** dialog box, select a search mode, enter the corresponding information, and then click **Details**. Details of the user or group are displayed.

   Four search modes are available:

   - **RAM User Account**: Enter a RAM user in the format of RAM user@Apsara Stack tenant account ID to search for the RAM user.
   - **Account Primary Key**: Search by using the unique ID of the Apsara Stack tenant account.
   - **Logon Account Name**: Search by using the logon name of the Apsara Stack tenant account.
   - **Group Name**: Search by group name.



6. Click **Transfer**.

12.1.5.5. Delete a role

You can delete roles that are no longer needed.

Prerequisites

The role to be deleted does not contain inherited roles, resources, or authorized users.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > Owned Roles**.
3. Find the role that you want to delete and click **Delete** in the Actions column. In the message that appears, click **OK**.

12.1.5.6. View assigned roles

You can view the roles assigned to you and the permissions granted to the roles.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > Authorized Roles**.
3. On the **Authorized Roles** page, you can view the name, owner, description, modification time, and expiration time of each role assigned to you.You can also click **Details** in the **Actions** column corresponding to a role to view the inherited roles, resources, and inheritance tree of the role.

12.1.5.7. View all roles

You can view all the roles in OAM on the All Roles page.

Procedure

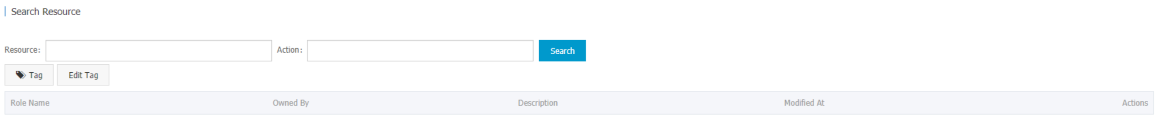
1. Log on to OAM.
2. In the left-side navigation pane, choose **Role Management > All Roles**.
3. On the **All Roles** page, view all the roles in the system.You can search for roles by **Role Name**.
4. Click **Details** in the **Actions** column corresponding to a role to view the inherited roles, resources, and inheritance tree of the role.

12.1.6. Search for resources

You can search for resources to view the roles to which the resources are assigned.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, click **Search Resource**.
3. Set **Resource** and **Action**, and click **Search** to search for the roles that meet the specified conditions.



4. Click **Details** in the **Actions** column corresponding to a role to view the inherited roles, resources, and inheritance tree of the role.

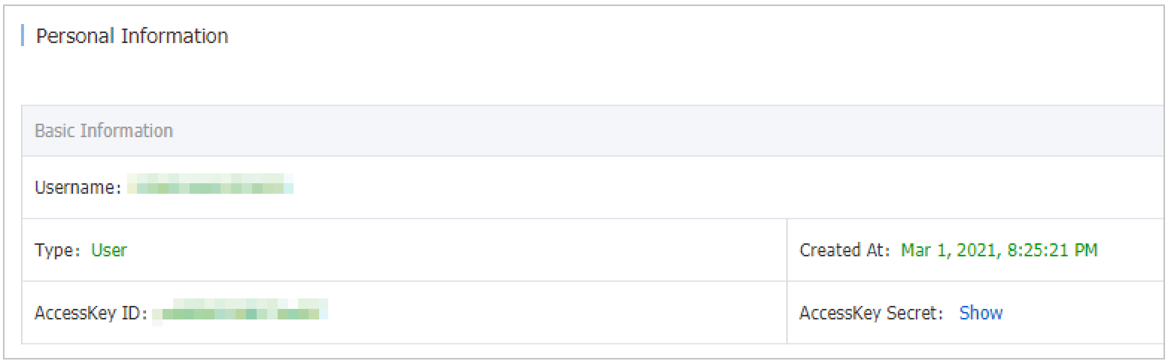
12.1.7. View personal information

You can view the personal information of the current user on the Personal Information page and test the user permissions.

Procedure

1. Log on to OAM.
2. In the left-side navigation pane, click **Personal Information**.
3. In the **Basic Information** section, view the username, type, creation time, AccessKey ID, and

AccessKey secret of the current user.



Personal Information

Basic Information

Username: [redacted]

Type: User

Created At: Mar 1, 2021, 8:25:21 PM

AccessKey ID: [redacted]

AccessKey Secret: Show

> Note You can click **Show** or **Hide** to show or hide the AccessKey secret.

4. In the **Test Permission** section, check whether the current user has a specific permission.

   i. Enter the resource information in the **Resource** field.

   > Note Use the English input method when you enter values in the **Resource** and **Action** fields.

   ii. Enter the permissions such as create, read, and write in the **Action** field. Separate multiple permissions with commas (,).

12.1.8. Default roles and permissions

12.1.8.1. Default roles and their functions

This topic describes the default roles in Operation Access Manager (OAM) and their functions.

12.1.8.1.1. Default role of OAM

This topic describes the default role of Operation Access Manager (OAM) and the corresponding available authorizations.

Role name	Role description	Resource	Actions	Available authorizations
Super administrator	An administrator with root permissions	*:*	*	10

12.1.8.1.2. Default roles of Tablestore Operations and Maintenance System

This topic describes the default roles of Tablestore Operations and Maintenance System and the corresponding grant options.

Tablestore Operations and Maintenance System is an operations and maintenance platform for Tablestore.

The following table describes the default roles of Tablestore Operations and Maintenance System and the corresponding grant options.

Role	Description	Resource	Action	Grant option
Public permissions on Tablestore Operations and Maintenance System	Has the basic permissions on Tablestore Operations and Maintenance System. This role is required for granting.	*:ots:*	["*"]	0

12.1.8.1.3. Default roles of Apsara Infrastructure Management Framework

This topic describes the default roles of Apsara Infrastructure Management Framework and the corresponding grant options.

Apsara Infrastructure Management Framework is a distributed data center management system. It can manage applications within clusters that include multiple machines and provide basic features such as deployment, upgrade, scale-in, scale-out, and configuration change.

The following table describes the default roles of Apsara Infrastructure Management Framework and the corresponding grant options.

Role	Description	Resource	Action	Grant option
Tianji_Project read-only	Has the read-only permission on Apsara Infrastructure Management Framework projects, which allows you to view the configurations and statuses of all projects and clusters.	*:tianji:projects	["read"]	0

Role	Description	Resource	Action	Grant option
Tianji_Project administrator	Has all the permissions on Apsara Infrastructure Management Framework projects, which allows you to view and modify the configurations and statuses of all projects and clusters.	*:tianji:projects	["*"]	0
Tianji_Service read-only	Has the read-only permission on Apsara Infrastructure Management Framework services, which allows you to view the configurations and templates of all services.	*:tianji:services	["read"]	0
Tianji_Service administrator	Has all the permissions on Apsara Infrastructure Management Framework services, which allows you to view and modify the configurations and templates of all services.	*:tianji:services	["*"]	0
Tianji_IDC administrator	Has all the permissions on Apsara Infrastructure Management Framework data centers, which allows you to view and modify the data center information.	*:tianji:idcs	["*"]	0

Role	Description	Resource	Action	Grant option
Tianji administrator	Has all the permissions on Apsara Infrastructure Management Framework, which allows you to perform operations on all Apsara Infrastructure Management Framework configurations.	*:tianji	["*"]	0

12.1.8.1.4. Default roles of Webapp-rule

This topic describes the default roles of Webapp-rule and the corresponding available authorizations.

Role name	Role description	Resource	Actions	Available authorizations
Webapp-rule operations administrator	Has all the permissions to Webapp-rule projects, which allows you to view, modify, add, and delete all the configurations and statuses	26842:webapp-rule:*	["read", "write"]	0
Webapp-rule read-only	Has the read-only permission to Webapp-rule projects, which allows you to view all the configurations and statuses	26842:webapp-rule:*	["read"]	0

12.1.8.1.5. Default roles of the workflow console

This topic describes the default roles of the workflow console and the corresponding available authorizations.

The workflow console Grandcanal is an internally distributed process development framework. Developers can assemble, retry, roll back, and manually intervene the process based on this framework. Operations engineers can use the workflow console to manually intervene the corresponding processes.

For more information about the default roles of the workflow console and the corresponding available authorizations, see the following table.

Role name	Role description	Resource	Actions	Available authorizations
grandcanal.ADMIN	The workflow console administrator, who can query the workflow and activity details, and retry, roll back, terminate, and restart a workflow	26842:grandcanal	[“write” ,"read"]	0
grandcanal.Reader	Has the read-only permission to the workflow console and can only perform the read operation	26842:grandcanal	["read"]	0

12.1.8.1.6. Default roles of Tianjimon

This topic describes the default roles of Tianjimon and the corresponding grant options.

Tianjimon is the monitoring module of Apsara Infrastructure Management Framework and monitors the physical machines and services deployed based on Apsara Infrastructure Management Framework.

The following table describes the default roles of Tianjimon and the corresponding grant options.

Role	Description	Resource	Action	Grant option
Tianjimon O&M	Has all the permissions on Tianjimon, which allows you to perform basic monitoring and O&M operations.	26842:tianjimon:*	["*"]	0

12.1.8.1.7. Default roles of Rtools

This topic describes the default roles of Rtools and the corresponding grant options.

Rtools is an assistant O&M system of Distributed Relational Database Service (DRDS). It is used to query metadata in the Diamond configuration management system.

The following table describes the default roles of Rtools and the corresponding grant options.

Role	Role description	Resource	Action	Grant option
Rtools administrator	Has all permissions in the Rtools console.	26842:drds:rtools:*	*	0

12.1.8.1.8. Default roles of the Apsara Uni-manager Operations Console

This topic describes the default roles of the Apsara Uni-manager Operations Console and the corresponding grant options.

The Apsara Uni-manager Operations Console is a centralized O&M management system that is developed for the Apsara Stack O&M personnel to perform centralized O&M operations.

The following table describes the default roles of the Apsara Uni-manager Operations Console and the corresponding grant options.

Role	Description	Resource	Action	Grant option
System administrator of the Apsara Uni-manager Operations Console	Has the permissions to manage platform nodes, physical devices, and virtual resources, back up, restore, and migrate product data, and query and back up system logs.	*:aso:api-adapter:*	["read","write"]	0
		:aso:auth:	["read"]	0
		:aso:backup:	["read","write"]	0
		:aso:cmdb:	["read","write"]	0
		:aso:doc:	["read","write"]	0
		:aso:fullview:	["read","write"]	0
		:aso:init:	["read","write"]	0
		:aso:inventory:	["read","write"]	0
		:aso:itil:	["read","write"]	0
		:aso:lock:	["read","write"]	0
		:aso:physical:	["read","write"]	0
		:aso:psm:	["read","write"]	0
		:aso:scm:	["read","write"]	0
		:aso:serviceWhitelist:	["read","write"]	0
		:aso:slalink:	["read","write"]	0

Role	Description	Resource	Action	Grant option
		:aso:task:	["read","write"]	0
Security officer of the Apsara Uni-manager Operations Console	Has the permissions to manage permissions, security polices, and network security, and review and analyze security logs and activities of security auditors.	*:aso:auth:*	["read","write"]	0
		:aso:plat-access:	["read","write"]	0
		:aso:twoFactorAuth:	["read","write"]	0
Security auditor of the Apsara Uni-manager Operations Console	Has the permissions to audit, track, and analyze the activities of the system administrator and security officer.	*:aso:audit:*	["read","write"]	0
		:aso:auth:	["read"]	0
		:aso:serviceWhitelist:	["read"]	0
Product O&M officer of the Apsara Uni-manager Operations Console	Has the permissions to perform O&M operations such as data import and export, modification, configuration, upgrade, and troubleshooting coordination.	*:aso:api-adapter:*	["read"]	0
		:aso:backup:	["read"]	0
		:aso:cmdb:	["read"]	0
		:aso:doc:	["read"]	0
		:aso:fullview:	["read","write"]	0
		:aso:init:	["read"]	0
		:aso:inventory:	["read","write"]	0
		:aso:itil:	["read"]	0
		:aso:lock:	["read"]	0
		:aso:physical:	["read","write"]	0
		:aso:psm:	["read"]	0
		:aso:scm:	["read"]	0
		:aso:slalink:	["read"]	0
		:aso:task:	["read"]	0

Role	Description	Resource	Action	Grant option
Common O&M officer of the Apsara Uni-manager Operations Console	Has the permissions to perform daily health checks and query service status, inventory information, and product usage.	*:aso:api-adapter:*	["read"]	0
		:aso:backup:	["read"]	0
		:aso:cmdb:	["read"]	0
		:aso:doc:	["read"]	0
		:aso:fullview:	["read"]	0
		:aso:init:	["read"]	0
		:aso:inventory:	["read","write"]	0
		:aso:itil:	["read"]	0
		:aso:lock:	["read"]	0
		:aso:physical:	["read","write"]	0
		:aso:psm:	["read"]	0
		:aso:scm:	["read"]	0
		:aso:slalink:	["read"]	0
		:aso:task:	["read"]	0
Duty observer of the Apsara Uni-manager Operations Console	Has the permissions to view and monitor the dashboard and monitor system alerts.	*:aso:doc:*	["read"]	0
		:aso:fullview:	["read"]	0

12.1.8.1.9. Default roles of PaaS

This topic describes the default roles of the Platform as a Service (PaaS) console and the corresponding grant options.

The PaaS console is an O&M platform designed for the PaaS platform and products, and is used to view, manage, and upgrade the products deployed on the PaaS platform.

The following table describes the default roles of the PaaS console and the corresponding grant options.

Role	Description	Resource	Action	Grant option
PaaS_Operation_Manager	Has all the permissions on the PaaS console.	*:paas-ops:*	["*"]	0

12.1.8.1.10. Default roles of OCP

This topic describes the default roles of the OceanBase Cloud Platform (OCP) and the corresponding grant options.

OCP is an enterprise-level database management platform with ApsaraDB for OceanBase as the core. It provides full lifecycle management for ApsaraDB for OceanBase components related to clusters, tenants, and databases, and manages ecosystem tools of ApsaraDB for OceanBase.

The following table describes the default roles of OCP and the corresponding grant options.

Role	Role description	Resource	Action	Grant option
ocp_readonly	Has the read-only permissions on OCP.	*:oceanbase:role:ocp_readonly	["access"]	0
ob_dev	Has permissions on the performance and monitoring modules.	*:oceanbase:role:ob_dev	["access"]	0
ocp_dev	Has all permissions on OCP, but does not have the grant permission.	*:oceanbase:role:ocp_dev	["access"]	0

12.1.8.1.11. Default roles of Apsara Stack Security

This topic describes the default roles of Apsara Stack Security and the corresponding grant options.

Apsara Stack Security is a solution that provides Apsara Stack with a full suite of security features, such as network security, server security, application security, data security, and security management.

The following table describes the default roles of Apsara Stack Security and the corresponding grant options.

Role	Role description	Resource	Action	Grant option
Apsara Stack Security administrator	Has all the permissions on Apsara Stack Security and can manage data in all the Apsara Stack Security modules.	*:yundun-luban:*	["*"]	0

Role	Role description	Resource	Action	Grant option
Apsara Stack Security viewer	Has the read permissions on Apsara Stack Security and can read data in all the Apsara Stack Security modules.	*:yundun-luban:*	["read"]	0

12.1.8.1.12. Default roles of Apsara Network Intelligence

This topic describes the default roles of Apsara Network Intelligence and the corresponding grant options.

Apsara Network Intelligence is a system designed for network traffic analysis. It provides data to facilitate resource planning, diagnosis, monitoring, system management, and user behavior analysis.

The following table describes the default roles of Apsara Network Intelligence and the corresponding grant options.

Role	Role description	Resource	Action	Grant option
Apsara Network Intelligence instance querier	Has permissions to query various instance resources.	- *:qitian:instance:* - *:qitian:user:*	["read","create","delete","update"]	0
Apsara Network Intelligence product O&M personnel	Has permissions to use the functions under the "Products" menu of Apsara Network Intelligence.	*:qitian:product:*	["read","create","delete","update"]	0
Apsara Network Intelligence R&D and O&M personnel	Has permissions to use the functions under the "System" menu of Apsara Network Intelligence.	*:qitian:system:*	["read","create","delete","update"]	0

12.1.8.2. Operation permissions on O&M platforms

This topic describes the operation permissions on O&M platforms.

12.1.8.2.1. Permissions on Apsara Infrastructure Management Framework

This topic describes the operation permissions on Apsara Infrastructure Management Framework.

Resource	Operation	Description
*:tianji:services:[sname]:tjmontemplates:[tmplname]	delete	Deletes a monitoring template.
*:tianji:services:[sname]:tjmontemplates:[tmplname]	write	Creates a monitoring template.
*:tianji:services:[sname]:templates:[tmplname]	write	Creates a service template.
*:tianji:services:[sname]:templates:[tmplname]	delete	Deletes a service template.
*:tianji:services:[sname]:serviceinstances:[siname]:tjmontemplate	read	Obtains a monitoring template.
*:tianji:services:[sname]:serviceinstances:[siname]:tssessions	terminal	Creates a remote service.
*:tianji:services:[sname]:serviceinstances:[siname]:template	write	Updates a service template reference.
*:tianji:services:[sname]:serviceinstances:[siname]:template	delete	Deletes a service template.
*:tianji:services:[sname]:serviceinstances:[siname]:template	read	Obtains a service template.
*:tianji:services:[sname]:serviceinstances:[siname]:tags:[tag]	delete	Deletes a service template tag.
*:tianji:services:[sname]:serviceinstances:[siname]:tags:[tag]	write	Adds a service template tag.
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:resources	read	Obtains a service resource.
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]	write	Modifies a machine.

Resource	Operation	Description
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]	read	Obtains a machine.
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]	delete	Deletes a machine.
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines	read	Obtains a machine role.
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines	delete	Batch deletes machines.
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:machines	write	Modifies a machine role.
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:resources	read	Obtains a service resource.
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:machines:[machine]:tianjilogs	read	Obtains Apsara Infrastructure Management Framework logs.
*:tianji:services:[sname]:serviceinstances:[siname]:serverroles	read	Obtains a service role.
*:tianji:services:[sname]:serviceinstances:[siname]:schema	write	Sets a service specification.
*:tianji:services:[sname]:serviceinstances:[siname]:schema	delete	Deletes a service specification.
*:tianji:services:[sname]:serviceinstances:[siname]:rollings:[version]	write	Modifies an upgrade task.

Resource	Operation	Description
*:tianji:services:[sname]:serviceinstances:[siname]:rollings	read	Lists upgrade tasks.
*:tianji:services:[sname]:serviceinstances:[siname]:resources	read	Obtains an instance resource.
*:tianji:services:[sname]:serviceinstances:[siname]:machines:[machine]	read	Obtains all the machine roles.
*:tianji:services:[sname]:serviceinstances:[siname]	write	Deploys a service instance.
*:tianji:services:[sname]:serviceinstances:[siname]	read	Obtains service configurations.
*:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:name	read	Obtains a list of machine service files.
*:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:download	read	Obtains the information about downloading a machine service file.
*:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:content	read	Obtains the content of a machine service file.
*:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:filelist	read	Obtains a list of machine files.
*:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:dockerlogs	read	Obtains container logs.
*:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:debuglog	read	Obtains machine debugging information.

Resource	Operation	Description
*:tianji:services:[sname]:serverroles:[serverrole]:machines:[machine]:apps	read	Obtains a list of machine services.
*:tianji:services:[sname]:serverroles:[serverrole]:apps:[app]:dockerinspect	read	Obtains the information about a container.
*:tianji:services:[sname]:schemas:[schemaname]	write	Modifies a service specification.
*:tianji:services:[sname]:schemas:[schemaname]	delete	Deletes a service specification.
*:tianji:services:[sname]:resources	read	Obtains a service resource.
*:tianji:services:[sname]	delete	Deletes a service.
*:tianji:services:[sname]	write	Creates a service.
*:tianji:projects:[pname]:machinebuckets:[bname]:machines:[machine]	read	Obtains machine information.
*:tianji:projects:[pname]:machinebuckets:[bname]:machines	read	Obtains a list of machines.
*:tianji:projects:[pname]:machinebuckets:[bname]	write	Creates a machine pool.
*:tianji:projects:[pname]:machinebuckets:[bname]	write	Modifies a machine pool.
*:tianji:projects:[pname]:machinebuckets:[bname]	delete	Deletes a machine pool.
*:tianji:projects:[pname]:machinebuckets:[bname]	read	Obtains a list of machines.
*:tianji:projects:[pname]:machinebuckets	read	Obtains a list of machine pools.

Resource	Operation	Description
*:tianji:projects:[pname]:projects:[pname]:clusters:[cname]:tssessions:[tssessionname]:tsses	terminal	Updates a remote connection.
*:tianji:projects:[pname]:projects:[pname]:clusters:[cname]:tssessions	terminal	Creates a remote connection.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:tjmontemplate	read	Obtains a service monitoring instance.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:template	delete	Deletes a service monitoring instance.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:template	write	Sets a service template.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:template	read	Obtains a service template.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:tags:[tag]	write	Adds a service product tag.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:tags:[tag]	delete	Deletes a service product tag.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:resources	read	Obtains a role resource.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:name	read	Obtains a list of machine service files.

Resource	Operation	Description
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:download	read	Obtains the information about downloading a machine service file.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:content	read	Obtains the content of a machine service file.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:filelist	read	Obtains a list of machine files.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:dockerlogs	read	Obtains container logs.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:debuglog	read	Obtains machine debugging information.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps	read	Obtains a list of machine files.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]	read	Obtains role information.

Resource	Operation	Description
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]	write	Modifies machine role information.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]	delete	Deletes a machine role.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines	write	Modifies machine role information.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines	delete	Batch deletes machine roles.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines	read	Obtains the information about all machine services.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:resources	read	Obtains a service resource.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:machines:[machine]:tianjilogs	read	Obtains Apsara Infrastructure Management Framework logs.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:dockerinspect	read	Obtains information about the container group.

Resource	Operation	Description
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles	read	Obtains a service instance role.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:schema	delete	Deletes a service specification.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:schema	write	Sets a service specification.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:resources	read	Obtains an instance resource.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]	delete	Deletes a service instance.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]	write	Creates a service instance.
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]	read	Obtains service instance configurations.
*:tianji:projects:[pname]:clusters:[cname]:rollings:[version]	write	Modifies an upgrade task.
*:tianji:projects:[pname]:clusters:[cname]:rollings	read	Obtains a list of upgrade tasks.
*:tianji:projects:[pname]:clusters:[cname]:resources	read	Obtains a cluster resource.
*:tianji:projects:[pname]:clusters:[cname]:quota	write	Sets a cluster quota.
*:tianji:projects:[pname]:clusters:[cname]:machinesinfo	read	Obtains machine information.

Resource	Operation	Description
*:tianji:projects:[pname]:clusters:[cname]:machines:[machine]	read	Obtains all the machine roles.
*:tianji:projects:[pname]:clusters:[cname]:machines:[machine]	write	Configures a machine operation.
*:tianji:projects:[pname]:clusters:[cname]:machines:[machine]	delete	Deletes a machine operation.
*:tianji:projects:[pname]:clusters:[cname]:machines	write	Modifies a machine cluster.
*:tianji:projects:[pname]:clusters:[cname]:difflist	read	Obtains a list of edition differences.
*:tianji:projects:[pname]:clusters:[cname]:diff	read	Obtains the content of an edition difference.
*:tianji:projects:[pname]:clusters:[cname]:deploylogs:[version]	read	Obtains the content of a cluster deployment log.
*:tianji:projects:[pname]:clusters:[cname]:deploylogs	read	Obtains a list of cluster deployment logs.
*:tianji:projects:[pname]:clusters:[cname]:builds:[version]	read	Obtains the information about a build task.
*:tianji:projects:[pname]:clusters:[cname]:builds	read	Obtains a list of build tasks.
*:tianji:projects:[pname]:clusters:[cname]	write	Modifies a cluster.
*:tianji:projects:[pname]:clusters:[cname]	delete	Deletes a cluster.
*:tianji:projects:[pname]:clusters:[cname]	read	Obtains cluster configurations.
*:tianji:projects:[pname]:clusters:[cname]	write	Deploys a cluster.
*:tianji:projects:[pname]	write	Creates a project.
*:tianji:projects:[pname]	delete	Deletes a project.

Resource	Operation	Description
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]:rackunits:[rackunit]	write	Creates a slot.
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]:rackunits:[rackunit]	write	Sets slot properties.
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]:rackunits:[rackunit]	delete	Deletes a slot.
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]	write	Sets rack properties.
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]	write	Creates a rack.
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]	delete	Deletes a rack.
*:tianji:idcs:[idc]:rooms:[room]	write	Creates a room.
*:tianji:idcs:[idc]:rooms:[room]	delete	Deletes a room.
*:tianji:idcs:[idc]:rooms:[room]	write	Sets room properties.
*:tianji:idcs:[idc]	delete	Deletes a data center.
*:tianji:idcs:[idc]	write	Sets data center properties.
*:tianji:idcs:[idc]	write	Creates a data center.

12.1.8.2.2. Permission list of Webapp-rule

This topic describes the permissions of Webapp-rule.

Resource	Action	Description
26842:webapp-rule:*	write	Adds, deletes, and updates configuration resources
26842:webapp-rule:*	read	Queries configuration resources

12.1.8.2.3. Permission list of the workflow console

This topic describes the permissions of the workflow console.

Resource	Action	Description
26842:grandcanal	read	Queries the workflow activity details and summary
26842:grandcanal	write	Restarts, retries, rolls back, and terminates a workflow

12.1.8.2.4. Permissions on Monitoring System of Apsara Infrastructure Management Framework

This topic describes the operation permissions on Monitoring System of Apsara Infrastructure Management Framework.

Resource	Action	Description
26842:tianjimon:monitor-manage	manage	Monitoring and O&M

12.1.8.2.5. Permissions on Rtools

This topic describes the operation permissions on Rtools.

Resource	Action	Description
26842:drds:rtools:tddl	all	Publishes Taobao Distributed Data Layer (TDDL) configurations in the Rtools console.
26842:drds:rtools:jade	all	Queries and modifies configurations in the Rtools console.
26842:drds:rtools:gemini	all	Performs operations on gemini in the Rtools console.
26842:drds:rtools:system	all	Performs other operations in the Rtools console.