

Alibaba Cloud Apsara Stack Enterprise

Operation Guide

Version: 1808..

Issue: 20180831

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Note: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other contents.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	It is used for commands.	Run the <code>cd /d C:/windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is a optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Preparations.....	1
1.1 Learn about O&M process.....	1
1.2 Collect O&M information.....	1
1.2.1 Product delivery list.....	1
1.2.2 O&M tool.....	1
1.2.3 Log on to common modules.....	2
2 Basic platform operation.....	3
2.1 Apsara Stack Operation.....	3
2.1.1 Apsara Stack Operation overview.....	3
2.1.2 Log on to Apsara Stack Operation.....	4
2.1.3 O&M dashboard.....	5
2.1.4 Alarm management.....	6
2.1.4.1 Overview.....	6
2.1.4.2 View alarm overview.....	6
2.1.4.3 View alarms.....	7
2.1.4.4 Configure the information of on-duty operators for alarms.....	8
2.1.5 Resource management.....	9
2.1.5.1 Overview.....	9
2.1.5.2 Physical servers.....	9
2.1.5.3 Physical networks.....	9
2.1.5.3.1 View basic information of the physical network.....	9
2.1.5.3.2 View alarm information of the physical network.....	11
2.1.5.3.3 View network topology.....	11
2.1.6 Inventory management.....	12
2.1.6.1 Overview.....	12
2.1.6.2 View the ECS inventory.....	12
2.1.6.3 View the Server Load Balancer inventory.....	19
2.1.6.4 View the RDS inventory.....	19
2.1.6.5 View the OSS inventory.....	20
2.1.7 Product O&M management.....	20
2.1.8 API management.....	21
2.1.8.1 Overview.....	21
2.1.8.2 Catalog.....	21
2.1.8.3 Product management.....	22
2.1.8.4 Version management.....	23
2.1.9 ITIL management.....	23
2.1.9.1 Overview.....	23
2.1.9.2 Dashboard.....	24

2.1.9.3 Services.....	24
2.1.9.3.1 Basic functions.....	25
2.1.9.3.1.1 Manage requests.....	25
2.1.9.3.1.2 Manage tasks.....	26
2.1.9.3.2 Manage incidents.....	27
2.1.9.3.2.1 Create an incident request.....	27
2.1.9.3.2.2 Manage incident requests.....	29
2.1.9.3.2.3 Manage incident tasks.....	30
2.1.9.3.3 Manage problems.....	31
2.1.9.3.3.1 Create a problem request.....	31
2.1.9.3.3.2 Manage problem requests.....	33
2.1.9.3.3.3 Manage problem tasks.....	34
2.1.9.4 Version control.....	35
2.1.10 Configurations.....	35
2.1.10.1 Overview.....	35
2.1.10.2 Modify a configuration item of a product.....	36
2.1.10.3 Restore the modified configuration item.....	36
2.1.11 System management.....	37
2.1.11.1 Overview.....	37
2.1.11.2 Department management.....	37
2.1.11.3 Role management.....	38
2.1.11.4 Logon policy management.....	39
2.1.11.5 User management.....	40
2.1.11.6 Two-factor authentication.....	42
2.1.11.7 Application whitelist.....	44
2.1.11.8 Operation logs.....	45
2.1.11.9 Server password management.....	46
2.1.11.10 Offline backup.....	47
2.2 Apsara Infrastructure Management Framework operation.....	51
2.2.1 Overview.....	51
2.2.1.1 What is Apsara Infrastructure Management Framework?.....	51
2.2.1.2 Basic concepts.....	51
2.2.2 Homepage overview.....	53
2.2.3 System management.....	55
2.2.3.1 Permission management.....	55
2.2.3.2 Data source management.....	55
2.2.4 Project management.....	55
2.2.5 Cluster management.....	56
2.2.5.1 Cluster dashboard.....	56
2.2.5.2 Cluster Operation and Maintenance Center.....	59
2.2.5.3 Service final status.....	62
2.2.5.4 Cluster configuration.....	62
2.2.5.5 Operation logs.....	62
2.2.6 Modify a monitoring template.....	63

2.2.7 Ticket management.....	64
2.2.7.1 Manage ticket permissions.....	64
2.2.7.2 Create a ticket.....	64
2.2.7.2.1 Manually open a ticket.....	64
2.2.7.2.1.1 Process description.....	64
2.2.7.2.1.2 Procedure.....	65
2.2.7.2.2 Apsara Infrastructure Management Framework opens a ticket after self -check.....	66
2.2.8 Server management.....	67
2.2.8.1 Add a server.....	67
2.2.8.2 Change server bucket.....	68
2.2.8.3 Delete a server.....	68
2.2.9 Task management.....	68
2.2.9.1 Query tasks.....	68
2.2.9.2 Deployment overview.....	69
2.2.9.2.1 Deployment progress.....	69
2.2.9.2.2 Deployment details.....	70
2.2.10 Alarm center.....	72
2.2.11 Report management.....	72
2.2.11.1 Info of project component report.....	72
2.2.11.2 State of project component.....	73
2.2.11.3 Machine info report.....	74
2.2.11.4 Action of machine SR.....	75
2.2.11.5 State of machine clone.....	76
2.2.11.6 Service inspector report.....	77
2.2.11.7 Resource apply report.....	77
2.2.11.8 Rolling info report.....	78
2.2.11.9 Virtual machines map.....	80
2.2.11.10 Relationship of service dependency.....	80
2.2.11.11 Registration vars of service.....	80
2.2.11.12 Check report of network topology.....	81
2.2.11.13 Machine RPM approval pending list.....	81
2.2.11.14 Auto healing/install approval pending report.....	82
2.2.11.15 Machine power on or off state of cluster.....	82
2.2.11.16 Private service Tianji monitor state profile.....	83
2.2.11.17 Thermometer.....	83
2.2.11.18 Tianjimon data of project.....	84
2.2.11.19 Operation of ACC node.....	85
2.2.11.20 Operation of source node.....	85
2.2.11.21 Docker monitor - cluster.....	86
2.2.11.22 Docker monitor - single.....	86
2.2.11.23 JVM monitor - cluster.....	87
2.2.11.24 JVM monitor - single machine.....	87
2.2.11.25 Unusual reference var of service.....	87

3 Appendix.....	89
3.1 Operation Administrator Manager (OAM).....	89
3.1.1 OAM introduction.....	89
3.1.2 Basic concepts.....	90
3.1.3 Log on to OAM.....	91
3.1.4 Quick start.....	92
3.1.4.1 Create a group.....	92
3.1.4.2 Add group members.....	92
3.1.4.3 Add group roles.....	93
3.1.4.4 Create a role.....	93
3.1.4.5 Add inherited roles to a role.....	94
3.1.4.6 Add resources to a role.....	94
3.1.4.7 Add authorized users to a role.....	95
3.1.5 Manage groups.....	96
3.1.5.1 Modify group information.....	96
3.1.5.2 View group role details.....	97
3.1.5.3 Delete a group.....	97
3.1.5.4 View assigned groups.....	98
3.1.6 Manage roles.....	98
3.1.6.1 Query roles.....	98
3.1.6.2 Modify role information.....	98
3.1.6.3 View the role inheritance tree.....	99
3.1.6.4 Transfer roles.....	99
3.1.6.5 Delete a role.....	100
3.1.6.6 View assigned roles.....	100
3.1.6.7 View all roles.....	100
3.1.7 Search resources.....	101
3.1.8 View personal information.....	101
3.1.9 Typical applications.....	101
3.1.9.1 Assign a default role to a user.....	101
3.1.9.2 Group and RoleHierarchy.....	102
3.1.9.3 Use custom roles.....	103
3.1.10 Appendix.....	104
3.1.10.1 Default roles and their functions.....	104
3.1.10.1.1 OAM default role.....	104
3.1.10.1.2 ECS Operations and Maintenance System default roles.....	104
3.1.10.1.3 RDS Operations and Maintenance System default roles.....	105
3.1.10.1.4 Storage Operations and Maintenance System default roles.....	194
3.1.10.1.5 SLB/VPC Operations and Maintenance System default roles.....	197
3.1.10.1.6 Apsara Infrastructure Management Framework default roles.....	198
3.1.10.1.7 Webapp-rule default roles.....	200
3.1.10.1.8 Workflow (grandcanal) console default roles.....	200
3.1.10.1.9 baseService-yaochi-console default roles.....	201
3.1.10.1.10 BCC default roles.....	202

3.1.10.1.11 Tlog default role.....	204
3.1.10.1.12 Butler default roles.....	204
3.1.10.1.13 Data Replication System default roles.....	205
3.1.10.1.14 Tianjimon default role.....	206
3.1.10.1.15 Rtools default role.....	206
3.1.10.1.16 MetaCenter default roles.....	207
3.1.10.1.17 Dayu default role.....	207
3.1.10.2 Operation permissions of O&M platforms.....	207
3.1.10.2.1 ECS Operations and Maintenance System permission list.....	207
3.1.10.2.2 RDS Operations and Maintenance System permission list.....	209
3.1.10.2.3 Storage Operations and Maintenance System permission list.....	232
3.1.10.2.4 SLB/VPC Operations and Maintenance System permission list.....	234
3.1.10.2.5 Apsara Infrastructure Management Framework permission list.....	235
3.1.10.2.6 Webapp-rule permission list.....	244
3.1.10.2.7 Workflow (grandcanal) console permission list.....	245
3.1.10.2.8 baseService-yaochi-console permission list.....	245
3.1.10.2.9 BCC permission list.....	245
3.1.10.2.10 Tlog permission list.....	246
3.1.10.2.11 Butler permission list.....	246
3.1.10.2.12 Data Replication System permission list.....	247
3.1.10.2.13 Tianjimon permission list.....	249
3.1.10.2.14 Rtools permission list.....	249
3.1.10.2.15 MetaCenter permission list.....	249
3.1.10.2.16 Dayu permission list.....	250
3.2 Common O&M operations.....	250
3.2.1 Log on to OPS.....	250
3.2.2 Log on to ECSAG.....	250
3.2.3 Log on to XGW.....	251
3.2.4 View Docker container status.....	251
3.2.5 View service status.....	251
3.2.6 View cluster status.....	252
3.2.7 View the status of project component.....	252
3.2.8 View Docker host status.....	252
3.2.9 View Docker host and container distribution.....	252
3.2.10 View monitoring status (formerly Alimonitor).....	253
3.2.11 View resource status (formerly CMDDB).....	253
3.2.12 View the number of physical machines for each project.....	253
3.2.13 View server SN based on IP address.....	253
3.2.14 Check whether a physical machine of a V3 Apsara Infrastructure Management Framework cluster is a control server or OPS 1-4.....	254
3.2.15 View deployment conditions.....	254

1 Preparations

1.1 Learn about O&M process

1.2 Collect O&M information

1.2.1 Product delivery list

Product	Version
Basic platform	
Apsara Infrastructure Management Framework	V3.5.0
Apsara Stack Operation	V3.5.0
Cloud product	
ECS	V3.5.0
RDS	V3.5.0
VPC	V3.5.0
...	
Big data product	
StreamCompute	V3.5.0
E-MapReduce	V3.5.0
...	

1.2.2 O&M tool

This section introduces the Apsara Stack Operation & Maintenance (O&M) tools and their functions.

O&M platform

Table 1-1: Apsara Stack O&M platform

Name	Function
Apsara Stack Inspection System	Improves the O&M efficiency.
Dashboard	Provides resource alarms in advance.
Apsara Stack Operation	The Apsara Stack O&M control system

Name	Function
Apsara Infrastructure Management Framework	The underlying system of Apsara Stack platform.
Big data manager	The O&M management platform for big data products.

Product O&M tool

Table 1-2: Product O&M tool

Product name	Tool
ECS	go2 tool
Apsara Distributed File System	puadmin tool
...	

1.2.3 Log on to common modules

This section introduces how to log on to common modules.

Table 1-3: Logon method

Module	Logon method
OPS	For more information, see Log on to OPS .
ECSAG	For more information, see Log on to ECSAG .
XGW	For more information, see Log on to XGW .

2 Basic platform operation

2.1 Apsara Stack Operation

2.1.1 Apsara Stack Operation overview

Apsara Stack Operation (ASO) is an Operation & Maintenance (O&M) management system developed for the Apsara Stack O&M personnel, such as onsite O&M engineers, O&M engineers of the customers, O&M management engineers, and O&M security or audit personnel. ASO allows the O&M engineers to master the operating conditions of the system in time and perform O&M operations.

ASO has the following main functions:

- [*O&M dashboard*](#)

The O&M dashboard displays the product version, inventory statistics, inventory usage trend, and alarm monitoring statistics of the current cloud platform, which allows you to know the current usage of resources.

- [*Alarm management*](#)

Alarm management allows O&M engineers to quickly know the alarm information generated by the system, locate the problems based on the alarm information, and track the problem processing process. Besides, they can also configure the alarm information.

- [*Resource management*](#)

Resource management monitors and manages hardware devices in the data center. You can monitor and manage the overall status information, monitoring indexes, alarm information, and port traffic information of physical servers, physical switches, and network security devices.

- [*Inventory management*](#)

Inventory management allows you to view the current usage and inventory of various product resources, and manage resources in the system effectively.

- [*Product O&M management*](#)

Product O&M management provides portals to O&M control services of other cloud platform products. You are redirected to the corresponding product O&M management page by Single Sign-On (SSO) and redirection.

- [*ITIL management*](#)

Information Technology Infrastructure Library (ITIL) manages the incidents and problems generated during the daily system O&M, which allows O&M engineers to better maintain the network stability, improve the performance indexes quickly, lower the O&M costs, and finally enhance the user satisfaction. Currently, ITIL has the following three modules: Dashboard, Services, and Version Control.

- [API management](#)

API management encapsulates the O&M APIs for all cloud products on the cloud platform, which facilitates third-parties secondary development of the O&M platform, and allows fine-grained access control and security audit of the O&M APIs. API management guarantees the centralized management in terms of versions and application interfaces, and provides various flexible and customizable functions.

- [Configurations](#)

Configuration item management allows you to modify the related configuration items of each product according to the actual O&M management requirements. To modify a configuration item of a product, you can modify the relevant configuration value in ASO to make the modification take effect. To restore the modified configuration value, you can perform a one-click reset by rolling it back.

- [System management](#)

System management includes the user management, two-factor authentication, role management, department management, logon policy management, application whitelist, server password management, offline backup, and operation logs. As the module for centralized management of accounts, roles, and permissions, system management supports the SSO function of ASO. After logging on to ASO, you can perform O&M operations on all components of the cloud platform or redirect to the O&M page without providing the username and password.

2.1.2 Log on to Apsara Stack Operation

This section introduces how to log on to Apsara Stack Operation (ASO) as O&M engineers and other users.

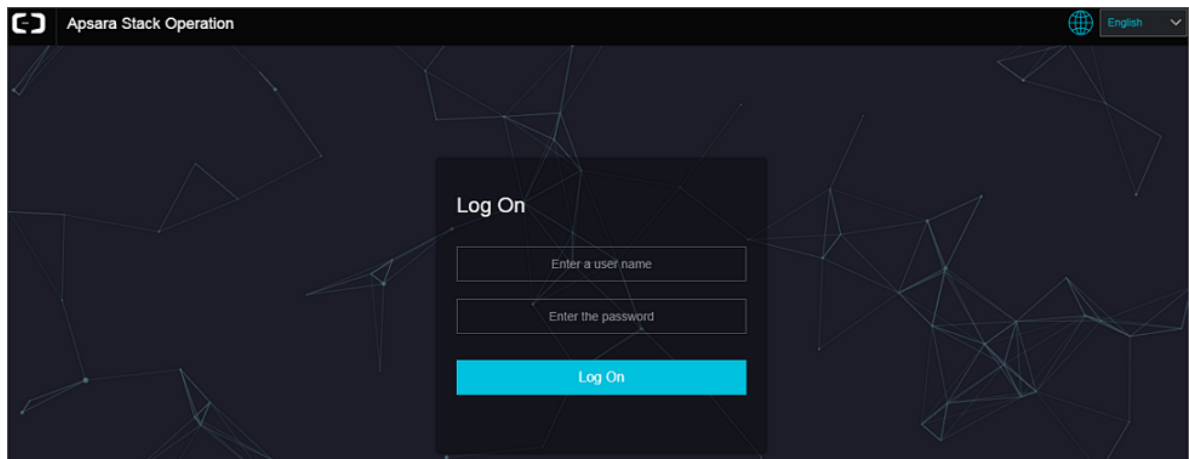
Prerequisites

- You have obtained the access address of ASO. The format of the access address is `http://region-id.aso.intranet-domain-id`.
- We recommend that you use the Chrome browser.

Procedure

1. Open the browser.
2. Enter the ASO access address `http://region-id.aso.intranet-domain-id` in the address bar and press Enter.

Figure 2-1: Log on to ASO



3. Enter the correct username and password.
 - The system has three default users:
 - The security officer manages other users or roles.
 - The auditor officer views audit logs.
 - The system administrator is used for other functions except for those of the security officer and auditor officer.
 - To improve security, the password must meet minimum complexity requirements, that is, 10-20 characters long and containing English uppercase or lowercase letters (A-Z or a-z), numbers (0-9), or special characters (such as exclamation marks (!), at signs (@), number signs (#), dollar signs (\$), and percent signs (%)).
4. Click **Log On** to go to the ASO page.

2.1.3 O&M dashboard

Apsara Stack Operation (ASO) displays the current usage and monitoring indexes of system resources in graphics, which allows you to know the current operating conditions of the system.

Log on to ASO. For more information, see [Log on to Apsara Stack Operation](#). Click **Operation and Maintenance** in the left-side navigation pane. The O&M dashboard mainly displays the product version, inventory statistics, and alarm monitoring statistics of the current cloud platform.

By viewing the dashboard, the O&M engineers can know the overall operating conditions of Apsara Stack products in time.

2.1.4 Alarm management

2.1.4.1 Overview

Alarm management allows O&M engineers to quickly know the alarm information generated by the system, locate the problems based on the alarm information, and track the problem processing process. Besides, they can also configure the alarm information.

Alarm management includes **Alarms**, **Outstanding Alarms**, **Alarm Configuration**, and **Alarm Overview**. The **Alarms** page displays all alarm events and alarm information generated by the system, and records the processing status of these alarm events. If an alarm event cannot be processed in time, it is processed and tracked in **Outstanding Alarms**. Besides, each alarm is associated with an on-duty operator and a product developer based on product names. In this way, the contact information can be immediately obtained after an alarm is triggered. The **Alarm Overview** page displays statistics and graphics of alarm events, which enables the O&M engineers to conveniently view the overall situation.

2.1.4.2 View alarm overview

By viewing the alarm overview, you can know the distribution of different levels of alarms for Apsara Stack products.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Alarm Management > Alarm Overview**.
 - The table in the upper-left corner shows the number of different levels (minor, major, and critical) of alarms and the number of cleared alarms for various products.
 - The pie chart in the upper-right corner shows the distribution ratio of all alarms at different levels.
 - The bar chart shows the statistics of alarms newly added per day in the past seven days.
 - The line chart at the bottom shows the trend of the alarms newly added per day in the past seven days.

2.1.4.3 View alarms

The **Alarms** page displays all alarm events and alarm information generated by the system.

You can search alarms by alarm level, product name, and time range, and then perform O&M operations on alarms.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Alarm Management** > **Alarms**. Click an alarm in the following list to display the on-duty operator and more detailed original alarm information in the row below the alarm.



Note:

- On this page, alarms are sorted by alarm level, time, and status to make sure that the most urgent alarms that are pending processing are listed at the top.
- The indicator flashes and the alarm sound is played when a new alarm appears on the page.

3. You can perform the following operations on this page:

- **Search an alarm**

In the search bar at the top of this page, you can search an alarm based on **Product**, **Severity**, and **Start date - End date**.

- **Export the alarm list**

Click **Export Report** in the upper-right corner. The system exports all alarms to a downloadable list. If you only want to export the alarms within a certain time range, enter the time range in **Start date - End date** and then click **Export Report**.

- **View alarm details**

Click the alarm name in blue under **Alarm Details**. In the displayed **Alarm Details** dialog box, you can view the alarm description, processing method, and other related information.

- **Process an alarm**

If an alarm is being processed by an O&M engineer, you can click **Process** under **Actions** to set the alarm status to **Processing**. After the alarm is processed, click **Finish**.



Note:

If the alarm cannot be processed in time or is unsolvable currently, you can click **Problem** under **Actions**. Then, the alarm is transferred to the **Outstanding Alarms** page for further processing and tracking.

2.1.4.4 Configure the information of on-duty operators for alarms

You can configure the information of on-duty operators for alarms. After completing the configurations, you can click an alarm on the **Alarms** page and **Outstanding Alarms** page to view the matching on-duty operator.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Alarm Management** > **Alarm Configuration**. On this page, you can search, add, modify, or delete alarm information.
3. You can perform the following operations on this page:

- **Search alarm contact information**

In the search bar in the upper-left corner, select a product name and other related information, and then click **Search** to view the alarm contact information of the product in the following list.

- **Add alarm contact information**

Click **Add** in the upper-right corner. In the displayed **Add Contact** dialog box, complete the configurations and then click **Confirm**.



Note:

After the on-duty operator information is added, you can click an alarm on the **Alarms** page and **Outstanding Alarms** page to view the matching on-duty operator. Product name and duty time are two matching conditions. For example, if you click an alarm occurred within the duty time, the matching on-duty operator is displayed.

- **Modify the alarm contact information**

At the right of the information to be modified, click **Modify** under **Actions**. In the displayed **Modify Contact** dialog box, modify the information and then click **Confirm**.

- **Delete the alarm contact information**

At the right of the information to be deleted, click **Delete** under **Actions**. Click **Confirm** to delete the entire alarm configuration.

2.1.5 Resource management

2.1.5.1 Overview

Resource management monitors and manages hardware devices in the data center. You can monitor and manage the overall status information, monitoring indexes, alarm information, and port traffic information of physical servers, physical switches, and network security devices.

2.1.5.2 Physical servers

The O&M personnel can monitor and view the physical server where a product is located.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Resource Management > Physical Servers**.

Expand the left-side navigation tree layer by layer based on regions, data centers, and cabinets till all products under a cabinet are displayed. Select a product, such as RDS. On the right side, a list of physical servers where the services in the RDS product are located is displayed.

3. At the right of a product, click **Details** under **Operation** to view the basic information, monitoring information, and alarms of the physical server.

You can switch tabs to view monitoring information and alarms, or select different time ranges to observe the monitoring values in different time ranges. The main indicators that can be monitored are CPU utilization, memory utilization, system load, host traffic, disk utilization, and disk I/O-related information.

2.1.5.3 Physical networks

On the **Physical Networks** page, you can view information about the physical devices, including basic ports, traffic, alarms, and network topologies.

2.1.5.3.1 View basic information of the physical network

On the **Physical Networks** page, you can view related information of the physical network.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Resource Management > Physical Networks**. A list of physical network devices in the current data center is displayed.

**Note:**

If multiple data centers are available on the current cloud platform, you can select to switch to another data center.

3. Click **Port Settings** under **Actions** to enable or disable to monitor a device port. If enabled, the system monitors traffic rate and other information of the port. If disabled, the system does not monitor the port.
4. Click the device name in blue under **Device ID** to go to the basic information page of the device. On this page, you can view the basic information of the device, and switch between the five tabs to view the device information of different dimensions.

- **Port Status**

The **Port Status** tab displays traffic rate status of the device which is used as an interconnected port. Click **Monitor Traffic Rate** to observe traffic rate details of the device and filter traffic rate by time range.

- **Running Status**

The **Running Status** tab displays status information of the device during running, including CPU, memory, system power consumption, power, optical module information, and fan status. You can expand each module in turn to view details.

- **Chart**

The **Chart** tab displays CPU utilization and memory utilization in running curves.

- **Common table item**

The **Common Table Item** tab displays common table items of the device, such as ARP table and route table.

- **Machine logs**

You can set **Start/End Time**, **Log Level**, and **Keyword** of the machine logs to search system logs of the device or download logs as required. Click **View** to view log details.

2.1.5.3.2 View alarm information of the physical network

On the **Physical Networks** page, you can view how many alarms are generated in the cloud platform physical network.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Resource Management > Physical Networks**.
3. Click **Alarm Generated** in the upper-right corner. A list of current alarms in the system is displayed.



Note:

The alarms are classified into followed alarms and unfollowed alarms. Set the alarm classification under the **Alarm Settings** tab.

- The followed alarms are identified by Monitoring System and sent to the O&M engineers.
- The unfollowed alarms are only stored in ASO and are not sent to the O&M engineers.

2.1.5.3.3 View network topology

On the Network Topology page, you can view the topology of the physical network.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Resource Management > Physical Networks > Network Topology**. The **Network Topology** page displays the physical network topology of a physical data center.



Note:

The colors of the connections between network devices represent the connectivity between the network devices.

- Green: Normal
- Red: Disconnected
- Grey: Not used

3. Click **View Details** in the upper-right corner to view the **Device Basic Attributes** and **Running Port Status**.
4. Click a physical network device in the network topology. The **Device Basic Attributes** and **Running Port Status** of the device are displayed on the right.

2.1.6 Inventory management

2.1.6.1 Overview

Inventory management allows you to view the current usage and inventory of various product resources, and manage resources in the system effectively.

2.1.6.2 View the ECS inventory

By viewing the ECS inventory, you can know the current usage and surplus of ECS product resources and perform O&M operations according to actual requirements.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Inventory Management > ECS Instances**.
 - **CPU Inventory Details** and **Memory Inventory Details** display the used and available CPUs (cores) and memories (GB) of all ECS instances in the last seven days.
 - **ECS Inventory Details** allows you to query (paging query) the inventory of a certain type of ECS instances at a certain date by region, instance type, and date. For mapping between ECS instances and CPU/memory configurations of ECS instances, see [Instance type](#).

Table 2-1: Instance type

Instance type family	Type category code	Local storage (GB)	CPU (core)	Memory (GB)	ENI (including a master ENI)
N4	ecs.n4.small	None.	1	2.0	1
	ecs.n4.large	None.	2	4.0	1
	ecs.n4.xlarge	None.	4	8.0	2
	ecs.n4.2xlarge	None.	8	16.0	2

Instance type family	Type category code	Local storage (GB)	CPU (core)	Memory (GB)	ENI (including a master ENI)
	ecs.n4.4xlarge	None.	16	32.0	2
	ecs.n4.8xlarge	None.	32	64.0	2
MN4	ecs.mn4.small	None.	1	4.0	1
	ecs.mn4.large	None.	2	8.0	1
	ecs.mn4.xlarge	None.	4	16.0	2
	ecs.mn4.2xlarge	None.	8	32.0	3
	ecs.mn4.4xlarge	None.	16	64.0	8
	ecs.mn4.8xlarge	None.	32	128.0	8
E4	ecs.e4.small	None.	1	8.0	1
	ecs.e4.large	None.	2	16.0	1
	ecs.e4.xlarge	None.	4	32.0	2
	ecs.e4.2xlarge	None.	8	64.0	3
	ecs.e4.4xlarge	None.	16	128.0	8
XN4	ecs.xn4.small	None.	1	1.0	1
gn5	ecs.gn5-c4g1.xlarge	440	4	30.0	2
	ecs.gn5-c8g1.2xlarge	440	8	60.0	3
	ecs.gn5-c4g1.2xlarge	880	8	60.0	3
	ecs.gn5-c8g1.4xlarge	880	16	120.0	8

Instance type family	Type category code	Local storage (GB)	CPU (core)	Memory (GB)	ENI (including a master ENI)
	ecs.gn5-c28g1.7xlarge	440	28	112.0	8
	ecs.gn5-c8g1.8xlarge	1760	32	240.0	8
	ecs.gn5-c28g1.14xlarge	880	56	224.0	8
	ecs.gn5-c8g1.14xlarge	3520	56	480.0	8
d1	ecs.d1.2xlarge	4 * 5500	8	32.0	3
	ecs.d1.4xlarge	8 * 5500	16	64.0	8
	ecs.d1.6xlarge	12 * 5500	24	96.0	8
	ecs.d1-c8d3.8xlarge	12 * 5500	32	128.0	8
	ecs.d1.8xlarge	16 * 5500	32	128.0	8
	ecs.d1-c14d3.14xlarge	12 * 5500	56	160.0	8
	ecs.d1.14xlarge	28 * 5500	56	224.0	8
gn4	ecs.gn4-c4g1.xlarge	None.	4	30.0	2
	ecs.gn4-c8g1.2xlarge	None.	8	60.0	3
	ecs.gn4.8xlarge	None.	32	48.0	8
	ecs.gn4-c4g1.2xlarge	None.	8	60.0	3
	ecs.gn4-c8g1.4xlarge	None.	16	60.0	8

Instance type family	Type category code	Local storage (GB)	CPU (core)	Memory (GB)	ENI (including a master ENI)
	ecs.gn4.14xlarge	None.	56	96.0	8
ga1	ecs.ga1.xlarge	1*87	4	10.0	2
	ecs.ga1.2xlarge	1*175	8	20.0	3
	ecs.ga1.4xlarge	1*350	16	40.0	8
	ecs.ga1.8xlarge	1*700	32	80.0	8
	ecs.ga1.14xlarge	1*1400	56	160.0	8
se1ne	ecs.se1ne.large	None.	2	16.0	1
	ecs.se1ne.xlarge	None.	4	32.0	2
	ecs.se1ne.2xlarge	None.	8	64.0	3
	ecs.se1ne.4xlarge	None.	16	128.0	8
	ecs.se1ne.8xlarge	None.	32	256.0	8
	ecs.se1ne.14xlarge	None.	56	480.0	8
sn2ne	ecs.sn2ne.large	None.	2	8.0	1
	ecs.sn2ne.xlarge	None.	4	16.0	2
	ecs.sn2ne.2xlarge	None.	8	32.0	3
	ecs.sn2ne.4xlarge	None.	16	64.0	8

Instance type family	Type category code	Local storage (GB)	CPU (core)	Memory (GB)	ENI (including a master ENI)
	ecs.sn2ne.8xlarge	None.	32	128.0	8
	ecs.sn2ne.14xlarge	None.	56	224.0	8
sn1ne	ecs.sn1ne.large	None.	2	4.0	1
	ecs.sn1ne.xlarge	None.	4	8.0	2
	ecs.sn1ne.2xlarge	None.	8	16.0	3
	ecs.sn1ne.4xlarge	None.	16	32.0	8
	ecs.sn1ne.8xlarge	None.	32	64.0	8
gn5i	ecs.gn5i-c2g1.large	None.	2	8.0	1
	ecs.gn5i-c4g1.xlarge	None.	4	16.0	2
	ecs.gn5i-c8g1.2xlarge	None.	8	32.0	2
	ecs.gn5i-c16g1.4xlarge	None.	16	64.0	2
	ecs.gn5i-c28g1.14xlarge	None.	56	224.0	2
g5	ecs.g5.large	None.	2	8.0	2
	ecs.g5.xlarge	None.	4	16.0	3
	ecs.g5.2xlarge	None.	8	32.0	4
	ecs.g5.4xlarge	None.	16	64.0	8

Instance type family	Type category code	Local storage (GB)	CPU (core)	Memory (GB)	ENI (including a master ENI)
	ecs.g5.6xlarge	None.	24	96.0	8
	ecs.g5.8xlarge	None.	32	128.0	8
	ecs.g5.16xlarge	None.	64	256.0	8
	ecs.g5.22xlarge	None.	88	352.0	15
c5	ecs.c5.large	None.	2	4.0	2
	ecs.c5.xlarge	None.	4	8.0	3
	ecs.c5.2xlarge	None.	8	16.0	4
	ecs.c5.4xlarge	None.	16	32.0	8
	ecs.c5.6xlarge	None.	24	48.0	8
	ecs.c5.8xlarge	None.	32	64.0	8
	ecs.c5.16xlarge	None.	64	128.0	8
r5	ecs.r5.large	None.	2	16.0	2
	ecs.r5.xlarge	None.	4	32.0	3
	ecs.r5.2xlarge	None.	8	64.0	4
	ecs.r5.4xlarge	None.	16	128.0	8
	ecs.r5.6xlarge	None.	24	192.0	8
	ecs.r5.8xlarge	None.	32	256.0	8
	ecs.r5.16xlarge	None.	64	512.0	8
	ecs.r5.22xlarge	None.	88	704.0	15
se1	ecs.se1.large	None.	2	16.0	2

Instance type family	Type category code	Local storage (GB)	CPU (core)	Memory (GB)	ENI (including a master ENI)
	ecs.se1.xlarge	None.	4	32.0	3
	ecs.se1.2xlarge	None.	8	64.0	4
	ecs.se1.4xlarge	None.	16	128.0	8
	ecs.se1.8xlarge	None.	32	256.0	8
	ecs.se1.14xlarge	None.	56	480.0	8
d1ne	ecs.d1ne.2xlarge	4 * 5500	8	32.0	4
	ecs.d1ne.4xlarge	8 * 5500	16	64.0	8
	ecs.d1ne.6xlarge	12 * 5500	24	96.0	8
	ecs.d1ne.8xlarge	16 * 5500	32	128.0	8
	ecs.d1ne.14xlarge	28 * 5500	56	224.0	8
f3	ecs.f3-c16f1.4xlarge	None.	16	64.0	8
	ecs.f3-c16f1.8xlarge	None.	32	128.0	8
	ecs.f3-c16f1.16xlarge	None.	64	256.0	16
ebmg5	ecs.ebmg5.24xlarge	None.	96	384.0	32
i2	ecs.i2.xlarge	1 * 894	4	32.0	3
	ecs.i2.2xlarge	1 * 1788	8	64.0	4
	ecs.i2.4xlarge	2 * 1788	16	128.0	8
	ecs.i2.8xlarge	4 * 1788	32	256.0	8

Instance type family	Type category code	Local storage (GB)	CPU (core)	Memory (GB)	ENI (including a master ENI)
	ecs.i2.16xlarge	8 * 1788	64	512.0	8
re5	ecs.re5.15xlarge	None.	60	990.0	8
	ecs.re5.30xlarge	None.	120	1980.0	15
	ecs.re5.45xlarge	None.	180	2970.0	15

2.1.6.3 View the Server Load Balancer inventory

By viewing the Server Load Balancer inventory, you can know the current usage and surplus of Server Load Balancer product resources and perform O&M operations according to actual requirements.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Inventory Management > SLB Instances**.
 - The zone in the upper-left corner displays the used and available intranet VIP inventory and Internet VIP inventory in the last seven days.
 - The zone in the upper-right corner displays the current proportions of used intranet VIP inventory/Internet VIP inventory and available intranet VIP inventory/Internet VIP inventory.
 - The zone at the bottom displays the Server Load Balancer inventory details, which allows you to query (paging query) the inventory by **Type** and **Date**.

2.1.6.4 View the RDS inventory

By viewing the RDS inventory, you can know the current usage and surplus of RDS product resources and perform O&M operations according to actual requirements.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Inventory Management > RDS Instances**.

- **RDS Inventory** displays the inventories of different types of RDS instances in the last seven days. Different colors represent different types of RDS instances.
- **RDS Inventory Details** allows you to query (paging query) RDS inventory by **Engine** and **Date**.

2.1.6.5 View the OSS inventory

By viewing the OSS inventory, you can know the current usage and surplus of OSS product resources and perform O&M operations according to actual requirements.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Inventory Management > OSS Buckets**.
 - **Inventory Availability History (G)** displays the available OSS buckets in the last seven days.
 - **Inventory Usage History (G)** displays the percentage of used OSS buckets.
 - **OSS bucket inventory details** allows you to query (paging query) the OSS inventory by **Date**.

2.1.7 Product O&M management

Product O&M management provides portals to O&M control services of other cloud platform products. You are redirected to the corresponding product O&M management page by Single Sign-On (SSO) and redirection.

Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#). In the left-side navigation pane, select **Products**.

On the **Product List** page, you can view O&M control icons of different products, depending on your permissions. For example, if you are an ECS product O&M engineer, you can only view the **ECS Operations and Maintenance System** icon. Click this icon to display the ECS O&M control portal. If you are an O&M system administrator, you can view all O&M control components of the cloud platform. The read and write permissions for product O&M control are separated and can be dynamically assigned to different roles.

2.1.8 API management

2.1.8.1 Overview

API management encapsulates the O&M APIs for all cloud products on the cloud platform, which facilitates third-parties secondary development of the O&M platform, and allows fine-grained access control and security audit of the O&M APIs. API management guarantees the centralized management in terms of versions and application interfaces, and provides various flexible and customizable functions. API management mainly consists of the following parts:

- **Catalog:** Provides a list of all APIs published for various cloud platform products.
- **Manages and dynamically adjusts the current Apsara Stack version information, product version information, and mapping between the Apsara Stack version and product version.**
- **Version management:** Compares different Apsara Stack versions to analyze the product differences, including the details of API lists, API definition, and API parameters.

2.1.8.2 Catalog

You can view all APIs published for a product by using the catalog function.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **API Management** > **Catalog**.
3. On the **Catalog** page, you can perform the following operations:

- **Query an API**

Click **Select Product** under the catalog and select a product from the drop-down list to view its APIs. Enter an API name in the search box to query information about the API. Fuzzy search is also supported.

- **Edit an API**

To edit information about an API, click **Edit** under **Actions** to display the API editing page. You can edit **Basic Information** and **Parameter Information** of the API. Then, click **Save** to submit the changes.

- **Test an API**

To test an API, click **Test** under **Actions** to display the API test page. You can enter basic **Request Parameters** and click **Send** to start testing. The results returned for the request are displayed on the right side.

- **Delete an API**

To delete an API, click **Delete** under **Actions** and click **Confirm**.

- **Upload an API**

To upload an API to the system, Click **Upload API** in the upper-right corner and select the file to be uploaded.

2.1.8.3 Product management

Product management allows you to manage and dynamically adjust the current Apsara Stack version information, product version information, and mapping between the Apsara Stack version and product version.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).

2. In the left-side navigation pane, select **API Management** > **Products**.

On the **Products** page, you can view an Apsara Stack product-based list and related operation buttons.

3. You can perform the following operations on this page:

- **Add a product**

Click **Add Product** in the upper-right corner. In the displayed dialog box, enter **Product Name** and **Product Description**, and then click **Submit**.

- **Edit product information**

Click **Edit** under **Actions**. In the displayed dialog box, enter **Product Name** and **Product Description**, and then click **Submit**.

- **Add a product version**

Click **Add Version** under **Actions**. In the displayed dialog box, enter **Version Number** and **API Version Number**, and then click **Submit**.

- **View product version**

Click **View Version** under **Actions**. In the displayed dialog box, you can view the list of all versions of the product and edit or delete the version information.

- **Delete a product**

Click **Delete** under **Actions** and then click **Confirm**.

2.1.8.4 Version management

Version management compares different Apsara Stack versions to analyze the product differences, including the details of API lists, API definition, and API parameters.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **API Management** > **Version Control**.

On the **Version Control** page, you can view a list of all Apsara Stack versions and related operation buttons.

3. You can perform the following operations on this page:

- **Add a version**

Click **Add Version** in the upper-right corner. In the displayed dialog box, enter **Apsara Stack Version**, **Version Number**, and **Version Description**, and then click **Submit**.

- **Set a product**

Select the specified Apsara Stack version in the version list and click **Set Product**. In the displayed dialog box, select items based on product output, change the version, and then click **Submit**. To modify or delete an item after submission, click **Edit** or **Delete** under **Actions**.

- **Version comparison**

Click **Compare Version** in the upper-left corner. In the displayed dialog box, complete four steps, namely, **Select Version** > **Version Difference** > **Product Difference** > **Compare API Version**, to finally obtain version, product, and API differences.

2.1.9 ITIL management

2.1.9.1 Overview

Information Technology Infrastructure Library (ITIL) manages the incidents and problems generated during the daily system O&M, which allows O&M engineers to better maintain the network stability, improve the performance indexes quickly, lower the O&M costs, and finally enhance the user satisfaction.

ITIL has the following three functions:

- **Dashboard**

Displays the summary of incidents and problems and the corresponding data in specific days.

- **Services**

Used to record, analyze, and monitor the incidents and problems generated during the O&M.

Multiple types of process transactions are supported.

- Incident management: Used to recover from exceptions and guarantee the normal production by a series of recovery operations, including analysis, processing, troubleshooting, and confirmation. Incident management provides a unified mode and standardizes the process for processing incidents. Besides, incident management supports the automatic collection or input of incident information.
- Problem management: Temporarily resolved incidents or incidents whose root cause is not clear can be transformed to problems for further analysis and thorough troubleshooting. Incidents aim to resume the production, while problems aim to be completely solved to make sure the problems do not recur. Problem management allows you to find the root cause of incidents, thoroughly troubleshoot the incidents, and reduce repeated incidents.

- **Version Control**

Used to display the version information of Apsara Stack products.

2.1.9.2 Dashboard

Displays the summary of incident requests and problem requests, including the total numbers of incident requests and problem requests, the numbers of new and closed incident requests and problem requests, and their change trend.

Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management > Dashboard**. The **Dashboard** page is displayed.

2.1.9.3 Services

Used to record, analyze, and monitor the incidents and problems generated during the O&M.

Multiple types of process transactions are supported.

You can submit the incidents and problems generated when using the system to the service request platform and receive the information about the problem processing.

2.1.9.3.1 Basic functions

Services are composed of requests and tasks. This section focuses on the basic functions of requests and tasks.

- **Requests**

Requests are composed of incident management and problem management. A request is a complete process of an incident request or problem request. For example, the process of an incident request is a complete request that may consist of **Diagnose**, **Resolve**, and **Confirm** phases.

- **Tasks**

A task is an operation in the incident request or problem request processing. For example, the reason analysis in the incident request processing can be considered as a task.


2.1.9.3.1.1 Manage requests

Requests are composed of incident management and problem management. This section describes how to create, query, and view details of requests.


Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management > Services**. Select the **Request** tab.
3. You can perform the following operations under the **Request** tab:


- **Create a request**

Click  at the right of **+ New** and then select **Incident** or **Problem**. Configure the parameters and then click **Confirm**. For more information, see [Create an incident request](#) and [Create a problem request](#).

- **Filter requests**

Click  at the right of the second drop-down list and then select **Incident** or **Problem** to filter out the incident requests or problem requests in the list.

- **Query requests**

Select **Request No.** or **Summary** from the third drop-down list, enter the corresponding information in the search box, and then click .

- **View request details**

At the right of the request, click **Detail** to view the request details. The request details page is composed of the following sections:

- **Function:** The function buttons for the request processing. For more information, see [Manage incident requests](#) and [Manage problem requests](#).
- **Request Flow:** The current process flow of this request.
- **Basic Information:** The basic information of this request, which is generally the information configured when you create the request.
- **Incident Source/Problem Source:** The source of the incident or problem, which is described in terms of product, service, physical machine, virtual machine, Docker name, and Docker IP address.
- **Track:** Each part of the request processing and their corresponding time point.
- **Detail Tabs:** The task list and comments related to this request.

2.1.9.3.1.2 Manage tasks

After a request is created, the system automatically goes to the **Diagnose** phase. In the **Diagnose** phase, the system automatically generates a task. Each task corresponds to a specific processing part.


Context

Tasks are currently divided into the following three types:

- **My Task:** Tasks waiting to be processed by you.
- **Task Pool:** A collection of tasks that are not assigned to related person in charge. You can check out the tasks in the task pool to make the tasks exclusive to you. Others cannot process the tasks that you have checked out. You can view the checked out tasks in **My Task**.
- **Processed by me:** The history tasks that have been processed by you. After you process the tasks in **My Task**, they are displayed in **Processed by me**.


Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management > Services**. Select the **My Task** tab.
3. You can perform the following operations under the **My Task** tab:
 - **Filter tasks**

Click  at the right of the first drop-down list and then select **My Task**, **Task Pool**, or

Processed by me to filter out the corresponding tasks in the list.

- **Query tasks**

Select **Task No.**, **Request No.**, or **Summary** from the second drop-down list, enter the corresponding information in the search box, and then click .

- **View task details**

At the right of the task, click **Detail** to view the task details. On the task details page, you can view the request details related to the task. For more information, see View request details in [Manage requests](#).

2.1.9.3.2 Manage incidents

An incident is a system runtime exception that affects the normal production. Incident management is used to recover from exceptions and guarantee the normal production by a series of recovery operations, including analysis, diagnosis, troubleshooting, recovery, and confirmation.

ITIL management uses a set of standardized processes for processing incidents to guide and help you to standardize the emergency response of incidents.

2.1.9.3.2.1 Create an incident request

If the system has an exception, you can create an incident request to track the incident processing.

Context

Currently, ITIL management supports creating incident requests in the following two ways:


- **Automatically created**

The incident information comes from the alarm information in Apsara Stack Operation (ASO). The alarm module transfers the actual conditions, such as alarm level and alarm filter, to ITIL module to generate the incident request.

- **Manually created**

You can manually create incident requests, which is supplementary to the automatic way. For example, you can manually create an incident request if the incident is not automatically recognized. This section describes how to manually create an incident request.

Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management** > **Services**. Select the **Request** tab.
3. Click  at the right of **+ New** and then select **Incident**. Configure the parameters on the displayed page.

For more information about the parameters, see [Parameter descriptions](#).

Table 2-2: Parameter descriptions

Parameter	Description
Report Object	The person who needs to process the request.
Callback Email	The email of the person who records the request.
Callback Telephone	The telephone number of the person who records the request.
Product	The product to which the request belongs. Select a specific product from the drop-down list.
Service Name	The service related to the selected product. Select a specific service from the drop-down list.
Happen Date	The time when the request happens.
Priority	<p>The priority for processing this request. The priority indicates the urgency of the request. The higher the urgency is, the higher priority the request must have. The priority has the following four levels, from high to low, based on the urgency:</p> <ul style="list-style-type: none"> • Critical • Major • Minor • Inquiry
Alarm Code	The alarm ID.
Summary	The summary of this request.
Description	The detailed description about the request.
Suggestion	(Optional) The suggestion about the request processing.

4. After configuring the preceding parameters, click **Confirm**.


2.1.9.3.2 Manage incident requests

After creating an incident request, you can change the priority for, comment, suspend, and resume the created incident request.

Prerequisites

For how to create an incident request, see [Create an incident request](#).

Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management** > **Services**. Select the **Request** tab.
3. Click  at the right of the second drop-down list and then select **Incident** to filter out the incident requests in the list.
4. At the right of the request, click **Detail** to view the request details.
5. You can perform the following operations on the request details page.

- **Change Priority**

Click **Change Priority**. In the displayed dialog box, select the new priority. Perform this operation for temporary adjustment or correcting the error in priority.



Note:

You can only change the priority for incident requests that are in the **Diagnose** phase.

- **Comment**

Click **Comment**. In the displayed dialog box, enter the comments for this incident request. Perform this operation for collaborative scenarios. For example, users can comment the incident request to share the information between each other and guide each other when they process the same incident.

- **Suspend**

Click **Suspend**. In the displayed dialog box, enter the remarks. Perform this operation for incident requests that do not need to be processed.

- **Resume**

Click **Resume**. In the displayed dialog box, enter the remarks. Perform this operation for suspended incident requests that need to be processed.

2.1.9.3.2.3 Manage incident tasks

A created incident request is divided into different tasks based on the incident process flow.


Different tasks are to be processed by different people in charge.

Context

The processing of an incident task is divided into the following three steps:

- **Diagnose:** After an incident request is created, the system automatically goes to the **Diagnose** phase and analyzes the reason of the incident.
- **Resolve:** The system goes to the **Resolve** phase after the **Diagnose** phase. The incident is repaired in this phase.
- **Confirm:** The system goes to the **Confirm** phase after the **Resolve** phase and reviews if the incident processing is reasonable. If **Temporary Solution** is selected in the **Diagnose** phase, or an incident requires further analysis, you can create a problem request in this phase to track the problem processing.

Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management > Services**. Select the **My Task** tab.
3. Click  at the right of the first drop-down list and then select **My Task**.



Note:

To check out the tasks in the task pool, select **Task Pool** and then click **Detail** at the right of the task. Click **Check Out**. In the displayed dialog box, enter the description and then click **OK**.

4. At the right of the task, click **Detail** to view the task details.
5. Click **Diagnose**. In the displayed dialog box, complete the configurations and then click **OK**.
 - **Diagnose Step:** Analyzes the task steps.
 - **Solution Type:** Select **Permanent Solution** or **Temporary Solution**. If you select **Temporary Solution**, you may have to create a problem request in the **Confirm** phase for further troubleshooting and locating the root cause of the problem.
 - **Is Complete:** Select **Yes** or **No** to indicate whether or not the task processing is completed. Sometimes the incident has been processed after being reported because of the time difference. In this case, you can directly select **Yes** and configure the resolved time. Then, the **Resolve** phase is skipped and the system goes to the **Confirm** phase directly.

- **Remarks:** Enter the information about the task.
6. The system goes to the **Resolve** phase after the **Diagnose** phase. The **Resolve** phase includes the incident troubleshooting and solving. ITIL only tracks this step in a standardized way and processes the log records. After processing the incident offline, click **Resolve** on the page. In the displayed dialog box, configure the resolved time and handling steps. Then, click **OK**.
 7. The system goes to the **Confirm** phase after the **Resolve** phase. This phase reviews the processing result of the incident. Then, click **Confirm**. In the displayed dialog box, select the review result from the **Is Pass** drop-down list. Then, click **OK**.

The review results have the following three statuses:

- **Solved:** The incident is completely solved.
- **Unsolved, re-analysis:** The incident cannot be solved effectively because of an error in the reason analysis. The task is sent back to the **Diagnose** phase to restart the processing until the incident is solved.
- **Unsolved, reprocessing:** The reason of the incident is clear. The incident cannot be solved effectively because the incident is not effectively processed. The task is sent back to the **Resolve** phase to restart the processing until the incident is solved.

2.1.9.3.3 Manage problems

Temporarily resolved incidents or incidents whose root cause is not clear can be transformed to problems for further analysis and thorough troubleshooting. Problem management allows you to find the root cause of incidents, thoroughly troubleshoot the incidents, and reduce repeated incidents.


Compared to the incident processing, problems have lower timeliness. The occurrence of repeated incidents is used to determine whether the problem management is good or not. The lower the occurrence is, the more effective the problem processing is.

ITIL management uses a set of standardized processes for processing problems to guide and help you to standardize the problem tracking and processing.

2.1.9.3.3.1 Create a problem request

If the system has an exception that requires further troubleshooting, you can create a problem request to track the problem processing.

Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management** > **Services**. Select the **Request** tab.
3. Click  at the right of **+ New** and then select **Problem**. Configure the parameters on the displayed page.

For more information about the parameters, see [Parameter descriptions](#).

Table 2-3: Parameter descriptions

Parameter	Description
Report Object	The person who needs to process the request.
Callback Email	The email of the person who records the request.
Callback Telephone	The telephone number of the person who records the request.
Product	The product to which the request belongs. Select a specific product from the drop-down list.
Service Name	The service related to the selected product. Select a specific service from the drop-down list.
Happen Date	The time when the request happens.
Priority	<p>The priority for processing this request. The priority indicates the urgency of the request. The higher the urgency is, the higher priority the request must have. The priority has the following four levels, from high to low, based on the urgency:</p> <ul style="list-style-type: none"> • Critical • Major • Minor • Inquiry
Alarm Code	The alarm ID.
Summary	The summary of this request.
Description	The detailed description about the request.
Suggestion	(Optional) The suggestion about the request processing.

4. After configuring the preceding parameters, click **Confirm**.


2.1.9.3.3.2 Manage problem requests

After creating a problem request, you can change the priority for, comment, suspend, and resume the created problem request.

Prerequisites

For how to create a problem request, see [Create a problem request](#).

Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management > Services**. Select the **Request** tab.
3. Click  at the right of the second drop-down list and then select **Problem** to filter out the problem requests in the list.
4. At the right of the request, click **Detail** to view the request details.
5. You can perform the following operations on the request details page.

- **Change Priority**

Click **Change Priority**. In the displayed dialog box, select the new priority. Perform this operation for temporary adjustment or correcting the error in priority.



Note:

You can only change the priority for problem requests that are in the **Diagnose** phase.

- **Comment**

Click **Comment**. In the displayed dialog box, enter the comments for this problem request. Perform this operation for collaborative scenarios. For example, users can comment the problem request to share the information between each other and guide each other when they process the same problem.

- **Suspend**

Click **Suspend**. In the displayed dialog box, enter the remarks. Perform this operation for problem requests that do not need to be processed.

- **Resume**

Click **Resume**. In the displayed dialog box, enter the remarks. Perform this operation for suspended problem requests that need to be processed.

2.1.9.3.3 Manage problem tasks


A created problem request is divided into different tasks based on the problem process flow.

Context

The processing of a problem task is divided into the following three steps:

- **Diagnose:** Analyzes the reason of the problem.
- **Resolve:** The system goes to the **Resolve** phase after the **Diagnose** phase. The problem is repaired in this phase.
- **Confirm:** The system goes to the **Confirm** phase after the **Resolve** phase and reviews if the problem processing is reasonable.

Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management > Services**. Select the **My Task** tab.
3. Click  at the right of the first drop-down list and then select **My Task**.



Note:

To check out the tasks in the task pool, select **Task Pool** and then click **Detail** at the right of the task. Click **Check Out**. In the displayed dialog box, enter the description and then click **OK**.

4. At the right of the task, click **Detail** to view the task details.
5. Click **Diagnose**. In the displayed dialog box, complete the configurations and then click **OK**.
 - **Diagnose Step:** Analyzes the task steps.
 - **Solution Type:** Select **Permanent Solution** or **Temporary Solution**. If you select **Temporary Solution**, you may have to create a problem request in the **Confirm** phase for further troubleshooting and locating the root cause of the problem.
 - **Is Complete:** Select **Yes** or **No** to indicate whether or not the task processing is completed. Sometimes the problem has been processed after being reported because of the time difference. In this case, you can directly select **Yes** and configure the resolved time. Then, the **Resolve** phase is skipped and the system goes to the **Confirm** phase directly.
 - **Remarks:** Enter the information about the task.
6. The system goes to the **Resolve** phase after the **Diagnose** phase. The **Resolve** phase includes the problem troubleshooting and solving. ITIL only tracks this step in a standardized

way and processes the log records. After processing the problem offline, click **Resolve** on the page. In the displayed dialog box, configure the resolved time and handling steps. Then, click **OK**.

7. The system goes to the **Confirm** phase after the **Resolve** phase. This phase reviews the processing result of the problem. Then, click **Confirm**. In the displayed dialog box, select the review result from the **Is Pass** drop-down list. Then, click **OK**.

The review results have the following three statuses:

- **Solved**: The problem is completely solved.
- **Unsolved, re-analysis**: The problem cannot be solved effectively because of an error in the reason analysis. The task is sent back to the **Diagnose** phase to restart the processing until the problem is solved.
- **Unsolved, reprocessing**: The reason of the problem is clear. The problem cannot be solved effectively because the problem is not effectively processed. The task is sent back to the **Resolve** phase to restart the processing until the problem is solved.

2.1.9.4 Version control

Version control allows you to view the version information and history versions of Apsara Stack products.


Procedure

1. [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **ITIL Management > Version Control**.

Select the product in the tree or enter the product name in the search box. The version and cluster information is displayed on the right.



Note:

Before the query, click  to synchronize the information to Apsara Stack Operation (ASO).

2.1.10 Configurations

2.1.10.1 Overview

Configuration item management allows you to modify the related configuration items of each product according to the actual O&M management requirements. To modify a configuration item of a product, you can modify the relevant configuration value in ASO to make the modification take

effect. To restore the modified configuration value, you can perform a one-click reset by rolling it back.

2.1.10.2 Modify a configuration item of a product

You can modify a configuration item of a product according to the actual O&M requirements.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Configurations > Configuration Items**.
3. Enter the name of the product or configuration item to be modified in the **Product** or **Configuration Name** field. Click **Search** to check if the configuration item already exists in the configuration list.
 - **If the configuration item already exists in the configuration list,**
 1. (Optional) Click **Obtain** under **Actions** to load the data from the product end to the local host.
 2. Click **Modify** under **Actions**. In the displayed dialog box, enter a new parameter value.
 - **If the configuration item does not exist in the configuration list,**

You must add a configuration item. Click **Add** in the upper-right corner. In the displayed dialog box, enter **Product**, **KEY**, **Configuration Code**, **Configuration Name**, **Default Value**, **Data Source**, and other related information about the configuration item. Then, the configuration item appears in the configuration list. You can search or modify the configuration item.
4. After the configuration item is modified, click **Apply** under **Actions** to make the modifications take effect.

2.1.10.3 Restore the modified configuration item

To restore the modified configuration value, you can perform a one-click reset by rolling it back.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **Configurations > Restore**.

3. On the **Restore** page, enter the name of the configuration item to be rolled back in the **Configuration Name** field and then click **Search**. All modification history records of the configuration item appear in the following list.
4. At the right of the record to be rolled back, click **Roll Back** under **Actions**. Click **Confirm** to restore the configuration item value.

2.1.11 System management

2.1.11.1 Overview

System management centrally manages the departments, roles, and users involved in Apsara Stack Operation (ASO), making it easy to grant different resource access permissions to different users. As the core module for centralized permission management, the user center integrates the functions, including department management, role management, policy management, user management, and password management.

2.1.11.2 Department management

Department management allows you to create, modify, delete, and search departments.

Context

After Apsara Stack Operation (ASO) is deployed, a root department is generated by default. You can create other departments under the root department. The departments are displayed in hierarchy and you can create sub-departments under each department level.

Departments added under the root department are level-1 departments, departments added under the level-1 departments are level-2 departments, and so on. In ASO, the sub-departments of a department refer to departments of all levels under the department. Departments reflect the tree structure of an enterprise or business unit. A user can only belong to one department.

Procedure

1. Log on to ASO. For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **System Management > Departments**.

On the **Department Management** page, you can view the tree structure of all departments that have been created, and the user information under each department.

3. You can perform the following operations on this page:
 - **Add a department**

Click **Add Department** in the upper-left corner. In the displayed dialog box, enter **Department Name** and click **Confirm**. Then, you can find the created department under the catalog you selected.

- **Modify a department**

Select a department in the catalog tree and click **Modify Department** at the top of the page. In the displayed dialog box, enter **Department Name** and click **Confirm**.

- **Delete a department**

Select a department in the catalog tree and click **Delete Department** at the top of the page. Click **Confirm**.

2.1.11.3 Role management

You can add custom roles on Apsara Stack Operation (ASO) to facilitate the allocation of permissions to users.

Context

A role is a collection of access permissions. When creating users, you must assign roles to users to meet their access control requirements on the system. Roles are classified into basic roles and user-created roles. The basic roles, also known as atomic roles, are preset by the OAM system and cannot be modified or deleted by users. The user-created roles can be modified, updated, and deleted.

Procedure

1. Log on to ASO. For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **System Management > Roles**.
3. On the **Roles** page, you can perform the following operations:

- **Search roles**



Note:

Both the ASO security officer and the system administrator can search roles.

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

- **Add a role**



Note:

In ASO, only the ASO security officer can create roles.

Click **Add Role** at the top of the page. In the displayed dialog box, enter **Role Name**, **Role Description**, and **Base Role**, and then click **Confirm**.

- **Modify a role**



Note:

In ASO, only the ASO security officer can modify roles.

At the right of the role, click **Modify** under **Actions**. In the displayed dialog box, enter new role information and then click **Confirm**.

- **Delete a role**

At the right of the role, click **Delete** under **Actions** and then click **Confirm**.

2.1.11.4 Logon policy management

The administrator can set logon polices to control users logon and read/write permissions.

Context

During system initialization, the system has a default policy for the read/write permissions of users . After you set logon policies, the read/write permissions of users can be better guaranteed, which improves system security.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **System Management > Logon Policies**.
3. On the **Logon Policy Management** page, you can perform the following operations:

- **Search policies**

In the upper-left corner, enter a policy name in the **Policy Name** field and then click **Search** to view the policy information in the list.

- **Add a policy**

Click **Add policy**. In the displayed dialog box, set **Policy Name**, **Start Time**, **End Time**, and allowed logon address. Click **Confirm**.

- **Modify a policy**

At the right of the policy, click **Modify** under **Actions**. In the displayed dialog box, modify the policy information and click **Confirm**.

- **Delete a policy**

At the right of the policy, click **Delete** under **Actions**. Click **Confirm** to delete the policy.

2.1.11.5 User management

The administrator can create a user and assign roles to users to meet their access control requirements on the system.

Prerequisites

Before creating a user, make sure that:

- You have created a department. For more information, see [Department management](#).
- You have created a custom role if required. For more information, see [Role management](#).

Context

Role management provides different operation permissions for different users. During the system initialization, the system creates three default users: asosysadmin, asosecurity, and asoauditor. The default users respectively correspond to three default roles: system administrator, security officer, and security auditor. The three roles have the same default password: AliOS%1688. See permissions of these three roles as follows:

- The system administrator can view, modify, delete, and update the O&M dashboard, alarm management, physical management, inventory management, backup service, configuration management, help center, and app whitelist, and can view user management, role management, department management, logon policy management, and physical machine password management in system management.
- The security officer can view, modify, delete, and update the user management, role management, department management, logon policy management, and physical machine password management in system management.
- The security auditor can read and write Apsara Stack Operation (ASO) system logs.

Procedure

1. Log on to ASO. For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **System Management** > **Users**. Click the **Users** tab.

The **Users** tab allows you to view a list of all created users. In the list, you can query, add, modify, and delete users and bind logon policies.

- **Search users**

**Note:**

In ASO, only the system administrator and security officer can search the user list.

In the upper-left corner, set **User Name**, **Role**, and **Department**, and then click **Search** to view user information in the list.

- **Add a user**

**Note:**

In ASO, only the security officer can add users.

At the top of the page, click **Add**. In the displayed dialog box, set **User Name**, **Password**, and other information, and then click **Confirm** to add the user.

- **Modify a user**

**Note:**

In ASO, only the security officer can modify user information.

At the right of the user, click **Modify** under **Actions**. In the displayed dialog box, enter new user information and then click **Confirm** for the new settings to take effect.

- **Delete a user**

At the right of the user, click **Delete** under **Actions** and then click **Confirm**.

**Note:**

Deleted users are in the recycle bin. To restore a deleted user, click the **Recycled** tab. At the right of the user, click **Restore** under **Actions** and then click **Confirm**.

- **Bind logon policies**

Select a user in the user list. Click **Bind Logon Policy** to bind logon policies for the user.

- **Query the personal information of the current user**

In the upper-right corner, select **Personal Information** from the drop-down list. The personal information of the current user is displayed in the appeared dialog box.

2.1.11.6 Two-factor authentication

To improve the security for user login, you can configure the two-factor authentication for users.

Context

Currently, Apsara Stack Operation (ASO) supports three authentication methods. Select one method to configure the authentication:

- **Google Two-Factor Authentication**

Uses password and mobile phone to provide double protection for accounts. You can obtain the login key after configuring users in ASO, and then enter the key in Google authentication app of your mobile phone. The app dynamically generates a verification code based on the time and key for you to log on to ASO.

- **USB Key Authentication**

Install the drive and browser control (currently, only Windows + IE 11 environment is supported) according to the third-party manufacturer instructions if you use this method. The third-party manufacturer provides the hardware USB key and the service that the backend authenticates and verifies the certificates. The hardware USB key includes the serial number and certificate information. Before the authentication, bind the serial number with user account and configure the authentication server provided by the third-party manufacturer, and then enable the USB key authentication for the user when you configure the authentication method in ASO.

Upon login, if the cloud account enables USB key authentication, ASO frontend calls the browser control, reads the certificate in USB key, obtains the random code from the backend , encrypts the information, and sends the information to the backend. The backend calls the authentication server to parse the encrypted strings, verifies the certificate and serial number, and then completes the other login processes if the verification is passed.

- **PKI Authentication**


Enable the ASO HTTPS mutual authentication and change the certificate provided by the user if you select this method. The third-party manufacturer generates the certificate and provides the service that the backend verifies the certificate. After the mutual HTTPS authentication is enabled, the request carries the client certificate upon login to send the certificate to the backend, and the backend calls the parsing and verification service of the third-party manufacturer to verify the certificate. The certificate includes the user's name and ID number . Therefore, bind the name and ID number with the user account when you configure the authentication method in ASO.

Authentication server

Both USB key authentication and PKI authentication depend on the authentication server provided by the third-party manufacturer to verify the encrypted information or certificate provided upon login. Therefore, add the authentication server configurations if you select these two authentication methods.

Google two-factor authentication is an implementation based on public algorithms. Therefore, no third-party authentication service is required and you are not required to configure the authentication server.

Procedure

1. Log on to ASO. For more information, see [Log on to Apsara Stack Operation](#).
 2. In the left-side navigation pane, select **System Management > Two Factor Authentication**.
 3. On the **Two Factor Authentication** page, you can perform the following operations:
 - **Google Two-Factor Authentication**
 1. Select **Google Two-Factor Authentication** as the **Current Authentication Method**.
 2. Click **Add User** in the upper-right corner. The added user is displayed in the user list.
 3. At the right of the user, click **Create Key**. After the key is successfully created, **No Key** is changed to **Show Key**. Click **Show Key**, the created key is displayed in plain text.
 4. Enter the key in the Google authentication app of your mobile phone. The app dynamically generates a verification code based on the time and key for you to log on to ASO. With two-factor authentication enabled, you are required to enter the verification code on your app when logging on to the system.
- 

Note:

Both Google two-factor authentication app and server generate the verification code based on the public algorithms of time and keys, and can work offline without connecting to the Internet or Google server. Therefore, keep your key confidential.
5. To disable the two-factor authentication, click **Delete Key** under **Actions**. After the successful deletion, **Show Key** is changed to **No Key**.
- **USB Key Authentication**
 1. Select **USB Key Authentication** as the **Current Authentication Method**.
 2. In **Authentication Server Configuration**, click **Add Server**. In the displayed dialog box, enter the IP address and port of the server, and then click **Confirm**. The added server is

displayed in **Authentication Server Configuration**. Click **Test** to test the connectivity of the authentication server.

3. In **User List**, click **Add User**. The added user is displayed in the user list.

4. At the right of the user, click **Bind Serial Number**. In the displayed dialog box, enter the serial number to bind the user account with this serial number.

5. Then, click **Enable Authentication** under **Actions**.

- **PKI Authentication**

1. Select **PKI Authentication** as the **Current Authentication Method**.

2. In **Authentication Server Configuration**, click **Add Server**. In the displayed dialog box, enter the IP address and port of the server, and then click **Confirm**. The added server is displayed in **Authentication Server Configuration**. Click **Test** to test the connectivity of the authentication server.

3. In **User List**, click **Add User**. The added user is displayed in the user list.

4. At the right of the user, click **Bind**. Enter the full name and ID number of the user to bind the user account with the name and ID number.

5. Then, click **Enable Authentication** under **Actions**.

- **No Authentication**

Select **No Authentication** as the **Current Authentication Method**. Then, the two-factor authentication is disabled. All the two-factor authentication methods become invalid.

2.1.11.7 Application whitelist

You can perform operations on the application whitelist.

Context

All the Apsara Stack Operation (ASO) services are accessed based on OAM permission management. Therefore, if your account does not have the corresponding role, your access requests are rejected. The application whitelist function allows you to access ASO in scenarios where no permissions are assigned. With the whitelist function enabled, the application can be accessed by all users who have successfully logged on. The application whitelist permissions include read-only and read-write. The configured value is the logon user permission.

The application whitelist is managed by a super administrator or system administrator. You can access this page after logging on as a super administrator.

When adding a whitelist, enter the product name and service name. The current product name is `aso`, and the service name is the name of the backend service registered in ASO. The whitelist takes effect only if the configurations are correct.

Procedure

1. Log on to ASO. For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **System Management > Application Whitelist**.
3. On the **Application Whitelist** page, you can perform the following operations:

- **Add a whitelist**

In the upper-right corner, click **Add to Whitelist**. In the displayed dialog box, enter the whitelist information, and then click **Confirm**.

- **Modify permissions**

Select the product permissions from the **Permissions** drop-down list.

- **Delete a whitelist**

At the right of the record, click **Delete** under **Actions** and then click **Confirm**.

2.1.11.8 Operation logs

You can view logs to learn about the usage of all resources and the operating conditions of all function modules on the platform in real time.

Context

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

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **System Management > Operation Logs**.
3. On the **Log Management** page, you can perform the following operations:

- **Search logs**

In the upper-left corner, set **User Name** and **Time Period**, and then click **Search** to view log information in the list.

- **Delete a log**

Select a log. Click **Delete logs** and then click **Confirm** to delete the log.

- **Export a log**

Select a log, and then click **Export**.

2.1.11.9 Server password management

You can configure and manage passwords of physical machines and search historical passwords.

Context

Server password management allows you to manage the passwords of all physical machines in the Apsara Stack environment.

- The system automatically collects the information of all physical machines in the Apsara Stack environment.
- The password of a physical machine is automatically updated periodically.
- You can set the password update period and password length.
- You can manually change the password of one or more physical machines at a time.
- The system records the history of password updates.
- You can search the passwords of physical machines by product, hostname, or IP address.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **System Management** > **Server Password**.
3. You can perform the following operations:
 - **Password Management**
 1. Click the **Password Management** tab. This tab displays the password information of all physical machines in the Apsara Stack environment.
 2. After clicking **Search** under **Password**, the system displays the host password in plain text, which turns into cipher text after 10 seconds. Alternatively, directly click **Hide** to display cipher text.
 3. Click **Update Password** under **Actions**. In the displayed dialog box, set **Password** and **Confirm Password**, and then click **Confirm**. The password of the physical machine is updated.

4. Select one or more physical machines and then click **Batch Update**. Set **Password** and **Confirm Password**, and then click **Confirm** to update the passwords of the selected physical machines.
5. Click **Configuration**. In the displayed dialog box, set the password update period and unit. Click **Confirm**. Physical machines update their passwords immediately and will update the passwords again after an update period.

- **History Password**

The **History Password** tab shows the history of password updates for each physical machine. You can search the historical passwords of physical machines by product, hostname, or IP address.

- **Configuration**

The **Configuration** tab displays the metadata of server password management, including the initial password, password length, and retry times.

- The initial password is the one when server password management is deployed in the Apsara Stack environment. This parameter is important, which is used to change the password of the physical machine in the Apsara Stack environment.
- The password length is the length of passwords updated automatically in the system.
- Retry times is the number of retries when the password fails to be updated.

To modify configurations, click **Modify Configurations** under **Actions**. In the displayed dialog box, set **Initial Password**, **Password Length**, and **Retry Times**, and then click **Confirm**.

2.1.11.10 Offline backup

You can view backup information by using offline backup.

Context

Offline backup is used to back up the key metadata of Apsara Stack. Currently, only pangu metadata backup is supported. Other products such as nwa and opsdns will be supported in the near future. Metadata backup is used for fast restore of Apsara Stack faults. Offline backup services include:

- Backup service: Provides backup configuration, backup details, service status, and one-click backup.
- Service configuration: Provides backup service configuration and product management.

- **Service status:** Searches the current status of backup services, including backup products, completed backups, timeout backups, and failed backups, and displays the status of backup servers in a chart.

Procedure

1. Log on to Apsara Stack Operation (ASO). For more information, see [Log on to Apsara Stack Operation](#).
2. In the left-side navigation pane, select **System Management** > **Offline backup**.
3. You can perform the following operations:
 - **Backup Service**

Table 2-4: Description of backup service

Function menu	Description
Backup Configuration	<p>The left part of the Backup Configuration page is a tree. The tree displays backup configurations in a hierarchical structure. The root node is a product list, and displays backup products provided by the current backup system. Currently, only pangu metadata backup is supported. Below the product list are backup items, which are the minimum units of backup. You can back up the metadata of different pangus, such as ecs pangu, rds pangu, and ots pangu based on Apsara Stack. The preceding configurations are added in product management.</p> <p>The right part of the Backup Configuration page shows configuration details, including Product, Backup Items, Backup Script, Product Cluster Location, Backup File Folder, Script Execution Folder, Script Parameters, Backup Schedule, Backup Schedule Unit, and Time-out.</p> <p>In the upper-right corner of the page, click Modify to modify configurations.</p>
Backup Details	Displays the current backup status. The backup details include Product , Backup

Function menu	Description
	Items , File Name (files that need to be backed up), Start Time , and State (not started, in transmission, timeout, and error). You can configure the search conditions and then click Search to obtain backup details.
Service Status	Displays the status of the current backup server and provides usage charts for internal and external disks and CPUs.
One-click Backup	Provides the one-click backup function. Click One-click Backup . The backup system starts executing all backup items in serial and displays the current backup status.

- **Service Configuration**

Table 2-5: Description of service configuration

Function menu	Description
Backup Service Configuration	<p>Provides backup server configurations.</p> <ul style="list-style-type: none"> • Backup server IP address: Configure the IP address of the backup server. The server must be an independent physical server managed by Apsara Infrastructure Management Framework and communicate with other servers in Apsara Stack. Pangu cannot be deployed on the server, at least cannot be deployed on its disk that stores backup metadata. • Backup server monitoring path: The backup server detects new backup files by monitoring the specified folder on the backup server and determines whether the backup is successful or not by comparing the MD5 values of the backup file and the original file. The monitoring path is the file storage path on the backup server.

Function menu	Description
	<ul style="list-style-type: none"> Backup retention: The file storage time on the backup server. The backup file that exceeds the time will be deleted. <p>Click Modify under Actions to modify configurations.</p>
Product Management	<p>Provides basic management of backup products, including:</p> <ol style="list-style-type: none"> Click Add in the upper-right corner. In the displayed dialog box, set Product, Backup Items, Backup Script, and Retry Times. Click OK. The added product is displayed in Backup Configuration of Backup Service. The current backup status is displayed in a table. The Actions bar on the right provides Modify and Delete. Modifying a product is similar to adding a product. Click Delete to delete a backup item. <p>You can configure the search conditions and then click Search to obtain backup details.</p>

- Service Status**

Displays the current backup status. The status at the top of the table includes **In process**, **Complete**, **Time-out**, and **Failed**. The following table lists the status of the latest backup items. The single record indicates the current product, the number of backups and failures, and the status of the latest backup items. The backup status includes success, not started, in transmission, timeout, and failure.

The backup server status graphically displays the status of memory, disk, and CPU of the backup server.

2.2 Apsara Infrastructure Management Framework operation

2.2.1 Overview

2.2.1.1 What is Apsara Infrastructure Management Framework?

Apsara Infrastructure Management Framework is an automatic data center management system that manages the hardware lifecycles and various static resources, including programs, configurations, operating system images, and data of the data center.

Apsara Infrastructure Management Framework provides a set of universal version management, deployment, and hot upgrade solutions for the applications and services of various Apsara and Alibaba Cloud products. It implements automatic operation and maintenance on Apsara Infrastructure Management Framework-based services in a large-scale distributed environment, greatly improving the operation and maintenance efficiency and system availability.

Core features

- 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 repairing of software and hardware faults
- Basic monitoring and business monitoring of software and hardware

2.2.1.2 Basic concepts

Project

A project corresponds to a product.

In Apsara Infrastructure Management Framework, a project is a collection of clusters that provide service capabilities for external entities.

Cluster

A cluster is a collection of physical machines that logically provide services and used to deploy product softwares.

- A cluster can only belong to one product.
- Multiple services can be deployed in a cluster.

Service

In Apsara Infrastructure Management Framework system, a service is a software that provides specific functions. Generally, a cloud product is a service.

The service name is globally unique. We recommend that you use lowercase letters as the service name, with the business unit (BU) name as a prefix. For example, aliyunoss.

Each service corresponds to one service package, which is a standard tar.gz file. The directory structure of a service package must comply with the Apsara Infrastructure Management Framework service package specifications.

A service is composed of one or more server roles.

A service can be deployed on a group of hardware servers, that is, a cluster, to provide the service capabilities. For example, Apsara Distributed File System, Job Scheduler, and Apsara Name Service and Distributed Lock Synchronization System are all services.

Server role

A service can be divided by function into one or more server roles. A server role is an indivisible deployment unit and indicates a certain functional component of a service running on a hardware server. Deploying a server role to a server indicates that the server provides the corresponding function. Multiple server roles, such as PanguMaster and TianjiClient, can be deployed on the same server.

We recommend that you use Upper Camel Case to name a server role, with a number sign (#) as the suffix. For example, PanguMaster#. To support multiple tenants, the full name of a server role contains the service name prefix as the namespace. For example, pangu.PanguMaster.

Server role instance

An instance of a server role that is deployed in a cluster. A server role instance is expressed by <ServerRoleName>#[instanceNO], where ServerRoleName is the name of the server role, and instanceNO is the instance number that can be a number or null.

Multiple instances of the same server role can be deployed in the same cluster. For example, PanguLib can have multiple versions in a cluster. Different instances of the same server role are expressed by a number sign (#) and a suffix. For example, PanguLib#56 and PanguLib#57.

Application

An application corresponds to a process-level service component in a server role. Each application works independently. Application is the minimum unit for deployment and upgrade in the Apsara Infrastructure Management Framework system, and can be deployed to every server.

An application is named by using lowercase letters, with an underline (_) between two words. For example, the server role PanguMaster contains two applications: pangu_master and pangu_interval_runner.

Rolling

Each time when a user updates configurations, Apsara Infrastructure Management Framework issues the configurations, 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 in clusters. A service configuration template can be created to quickly write the same configurations to different clusters.

The service configuration template can be used for large-scale deployment and upgrade.

Associated service template

A *template.conf* file exists in the configuration. This file specifies the service configuration template and its version, of which the configuration is used by the service.

Service deployment

Deployment of new services in a cluster from scratch.

Service upgrade

Modifications made to services deployed in a cluster.

2.2.2 Homepage overview

This section describes the operation portals of main functions on Apsara Infrastructure Management Framework to familiarize you with Apsara Infrastructure Management Framework.

Log on to Apsara Infrastructure Management Framework.

The homepage is described as follows:

Menu bar

- **Operations:** Allows O&M personnel to quickly locate the operations and operation objects, and perform O&M operations.

Select **Project Operations**, **Cluster Operations**, **Service Operations**, and **Server Operations**.

- **Project Operations:** Manages projects with the project permission.
- **Cluster Operations:** Performs O&M management on clusters with the project permission, such as checking the cluster status.
- **Service Operations:** Manages services with the service permission, such as managing the monitoring templates.
- **Server Operations:** Maintains and manages all servers in Apsara Infrastructure Management Framework, such as logging on to the terminal service of a server directly, adding a server to Apsara Infrastructure Management Framework, and migrating buckets.
- **Tasks:** Tasks, such as rolling tasks, are generated after you modify configurations. You can view the running and history tasks.
- **Reports:** Allows you to access the portal report platform. Data can be displayed in tables, graphics, or texts.
- **Management:** Includes the portal permission management, data source management, and custom portal management.
- **Monitoring:** Includes alarm status and alarm rules.

Navigation bar


You can directly view the logical structure of Apsara Infrastructure Management Framework model in the navigation bar.

- **Cluster:** Supports fuzzy query of clusters under a project, and allows you to view the cluster information and cluster O&M information, manage and monitor clusters, view information about machines in a cluster, and log on to the machine terminal for further operations.
- **Service:** Supports fuzzy query of services and allows you to manage services and instances under a service.
- **Report:** Supports fuzzy query of reports and allows you to view the report details.

By selecting nodes at different levels in the navigation bar, you can view the detailed data analysis and operations of each node.

The navigation bar also provides a view list, in which you can open a view report.

Navigation bar fold/unfold button

You can click  to fold the navigation bar and increase the space of the content area when performing some O&M operations.

Special function button

- Synchronization time: Indicates the generation time of the data that is currently displayed on the portal.
- Final-state time: Indicates the computing time of the final-state data that is currently displayed on the portal.

After data is generated, the system processes the data at the maximum speed. As an asynchronous system, Apsara Infrastructure Management Framework is subject to delay. This delay helps explain the data results displayed on the portal and determine whether or not the current system has any fault.

2.2.3 System management

2.2.3.1 Permission management

Select **Management > Permission Management** to go to Operation Administrator Manager (OAM). For more information, see OAM user guide.

2.2.3.2 Data source management

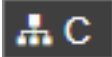
The data source Tianji DB exists by default. All users have the read-only permission, which cannot be modified. No need to apply for permissions. In addition, the data source serves the purpose of a report platform. Currently, the report platform is used as an auxiliary method for troubleshooting issues on Apsara Infrastructure Management Framework. Therefore, only the read permission is granted.


2.2.4 Project management

1. Select **Operations > Project Operations**. The **Project Operations** page is displayed.
2. Enter a project name in the **Fuzzy Search** field to locate the project.
3. Click **Refresh** to refresh the project list.
4. At the right of a project, click **Delete** to delete a project.
5. At the right of a project, click **Details** to go to the **Cluster Operations** page and view all the clusters of this project.

2.2.5 Cluster management

2.2.5.1 Cluster dashboard

On Apsara Infrastructure Management Framework, click the  tab in the upper-left corner.

Place your cursor on  at the right of the cluster and then select **Dashboard**. The **Cluster Dashboard** page is displayed.

The cluster dashboard provides the basic cluster information, final-status information, rolling job information, dependencies, resource information, virtual machines, and monitoring information.

For more information, see [Parameter descriptions](#).

Table 2-6: Parameter descriptions

Module	Parameter description
Cluster Basic Information	<ul style="list-style-type: none"> Project name. Cluster name. Final status version: The latest version of the cluster. Cluster in final status: Indicates whether or not the cluster reaches the final status. Servers not in final status: The number of servers not in final status if the cluster does not reach the final status. Real/pseudo clone: Indicates whether or not to clone the system when a server is added to the cluster. Expected servers: The number of servers that are expected in the cluster. Actual servers: The number of servers that are currently in the cluster. Servers not good: The number of servers whose status is not good in the cluster. Actual services: The number of services that are actually deployed in the cluster. Actual service roles: The number of server roles that are deployed in the cluster. Cluster status: Indicates if the cluster is started or shut down.

Module	Parameter description
Server Status Overview	The statistical table of the server status in the cluster.
Servers in Final Status	The final-status conditions of servers deployed in the cluster.
Load-System	The load chart of the cluster system.
CPU-System	The CPU load chart.
Mem-System	The memory load chart.
Disk_usage-System	The disk usage load chart.
Traffic-System	The system traffic chart.
TCP state-system	The TCP request status chart.
TCP retrans-System	The TCP retransmission volume information.
Disk_IO-System	The disk read/write information.
Service Instances List	<p>Displays the service instances currently deployed in the cluster and the related final status information.</p> <ul style="list-style-type: none"> • Service instance: Service deployed in the cluster. • Final status: Indicates whether or not the service reaches the final status. • Expected server roles: The number of server roles that are expected in the service instance. • Server roles in final status: The number of server roles that reach the final status in the service instance. • Server roles going offline: The number of server roles that are going offline in the service instance. • At the right of the service instance, click Details to go to the Service Instance Dashboard page.
Upgrade Tasks	<p>Displays the change tasks related to the cluster.</p> <ul style="list-style-type: none"> • Cluster name: The name of the cluster.



Module	Parameter description
	<ul style="list-style-type: none"> • Type: Type of the upgrade task. The options include app (version upgrade) and config (configuration change). • Git version: The changed version to which the upgrade task belongs. • Description: Description about the change. • Rolling result: Result of the upgrade task. • Submitted by: Person who submits the change. • Submitted at: Time for submitting the change. • Start time: Time for starting the rolling. • End time: Time for finishing the upgrade. • Time used: Time used for the upgrade. • Actions: Click Details to go to the Rolling Details page.
Cluster resource request status	<ul style="list-style-type: none"> • version: The changed version. • msg: Exception information. • begintime: Start time of change analysis. • endtime: End time of change analysis. • buildstatus: Result of change analysis. • resourceprocessstatus: Application status of the resource in the version.
Cluster Resource	<ul style="list-style-type: none"> • Service • serverrole: Name of the server role. • app: Application of the server role. • name: Resource name. • type: Resource type. • status: Resource application status. • error_msg: Exception information. • parameters: Resource parameter. • result: Resource application result. • res: Resource ID. • reprocess_status: Status of interaction with Business Foundation System during VIP resource application.

Module	Parameter description
	<ul style="list-style-type: none"> reprocess_msg: Error message of interaction with Business Foundation System during VIP resource application. reprocess_result: Result of interaction with Business Foundation System during VIP resource application. refer_version_list: Version that uses the resource.
VM Mappings	<p>Displays the information about virtual machines in the cluster. Data is available only when virtual machines are deployed in the cluster.</p> <ul style="list-style-type: none"> VM: Hostname of the virtual machine. Currently deployed on: The hostname of the physical machine where the virtual machine is deployed. Target deployed on: The hostname of the physical machine where the virtual machine is expected to be deployed.
Service Dependencies	<p>Displays the dependencies of the service instances and server roles in the cluster, and the final status information about the dependent service or role.</p> <ul style="list-style-type: none"> Service: Service name. Service role: Server role name. Dependent service: Service on which the server role depends. Dependent service role: Server role on which the server role depends. Not reaching final status: Number of the clusters in which the dependent server role does not reach the final status. Total: Number of clusters in which the dependent server role is deployed.

2.2.5.2 Cluster Operation and Maintenance Center

Log on to Apsara Infrastructure Management Framework.

Three methods are available to access the **Cluster Operation and Maintenance Center**:


- Click the  tab in the upper-left corner. Place your cursor on  at the right of the cluster and then select **Cluster Operation and Maintenance Center**.
- Select **Operations > Cluster Operations**, and then select **Monitoring > Cluster Operation and Maintenance Center** at the right of the cluster.
- On the **Cluster Dashboard** page, select **Operations Menu > Cluster Operation and Maintenance Center**.

The **Cluster Operation and Maintenance Center** page is displayed.

For more information about the parameters on this page, see [Parameter descriptions](#).

Table 2-7: Parameter descriptions

Parameter	Description
Total Servers	Indicates the total number of servers in the cluster.
Scale-in/Scale-out	Indicates that the server or server role is going online or offline.
Abnormal Server	Indicates the number of abnormal servers that encounter each type of the following fault: <ul style="list-style-type: none"> Ping failed: A ping_monitor error is reported, and the Apsara Infrastructure Management Framework master cannot successfully ping the server. No heartbeat: The tj-client on the server does not periodically report data to indicate the status of this server. This problem may be caused by a tj-client or network fault. Status error: The monitor reports an error or a fault of the critical or fatal level for the server. Check the alarm information and accordingly handle the fault.
Abnormal Service	Apsara Infrastructure Management Framework determines if a service reaches the final status according to the following criteria: <ul style="list-style-type: none"> The server role on the server is in GOOD status. The actual version of each application of the server role on the server must be the same as the HEAD version. Before Image Builder builds a HEAD version corresponding to an application, Apsara Infrastructure Management Framework cannot determine the value of the HEAD version and the service final status is unknown. This process is called by portal as the change preparation process. The service final status cannot be determined during the preparation process or upon a preparation failure.

Parameter	Description
SR not in Final Status	Displays all server roles that do not reach the final status in the cluster . Click the number to expand a list, and click a record in the list to filter servers.
Running Tasks	Displays the number of rolling tasks, if any.
HEAD Version Commit Time	Displays the time that the HEAD version is submitted. Click the time to view the submission details.
HEAD Version Analysis Status	Indicates the build status of the HEAD version.
Service	Select a service deployed in the cluster from the drop-down list.
Service Role	<p>Select a server role of a service in the cluster from the drop-down list.</p> <div>  Note: After you select a service and server role, the list below displays the status of server roles on the servers. </div>
Server List	<p>View all the servers in the cluster, or filter out the server where the corresponding server role is located by specifying the service and server role.</p> <ul style="list-style-type: none"> • Server: Click the search box to enter the server name in the displayed dialog box. Multiple servers can be searched at a time. • Click the hostname of a server to view the physical information of the server. Click Dashboard to view the server details. • Click Details under Final Status to view the status and exception information of services on the server. <ul style="list-style-type: none"> — Normal — Server scale-in: The server is being removed from the cluster for scale-in purpose. — Server scale-out: The server is being added to the cluster for scale-out purpose. — SR scale-in: A server role is being deleted from the server for scale-in purpose. • Click Details under Running Status to view the server running status and exception information. • Click Error, Warning, or Good under Monitoring Statistics to view the server monitoring items and server role monitoring items. • Click Terminal under Actions to log on to the server and perform related operations.

2.2.5.3 Service final status

Procedure

1. Select **Operations > Cluster Operations**.
2. At the right of the cluster, select **Monitoring > Service Final Status Query**. The **Service Final Status Query** page is displayed.

For more information about the parameters on this page, see [Parameter descriptions](#).

Table 2-8: Parameter descriptions

Parameter	Description
Final Status Version	Indicates the HEAD version of the cluster.
Modify Preparation Status	Indicates that Apsara Infrastructure Management Framework detects the latest version and has parsed it into specific content.
Cluster Rolling Status	Displays the information of the current rolling task in the cluster, if any. The rolling task may not be of the HEAD version.
Cluster Server Final Status Statistics	Indicates the status of all servers in the cluster. Click View Details to view the detailed information of all the servers.
Cluster SR Version Final Status	Indicates if the server role version is consistent on servers and if the status is GOOD.
SR Version Final Status	Displays the number of servers that do not reach the final status when a server role has tasks.

2.2.5.4 Cluster configuration

Procedure

1. Select **Operations > Cluster Operations**.
2. At the right of the cluster, click **Cluster Configuration**.

The **Cluster Configuration** page is displayed. You can view the related cluster configurations on this page.

2.2.5.5 Operation logs

Procedure

1. Select **Operations > Cluster Operations**.
2. At the right of the cluster, select **Monitoring > Operation Logs**. The **Operation Logs** page appears.

3. Click **View Release Changes**. The **Version Difference** page is displayed.
4. Configure the conditions for comparing the version differences.
 - Select Base Version: Select a base version.
 - Obtain Configuration Type
 - Extend Configuration: Displays the configuration differences after the configuration on the cluster is combined with the configuration in the template.
 - Cluster Configuration: Displays the configuration differences on the cluster.
5. Click **Obtain Difference**.

The differences are displayed in the **Differential File List**.

2.2.6 Modify a monitoring template

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Operations > Service Operations**.
3. At the right of the service, click **Management**.
4. Select the **Monitoring Instance** tab to view the services that trigger the alarms.

You can view the deployment status and deployment logs.
5. To modify a monitoring template, view the monitoring template used by the service under the **Monitoring Instance** tab and then select the **Monitoring Template** tab.
6. We recommend that you modify a monitoring template of the sub type. At the right of the template, click **Edit**.
7. Under the **Alarm Rule** tab, click **Edit** at the right of the alarm. The template settings dialog box is displayed.
8. Set the monitoring parameters according to the actual conditions.
9. Click **Preview Change** to view the changes.
10. Click **Save Change** to save the changes.

Wait for about 10 minutes. The monitoring instance is automatically deployed, the check status is changed to **Success**, and the deployment time is the time after the template is modified, indicating that the latest changes have been successfully deployed.

2.2.7 Ticket management

2.2.7.1 Manage ticket permissions

The administrator can grant roles the permissions to process tickets. This section describes how to manage the ticket permissions.

Context

Users have the following four roles:

- Business Party: Users who manually open and check tickets.
- IDC Administrator: Users who diagnose faults based on manually opened tickets and fill in the fault details.
- Room Resident PE: Users who repair machines.
- Room Administrator: The administrator of the data center, who is generally not used.

Procedure

1. Log on to Apsara Infrastructure Management Framework as an administrator.
2. Select **Management > Ticket Management Permission**. The **Ticket Management Permission** page is displayed.
 - TianjiAPI is the account used to open a ticket on Apsara Infrastructure Management Framework, which cannot be operated or modified.
 - SiteAdmin is the current logon account.
3. At the right of the current logon account, click **Modify Permission**. The **Add User** dialog box is displayed.
4. Select a role as required.
 - To open a ticket, select **Business Party**.
 - To process a ticket, select **IDC Administrator**.
 - To repair a machine, select **Room Resident PE**.

2.2.7.2 Create a ticket

2.2.7.2.1 Manually open a ticket

2.2.7.2.1.1 Process description

The process of opening a ticket manually is as follows:

1. After detecting a machine fault, the Business Party opens an event ticket to describe the fault symptom.

When opening a ticket, switch the role of the logon account to Business Party or log on to the system as the Business Party.

2. The IDC administrator checks the event ticket opened by the Business Party, verifies the fault, and fills in the fault details.

When checking the event ticket, switch the role of the logon account to IDC administrator or log on to the system as the IDC administrator.

3. The room resident PE troubleshoots the fault and completes the repair process.

When troubleshooting the fault, switch the role of the logon account to room resident PE or log on to the system as the room resident PE.

2.2.7.2.1.2 Procedure

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Switch the role to Business Party and select **Management > Ticket Management**. The **Ticket Management** page is displayed.
3. Click **Create Ticket**. The event ticket settings dialog box is displayed.
4. Set the fault information.
5. Click **Confirm**.
6. Switch the role to IDC administrator and select **Management > Ticket Management**. The **Ticket Management** page is displayed.
7. Under the **Pending Tickets** tab, select tickets and click **Claim Multiple Tickets**.
8. Under the **Received Tickets** tab, view the event ticket details and determine if the event ticket is reasonable.
 - If not reasonable, select the event ticket and click **Cancel** to end the ticket.
 - If reasonable, select the event ticket and click **OK** to go to the next step.

The **Create Ticket** dialog box is displayed.

9. Enter the fault details.
10. Click **OK**.

Apsara Infrastructure Management Framework sends an action to the machine, whose status becomes `human_pending`.

11. Switch the role to Business Party and select **Reports > All Reports**.

12. Search Machine RPM Approval Pending List in fuzzy mode and click **Machine RPM Approval Pending List**. The **Machine RPM Approval Pending List** page is displayed.

13. Click **Action Approval**.

14. On the **Action Approval** page, set the status to **Pending**.

15. Click **OK**.

After the machine repair is approved, the system performs automatic data backup and service migration. The `rma_labor` opens a ticket.

16. Switch the role to room resident PE and select **Management > Ticket Management**. The **Ticket Management** page is displayed.

17. Under the **Pending Tickets** tab, select tickets and click **Claim Multiple Tickets**.

18. The room resident PE repairs the machine based on the ticket.

19. After the repair, click the **Received Tickets** tab on the **Ticket Management** page and then click the ticket ID. The details page is displayed.

20. Click **Repair Finished**.

The Apsara Infrastructure Management Framework repair process automatically starts. Apsara Infrastructure Management Framework performs repair operations, such as formatting and attaching a hard disk after it is changed.

21. The ticket ends after the Apsara Infrastructure Management Framework repair process is completed.

You can switch the account role to Business Party and select **Management > Ticket Management** to check the ticket details.

2.2.7.2.2 Apsara Infrastructure Management Framework opens a ticket after self-check

Procedure

1. The Apsara Infrastructure Management Framework client performs self-check.
2. The `rma_labor` opens a ticket after obtaining the approval from the service decider.
3. The room resident PE repairs the machine. After the repair, the room resident PE logs on to the system and clicks **Repair Finished** on the **Ticket Management** page.

4. The rma_labor synchronizes the ticket status, and the RMA is completed.
5. The ticket is closed.

2.2.8 Server management

2.2.8.1 Add a server

Procedure

1. On Apsara Infrastructure Management Framework, select **Operations > Server Operations**.
The **Server Operations** page is displayed.
2. Click **Server Online/Offline**.
3. In the displayed dialog box, click the **Add Server** tab.
4. Set the target project and target bucket, and upload the configuration file.

The configuration file is the server list to be uploaded. Click **Download Schema** to obtain the server list table in *.xlsx* format. You can use this table to supplement the server list. The table is as shown in [Schema format](#).



Note:

The attribute columns can be added. However, the added server attributes must be recognized by Apsara Infrastructure Management Framework.

Generally, servers are not expanded on portal. To expand servers on portal, Apsara Infrastructure Management Framework must provide all the required attribute columns for the onsite engineers.

Figure 2-2: Schema format

	A	B	C	D	E	F	G	H	I
1	nodename	Sn	Ip	Hw_cpu	Hw_harddisk	Hw_mem	Idc	Location_in_Rack	Model
2	required:hostname	required	required						
3									
4									
5									
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									

5. Click **Confirm Online**.

2.2.8.2 Change server bucket

Procedure

1. On Apsara Infrastructure Management Framework, select **Operations > Server Operations**.
2. Click **Server Bucket Change**.
3. In the displayed dialog box, select the target project and target bucket.
4. Enter the server hostnames in the **Enter server list** field, one on each line.

If the current user is the owner or user of the project where the server to be modified resides, go to step [5](#).

If the current user is not the owner or user of the project, click **View Owner** and contact the owner to set the current user as the user of the target project.

5. Click **Confirm**.

2.2.8.3 Delete a server

Procedure

1. On Apsara Infrastructure Management Framework, select **Operations > Server Operations**.
The **Server Operations** page is displayed.
2. Click **Server Online/Offline**.
3. Click the **Remove Server** tab.
4. Enter the server hostnames in the **Enter server list** field and verify that the information is correct.
5. Click **Clear Servers**.

2.2.9 Task management

2.2.9.1 Query tasks

Tasks are divided into running tasks and history tasks. This section describes how to query task details.

Procedure

1. On Apsara Infrastructure Management Framework, select **Tasks > Running Tasks**. The **Running Tasks** page is displayed.
2. View the running tasks.

- Cluster: The cluster where a running task resides.
 - Rolling task status: The status of the running task. Click **View Tasks** to view the running details.
 - Rolling time: The duration that a task runs.
 - Machine change state: Offline is displayed if any machine in the cluster is deprecated.
3. Select **Tasks > History Tasks**. The **History Tasks** page is displayed.
 4. You can filter tasks by cluster name, Git version, start time, and end time.

2.2.9.2 Deployment overview

This section describes how the clusters, services, and server roles in all the projects on Apsara Infrastructure Management Framework are deployed.

2.2.9.2.1 Deployment progress

On Apsara Infrastructure Management Framework, select **Tasks > Deployment Summary**. The **Deployment Summary** page is displayed.

- View the deployment status of each project and the duration of a certain status.
 - Grey: Wait to be deployed. It indicates that some services of the project depend on server roles or services that are being deployed, and other services 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 prohibited.
- Configure the global dependency switch.
 - normal: All the dependencies are checked.
 - ignore: The dependency is not checked.
 - ignore_service: The service-level dependency (including the server role dependencies across services) is not checked, and only the server role-level dependency is checked.

2.2.9.2.2 Deployment details

Select **Tasks > Deployment Summary**.

On the **Deployment Summary** page, click **Deployment Details**.

For more information about the parameters of deployment details, see [Parameter descriptions](#).

Table 2-9: Parameter descriptions

Parameter	Description
Status Statistics	<p>The general deployment statistics, including the 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:</p> <ul style="list-style-type: none"> Final: All the clusters in the project have reached the final status. The icon is a green tick. Deploying: The project has not reached the final status for one time yet. The icon is a blue in-progress symbol. Waiting: Some services of the project depend on server roles or services that are being deployed, and other services or server roles in the project have already been deployed. The icon is a grey pause symbol. 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. The icon is a red cross. Inspector Warning: An error is detected on services under the project during the inspection. The icon is a yellow exclamation mark.
Start Time	Time when Apsara Infrastructure Management Framework deployment starts.

Parameter	Description
Progress	The ratio of server roles under all projects that reach the final status to all the server roles under all projects.
Deployment Status	<p>The deployment duration for the following statuses: Final, Deploying, Waiting, and Inspector Warning.</p> <p>The duration before the final status is reached for the Non-final status.</p> <p>Click the time to view the detailed information.</p>
Deployment Progress	<p>The ratio of clusters, services, and server roles under the project that reach the final status to the total clusters, services, and server roles.</p> <p>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.</p>
Resource Application Progress	<p>Total indicates the total number of resources related to the project.</p> <ul style="list-style-type: none"> • 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 of which applications are blocked by other resources. • Failed: The number of resources of which applications fail.
Inspector Error	The number of inspection alarms for the current project.
Monitoring Information	The number of alarms generated for the machine monitor and the machine server role monitor in the current project.
Dependency	Click the icon to view the services under the project that depend on other services, and the current deployment status of the services that are depended on.

2.2.10 Alarm center

Alarm status

Select **Monitoring > Alarm Status**.

On the **Alarm Status** page, select the service and cluster from the drop-down lists and then set the start time and end time to view the status of the service and cluster on Apsara Infrastructure Management Framework.

Alarm rules

Select **Monitoring > Alarm Rules** to view the details of all alarms on Apsara Infrastructure Management Framework.

Click **Download alarm reference document** to download the reference document about how to handle the alarms.

Alarm history

Select **Monitoring > Alarm History** to view the details of all historical alarms on Apsara Infrastructure Management Framework.

You can enter the AlertKey to query a specific alarm.

2.2.11 Report management

2.2.11.1 Info of project component report

Provides the running status of services and server roles on servers under each cluster of the project.

- Project: The project name.
- Cluster: The cluster name.
- Service: The service name.
- Service role: The server role name.
- Service role status: The running status of a server role on the server.
- Service role action: The action of a server role on the server. Data is available only when Apsara Infrastructure Management Framework requests the server role to perform certain actions, such as rolling and restart.
- Machine name: The server hostname.
- IP: The server IP address.

- **Server status:** The running status of the server.
- **Server action:** The action that Apsara Infrastructure Management Framework requests the server to perform, such as clone.

2.2.11.2 State of project component

Provides the status of all server roles in an abnormal status on servers of the project, and monitoring information (alarm information written by the server role to the Apsara Infrastructure Management Framework monitor) of server roles and servers.

- **Error State Component table:** Only the server roles that are not in GOOD status and server roles to be upgraded are displayed.
 - **Project:** The project name.
 - **Cluster:** The cluster name.
 - **Service:** The service name.
 - **Service role:** The server role name.
 - **Machine name:** The server name.
 - **need_upgrade:** Indicates whether or not the current version reaches the final status.
 - **Service role status:** The server role status.
 - **Server status:** The server status.
- **Machine SR Monitor Info:** Select a row in **Error State Component table** to filter out the monitoring information (non-good and info) of the selected server role.
 - **Cluster:** The cluster name.
 - **Service:** The service name.
 - **Service role:** The server role name.
 - **Machine name:** The server name.
 - **Monitor:** The monitoring name of the server role.
 - **Level:** The alarm level.
 - **Description:** The monitoring report contents.
 - **Updated at:** The monitoring updated time.
- **Machine Monitor Info:** Select a row in **Error State Component table** to filter out the monitoring information (non-good and info) of the selected server.
 - **Cluster:** The cluster name.
 - **Machine name:** The server name.

- Monitor: The alarm information of the server.
- Level: The alarm level.
- Description: The alarm information.
- Updated at: The updated time.
- **Service Inspector Info:** Select a row in **Error State Component table** to filter out the monitoring information (non-good and info) of the selected server.
 - Cluster: The cluster name.
 - Service: The service name.
 - Service role: The server role name.
 - Monitor: The inspection report name.
 - Level: The level.
 - Description: The contents of the inspection report.
 - Updated at: The updated time.

2.2.11.3 Machine info report

Displays the server-related information.

- **Machine Status:** Displays all the servers currently managed by Apsara Infrastructure Management Framework and their statuses. In the global filter on top of the page, select the project, cluster, and server, and then click **Filter** on the right to filter the data.
 - Machine name: The server name.
 - IP: The server IP address.
 - Server status: The server status.
 - Server action: The action currently performed by the server.
 - Server action status: The action status.
 - State description: The server status description.
- **Expected SR list of Machine {{server selected in Machine Status}}:** The server roles that must be installed on the selected server.
 - Machine name: The server name.
 - Service role: The server role name.
- **Abnormal monitoring status of {{server selected in Machine Status}}:** The monitoring information of the selected server.
 - Machine name: The server name.

- Monitor: The monitoring item.
- Level: The level of the monitoring item.
- Description: The contents of the monitoring item.
- Updated at: The updated time of the monitoring item.
- **SR's version and status of machine {{server selected in Machine Status}}**: The server role status on the selected server.
 - Machine name: The server name.
 - Service role: The server role name.
 - Service role status: The server role name.
 - Target version: The expected version of the server role on the server.
 - Current version: The actual version of the server role on the server.
 - State description: The reason of the status change.
 - Error message: The error message of the server role.
- **Monitor of machine {{server selected in SR's version and status of machine}}{{server role selected in SR's version and status of machine}}**: Displays the monitoring information of the selected server role. Only the non-good monitoring information is displayed.
 - Machine name: The server name.
 - Service role: The server role name.
 - Monitor: The monitoring item of the server role.
 - Level: The monitoring level.
 - Description: The monitoring item information.
 - Updated at: The monitoring updated time.

2.2.11.4 Action of machine SR

Apsara Infrastructure Management Framework manages information of all servers that are performing the Apsara Infrastructure Management Framework actions, such as the clone action. If the server is a host, you can view the virtual machine status on the server and the server role status on the virtual machine.

- **Action of Machine SR**: Only displays the servers with actions.
 - Project: The project name.
 - Cluster: The cluster name.
 - Machine name: The server hostname.

- IP: The server IP address.
- Server status: The running status of the server.
- Server action: The action that Apsara Infrastructure Management Framework requests the server to perform, such as clone.
- Service role: The service name + server role name.
- Service role status: The running status of the server role.
- Service role action: The action of the server role on the server, such as rolling, restart, and offline.
- **VM SR Action on Host ({{server}}).**

Select a row in **Action of Machine SR** to filter out the information of virtual machines running on the selected server, with the hostname in the selected row as the filter condition. Data is available only when the selected server is a host.

- VM: The virtual machine hostname.
- IP: The virtual machine IP address.
- Server status: The running status of the virtual machine.
- Server action: The action performed by the server, such as clone.
- Service role: The server role running on the virtual machine.
- Service role status: The running status of the server role.
- Service role action: The action of the server role on the server, such as rolling, restart, and offline.

2.2.11.5 State of machine clone

Displays the server clone status.

- **The Progress of machine clone:** View the progress of the server clone.
 - Project: The project name.
 - Cluster: The cluster name.
 - Machine name: The server name.
 - Server status: The server status.
 - Progress of machine clone: The progress of the current clone process.
- **The State of machine clone:** View the status of the server clone process.
 - Project: The project name.
 - Cluster: The cluster name.

- Machine name: The server name.
- Server action: The Apsara Infrastructure Management Framework action currently performed by the server.
- Server action status: The action status.
- Server status: The server status.
- Level: Indicates whether or not the clone action performed by the server is normal.
- State of machine clone: The current status of the clone action performed by the server.

2.2.11.6 Service inspector report

Use the global filter to filter out the service inspection reports of a cluster.

Data is available in the service inspection report only when the service inspection is configured.

- Project: The project name.
- Cluster: The cluster name.
- Service: The service name.
- Description: The contents of the inspection report.
- Level: The inspection report level.

2.2.11.7 Resource apply report

In the global filter on top of the page, select the project, cluster, and server, and then click **Filter** on the right to filter the resource application data.

- **Commit List:** Resource change applications in the cluster can be detected.
 - project: The project name.
 - cluster: The cluster name.
 - version: The changed version.
 - resourceprocessstatus: The resource application status in the version.
 - msg: The exception information.
 - begintime: The start time of the change analysis.
 - endtime: The end time of the change analysis.
- **Commit Resource Map:** The list of resources corresponding to changes.
 - res: Version of the change.
 - 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 State:** The status of resources in the cluster.
 - project: The project name.
 - cluster: The cluster name.
 - Service: The service name.
 - serverrole: The server role name.
 - 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 interaction with Business Foundation System during VIP resource application.
 - reprocess_msg: The error message of interaction with Business Foundation System during VIP resource application.
 - reprocess_result: The result of interaction with Business Foundation System during VIP resource application.
 - refer_version_list: The version that uses the resource.
 - error_msg: The exception information.

2.2.11.8 Rolling info report

Displays the rolling jobs that are currently running and the related job status.

- **Choose a Job:** Displays only the rolling jobs that are currently running. No data is displayed in the table if no jobs are running.
 - Cluster: The cluster name.
 - Git version: The version of change that triggers the rolling job.

- Description: The description about the change entered by a user when the user submits the change.
- Start time: The start time of the job.
- End time: The end time of the job.
- Submitted by: The ID of the user who submits the change.
- Rolling task state: The running status of the job.
- Submitted at: The time when the change is submitted.
- **SR in Job:** Select a rolling job in **Choose a Job** to filter out the rolling status of server roles related to the selected job. If no rolling job is selected, the status of server roles of all the historical rolling jobs are displayed.
 - Service role: The server role name.
 - Service role status: The rolling status of the server role.
 - Error message: The rolling error message.
 - Git version: The version to which the change belongs.
 - Start time: The rolling start time.
 - End time: The rolling end time.
 - Approve rate: The ratio of servers that have the rolling approved by the decider.
 - Failure rate: The ratio of servers that encounter rolling failures.
 - Success rate: The ratio of servers that succeed in rolling.
- **SR Rolling Build Info:** Source version and target version of each application under the server role in the rolling process.
 - app: The name of the application that requires rolling in the server role.
 - Service role: The server role to which the application belongs.
 - from_build: The source version of the upgrade.
 - to_build: The target version of the upgrade.
- **SR State in Cluster:** Select a server role in **SR in Job** to filter out the status of this server role deployed on the server.
 - machine: The name of the server on which the server role is deployed.
 - expectedversion: The target version of the rolling process.
 - actualversion: The current version.
 - state: The server role status.

- **actionname:** The Apsara Infrastructure Management Framework action currently performed by the server role.
- **actionstatus:** The action status.

2.2.11.9 Virtual machines map

Use the global filter to filter out the virtual machines of a cluster.

VM Mappings: Displays the information of virtual machines in the cluster. Data is available only when virtual machines are deployed in the cluster.

- **project:** The project name.
- **cluster:** The cluster name.
- **VM:** The virtual machine hostname.
- **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.

2.2.11.10 Relationship of service dependency

Displays the dependencies among server roles. Use the global filter to filter out the cluster data.

- **Project:** The project name.
- **Cluster:** The cluster name.
- **Service:** The service name.
- **Service role:** The server role name.
- **Dependent service:** The service on which the server role depends.
- **Dependent service role:** The server role on which the server role depends.
- **Not reaching final state:** Number of the clusters in which the dependent server role does not reach the final state.
- **Total:** Number of clusters in which the dependent server role is deployed.

2.2.11.11 Registration vars of service

Displays values of all service registration variables.

Registration Vars of Service

- **service:** The service name.
- **service_registration:** The service registration variable.

- cluster: The cluster name.
- \$updatetime: The updated time.

2.2.11.12 Check report of network topology

Checks if any wirecheck alarms are generated for the network devices or servers.

- **Check Report of Network Topology:** Checks if any wirecheck alarms are generated for the network devices.
 - Cluster: The cluster name.
 - Network instance: The network device name.
 - Level: The alarm level.
 - Description: The alarm information.
- **Check Report of Server Topology:** Checks if any wirecheck alarms are generated for servers (machines).
 - Cluster: The cluster name.
 - Machine name: The server (machine) name.
 - Level: The alarm level.
 - Description: The alarm description.

2.2.11.13 Machine RPM approval pending list

Some Apsara Infrastructure Management Framework actions on servers and server roles can be triggered by users in a way similar to restart, 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**
 - Project: The project name.
 - Cluster: The cluster name.
 - Hostname: The server hostname.
 - IP: The server IP address.
 - State: The running status of the server.
 - Action name: The action on the server.
 - Action status: The status of the action on the server.
 - Actions: The approval button.
- **machine_serverrole**

- Project: The project name.
- Cluster: The cluster name.
- Hostname: The server hostname.
- IP: The server IP address.
- 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**
 - Project: The project name.
 - Cluster: The cluster name.
 - Hostname: The server hostname.
 - Component: The hard disk on the server.
 - 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.

2.2.11.14 Auto healing/install approval pending report

The table structure is the same as that of machine RPM approval pending list, except that this view is used to approve the installation.

2.2.11.15 Machine power on or off state of cluster

After the cluster on/off operation is triggered, you can read the related information from this report.

- **Cluster running state:** If a cluster is performing the on/off operation, corresponding data is available in this table.
 - Project: The project name.
 - Cluster: The cluster name.
 - Machine live state: On/off action that is being performed by the cluster.
- **SR Power on or off state in {{cluster selected in Cluster running state}}:** The on/off status of the server roles on the selected cluster.

- Cluster: The cluster name.
- Service role: The server role name.
- Machine live state: The on/off status of the server role.
- **{{Server role selected in SR Power on or off state}} State on Machine:** Displays the running status of the selected server role on the server.
 - Cluster: The cluster name.
 - Service role: The server role name.
 - Machine name: The server name.
 - Service role status: The running status of the server role.
 - Service role action: The action currently performed by the server role.
 - Service role action status: The action status.
 - Error message: The error message of the server role.
- **Machine State in {{cluster selected in Cluster running state}}:** Displays the running status of servers in the selected cluster.
 - Cluster: The cluster name.
 - Machine name: The server name.
 - IP: The server IP address.
 - Server status: The running status of the server.
 - Server action: The action currently performed by the server.
 - Server action status: The action status of the server.
 - Error message: The exception information.

2.2.11.16 Private service Tianji monitor state profile

Provides the statistics of the alarm amount and level of Tianji monitor.

- **Monitor Count in Every Hour:** The amount of alarms reported by the Tianji monitor.
- **Service Health Distribution:** The ServiceTest# server role monitoring and alarm statistics.
- **SR Health Distribution:** The post_check monitor monitoring and alarm statistics.
- **Hardware Health Distribution - ServerRole:** The monitoring of the server monitoring item independent_domain_check_syslog_sh.

2.2.11.17 Thermometer

Displays the cluster and server load statistics in the environment.

- **Machine CPU Health Distribution**

The load distribution of physical machines is displayed. The larger the color represents the number, the higher the load is.

- **Rank of Cluster Load**

The clusters in the list are sorted by load.

- **Rank of Cluster CPU Usage**

- **Rank of Cluster Memory Usage**

2.2.11.18 Tianjimon data of project

Displays the monitoring attributes based on projects monitored by Tianji monitor

- **Project read-data count**

- **Time**: The data updated time.

- **project**: The project name.

- **readCount**: The amount of data read by the project.

- **Sorted Shard**: The shard information list.

- **Time**: The recorded time.

- **project**: The project name.

- **key**: The shard name.

- **readCount**: The amount of data read by the shard.

- **uuid**: The shard ID.

- **latency**: The shard processing delay.

- **Partition**

- **Time**: The data updated time.

- **project**: The project name.

- **key**: The partition name.

- **readCount**: The amount of data read by the partition.

- **uuid**: The partition ID.

- **discardCount**: The amount of discarded data.

- **Flow**: The amount of data read by the project.

- **Lag**: The project read delay.

- **Count of Read Data**: Statistics of read data of the project.

- **OTS:** The output amount of the project compute node.
- **Compute Unit:** Statistics of the compute unit.
- **Exception:** Exception statistics.

2.2.11.19 Operation of ACC node

Displays the information of the Tianji monitor compute nodes.

- **Sorting of ACC Nodes**
 - Time: The data updated time.
 - address: The address.
 - readCount: The number of times data is read.
 - uuid: The compute node ID.
 - cacheCount: The data cache count.
- **CU Comparison**
 - Time: The data recorded time.
 - address: The node address.
 - computeUnit: The number of compute units.
- **Flow of In and Out:** Statistics of incoming and outgoing traffic of the compute node.
- **Amount of calculation:** The calculated amount of the compute node.
- **Failed Count:** Statistics of computing failures.
- **Partition List**
 - Time: The data updated time.
 - uuid: The partition ID.
 - key: The partition name.
 - computeUnit: The calculated amount of the partition.
 - discardCount: The amount of discarded data.
- **Partition State**

2.2.11.20 Operation of source node

Displays the information about the source nodes of Tianji monitor.

- **Source Node List Order by Flow**
 - Time: The recorded time.
 - address: The node address.

- inflow: The incoming traffic.
- uuid: The source node ID.
- **The Amount of Read Data (Node Load)**
 - Time: The recorded time.
 - address: The node address.
 - readCount: The number of times data is read.
- **Flow of In and Out:** The statistics of incoming and outgoing traffic.
- **Count of In and Out:** The total read or compute count.
- **Abnormal Index:** The statistics of abnormal data.
- **Lag of slsshard Recorded by Source:** Records the latency of Log Service shard.
- **Endpoint List:** The number of times that the endpoint sends data to the source.

2.2.11.21 Docker monitor - cluster

- Load
- CPU
- Memo
- Disk Usage
- Traffic
- TCP state
- TCP retrans
- Disk IO

2.2.11.22 Docker monitor - single

Statistical items include:

- Load
- CPU
- Memo
- Disk Usage
- Traffic
- TCP state
- TCP retrans
- Disk IO

2.2.11.23 JVM monitor - cluster

- Heap Memory
- Not Heap Memory
- Count of GC - Old
- Count of GC - New
- Time of GC - Old
- Time of GC - New
- Info of DeadLock
- Info of Process
- Class Loader
- Detail of Memory

2.2.11.24 JVM monitor - single machine

Displays the monitoring information of Java virtual machines on the server. The information is used by Tianji monitor.

- Heap Memory
- Not Heap Memory
- Count of GC - Old
- Count of GC - New
- Time of GC - Old
- Time of GC - New
- Info of DeadLock
- Info of Process
- Class Loader
- Detail of Memory

2.2.11.25 Unusual reference var of service

Displays changes to exposure variables, such as scale-up, scale-down, upgrade, and resource configuration changes. Apsara Infrastructure Management Framework can detect products on which rolling is performed again, changes to configurations, and specific changes.

- project
- cluster
- serverrole

- machine
- description
- \$updatetime

3 Appendix

3.1 Operation Administrator Manager (OAM)

3.1.1 OAM introduction

Overview

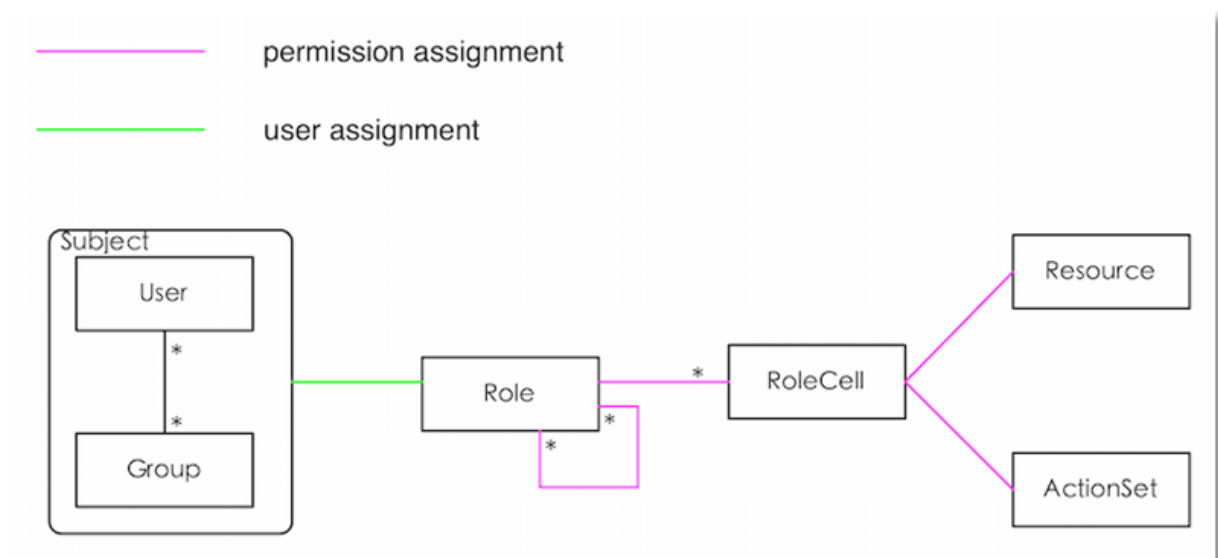
Operation Administrator Manager (OAM) is a centralized permission management platform of Apsara Stack Operation (ASO). OAM uses a simplified role-based access control (RBAC) model. Administrators can use OAM to assign roles to Operation & Maintenance (O&M) personnel, granting them corresponding operation permissions to O&M systems.

OAM permission model

In RBAC, administrators do not directly grant system operation permissions to users. Instead, they create a role set between the user set and the permission set. Each role corresponds to a group of permissions. If a role is assigned to a user, the user is granted all the operation permissions of that role. Therefore, when creating a user, administrators are only required to assign a role to the user, saving the trouble to grant specific permissions to the user. In addition, role permission change happens much less than user permission change does, simplifying user permission management and reducing system overhead.

See the [OAM permission model](#) as follows.

Figure 3-1: Permission model



3.1.2 Basic concepts

Before using OAM, you must know the following basic concepts about permission management.

Subject

Operators of the access control system. OAM subjects include users and groups.

User

Administrators and operators of ASO.

Group

A set of users.

Role

The core of the RBAC system.

Generally, a role can be regarded as a set of permissions. A role can contain multiple **RoleCells** and/or **roles**.

RoleHierarchy

In the OAM system, a role can contain other roles to form RoleHierarchy.

RoleCell

Specific description about a permission. A RoleCell consists of **resources**, **ActionSets**, and **WithGrantOptions**.

Resource

Description of the authorized object. For resources on each O&M platform, see [Operation permissions of O&M platforms](#).

ActionSet

Description of authorized operations. An ActionSet can contain multiple operations. For operations of O&M platforms, see [Operation permissions of O&M platforms](#)

WithGrantOption

Maximum number of authorizations in cascaded authorization, 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 **WithGrantOption** to 5 when granting a permission to administrator B, the permission can be granted for another five times at most. When administrator B grants the permission to administrator C, the value of **WithGrantOption** cannot be greater than 4. If **WithGrantOption** 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:

Currently, OAM does not support cascaded cancellation for cascaded authorization, that is, in the preceding example, administrator C and operator D still have the permission even if the permission is revoked for administrator B.

3.1.3 Log on to OAM

This section describes how to log on to OAM.

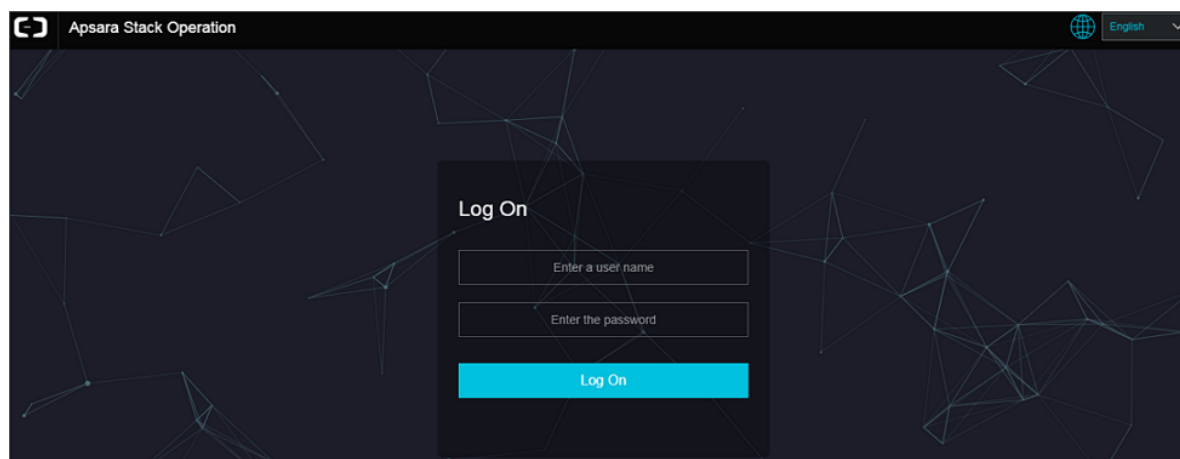
Prerequisites

- You have obtained the access address of ASO. The format of the access address is `http://region-id.aso.intranet-domain-id`.
- We recommend that you use the Chrome browser.

Procedure

1. Open the browser.
2. Enter the ASO access address `http://region-id.aso.intranet-domain-id` in the address bar and press Enter.

Figure 3-2: Log on to ASO



3. Enter the correct username and password.

- The system has three default users:
 - The security officer manages other users or roles.
 - The auditor officer views audit logs.
 - The system administrator is used for other functions except for those of the security officer and auditor officer.
 - To improve security, the password must meet minimum complexity requirements, that is, 10-20 characters long and containing English uppercase or lowercase letters (A-Z or a-z), numbers (0-9), or special characters (such as exclamation marks (!), at signs (@), number signs (#), dollar signs (\$), and percent signs (%)).
4. Click **Log On** to go to the ASO page.
 5. In the left-side navigation pane, select **Products** and then select **Operation Access Management**.

3.1.4 Quick start

3.1.4.1 Create a group

Create a user group for centralized management.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Group Management > Owned Groups**.
3. In the upper-right corner, click **Create Group**. In the displayed dialog box, enter the **Group Name** and **Memo**.
4. Then, click **Confirm**.

You can view the created group on the **Owned Groups** page.

3.1.4.2 Add group members

Add members to an existing group to grant permissions to the group members in a centralized way.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Group Management > Owned Groups**.
3. At the right of the group, click **Manage**.
4. Click **Add Member** in the **Group Members** section.

5. Select the search mode, enter the corresponding information, and then click **Detail**. The user details are displayed.

Three search modes are available:

- **RamAliasName**: Search the user in the format of *RAM username@primary account ID*. Use this mode for users who have activated Resource Access Management (RAM).
- **AliyunPk**: Search the user by using the unique ID of the user's cloud account.
- **AliyunId**: Search the user by using the logon name of the user's cloud account.

6. Click **Add**.

7. You can repeat the preceding steps to add more group members.

To remove a member from the group, click **Remove** at the right of the member in the **Group Members** section.

3.1.4.3 Add group roles

You can add roles to an existing group, namely, assign roles to the group.

Prerequisites

- The role to be added has been created. For how to create a role, see [Create a role](#).
- Make sure you are the owner of the group and role.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Group Management > Owned Groups**.
3. At the right of the group, click **Manage**.
4. Click **Add Role** in the **Role List** section.
5. Search roles by **Role Name**. Select one or more roles and set the expiration time.
6. Then, click **Confirm**.

To delete a role, click **Remove** at the right of the role in the **Role List** section.

3.1.4.4 Create a role

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Role Management > Owned Roles**.
3. In the upper-right corner of the **Owned Roles** page, click **Create Role**.

4. In the displayed dialog box, enter the **Role Name** and **Memo**, and then select the **Role Type**.
5. Optional: Set the role tag, which can be used for role search.

- a) Click **Edit Tag**.
- b) In the displayed **Edit Tags** dialog box, click **Create**.
- c) Enter the **Key** and the corresponding **Value** of the tag and then click **Confirm**.
- d) Repeat the preceding step to create more tags.

The created tags are displayed in the dotted box.

- e) Click **Confirm** to create the tags.
6. Click **Confirm** to create the role.

3.1.4.5 Add inherited roles to a role

Add inherited roles to a role to grant the permissions of the former to the latter.

Prerequisites

Make sure you are the owner of the current role and the inherited role to be added.

For how to query your roles, see [Query roles](#).

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Role Management > Owned Roles**.
3. At the right of the role, click **Manage**.
4. Select the **Inherited Role** tab and then click **Add Role**.
5. Search roles by **Role Name** and then select one or more roles.
6. Click **Confirm**.

3.1.4.6 Add resources to a role


You must add resources to a created role.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Role Management > Owned Roles**.
3. At the right of the role, click **Manage**.
4. Select the **Resource List** tab.
5. Click **Add Resource**.

6. Complete the configurations. For more information about the parameters, see [Parameter descriptions](#).

Table 3-1: Parameter descriptions

Parameter	Description
BID	Deployment region ID.
Product	Cloud product to be added. For example, rds. <div>  Note: The cloud product name must be lowercase. For example, enter <code>rds</code>, instead of <code>RDS</code>. </div>
Resource Path	For more information about resources of cloud products and O&M platforms, see Operation permissions of O&M platforms .
Actions	An action set, which can contain multiple actions. For operations of O&M platforms, see Operation permissions of O&M platforms .
Grant Option	Maximum number of authorizations in cascaded authorization, 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.
Memo	Description about the resource.

7. Click **Add**.

3.1.4.7 Add authorized users to a role

You can assign an existing role to users or user groups.

Prerequisites

Make sure the corresponding users or user groups are created. Users are created on the Apsara Stack console. For how to create user groups, see [Create a group](#).

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Role Management > Owned Roles**.

3. At the right of the role, click **Manage**.
4. Select the **Operator List** tab.
5. Click **Add Operator**.
6. Select the search mode and enter the corresponding information.

Four search modes are available:

- **RamAliasName**: Search in the format of *RAM username@primary account ID*. Use this mode for users who have activated Resource Access Management (RAM).
- **AliyunPk**: Search by using the unique ID of the user's cloud account.
- **AliyunId**: Search by using the logon name of the user's cloud account.
- **Group Name**: Search by group name.



Note:

You can search a single user or user group. For how to create a user group, see [Create a group](#).

7. Set the permission expiration time.

After the expiration time is reached, the user does not have the permissions of the role. To authorize the user again, the role creator must click **Renew** at the right of the authorized user under the **Operator List** tab, and then set the new expiration time.

8. Click **Add** to assign the role to the user.

To cancel the authorization, click **Remove** at the right of the authorized user under **Operator List**.

3.1.5 Manage groups

3.1.5.1 Modify group information

After creating a group, you can modify the group name and memo on the **Group Information** page.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Group Management > Owned Groups**.
3. At the right of the group, click **Manage**.
4. Click **Edit** in the upper-right corner.

5. In the displayed dialog box, modify the **Group Name** and **Memo**.
6. Click **Confirm**.

3.1.5.2 View group role details

You can view information about the inherited role, resource list, and inheritance tree of a group role.

Prerequisites

A role has been added to the group.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Group Management > Owned Groups**.
3. At the right of the group, click **Manage**.
4. In the **Role List** section, click **Detail** at the right of the role.
5. On the **Role Detail** page, you can perform the following operations:
 - Select the **Inherited Role** tab to view the information about the inherited roles.

To view detailed information about an inherited role, click **Detail** at the right of the inherited role.
 - Select the **Resource List** tab to view the resource information of the role.

To add other resources to this role, see [Add resources to a role](#).
 - Select the **Inheritance Tree** tab to view the basic information and resource information of a role and its inherited roles by using the inheritance tree on the left.

3.1.5.3 Delete a group

You can delete a group that is no longer in use as required.

Prerequisites

Make sure the group to be added does not contain members.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Group Management > Owned Groups**.
3. At the right of the group, click **Delete**.

3.1.5.4 View assigned groups

You can view the groups to which you are assigned on the **My Groups** page.

Context

You can only view the groups to which you belong, but cannot view groups of other users.

Procedure

1. [Log on to OAM](#).
2. Select **Group Management > My Groups**.
3. On the **My Groups** page, view the name, owner, memo, and modified time of the group to which you belong.

3.1.6 Manage roles

3.1.6.1 Query roles

You can view the roles that you or your group has on the **Owned Roles** page.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Role Management > Owned Roles**.
3. Select the display mode to display the roles that you or your group has.

By default, the roles that you have are displayed.

4. Optional: Enter the **Role Name**.
5. Click **Search** to search the roles that meet the search conditions.



Note:

If the role you want to query has a tag, you can click **Tag** and select the tag to search the role based on the tag.

3.1.6.2 Modify role information

After creating a role, you can modify the role information.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Role Management > Owned Roles**.
3. At the right of the role, click **Manage**.
4. Click **Edit** in the upper-right corner.

5. In the displayed dialog box, modify the name, memo, type, and tag of the role.
6. Then, click **Confirm**.

3.1.6.3 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, select **Role Management > Owned Roles**.
3. At the right of the role, click **Manage**.
4. Select the **Inheritance Tree** tab.

View the basic information and resource information of this role and its inherited roles by using the inheritance tree on the left.

3.1.6.4 Transfer roles

You can transfer roles to other groups or users as required.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Role Management > Owned Roles**.
3. Configure the search conditions and search the roles to be transferred.
4. Select one or more roles in the search results and click **Transfer**.
5. In the displayed dialog box, select the search mode, enter the corresponding information, and then click **Detail**. The user details or group details are displayed.

Four search modes are available:

- **RamAliasName**: Search in the format of *RAM username@primary account ID*. Use this mode for users who have activated Resource Access Management (RAM).
 - **AliyunPk**: Search by using the unique ID of the user's cloud account.
 - **AliyunId**: Search by using the logon name of the user's cloud account.
 - **Group Name**: Search by group name.
6. Click **Transfer** to transfer the roles to the user or group.

3.1.6.5 Delete a role

You can delete a role that is no longer in use as required.

Prerequisites

Make sure that 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, select **Role Management > Owned Roles**.
3. At the right of the role, click **Delete**.

3.1.6.6 View assigned roles

You can view the roles assigned to you and permissions granted to the roles.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Role Management > My Roles**.
3. On the **My Roles** page, you can view the name, owner, memo, modified time, and expiration time of the role assigned to you.

Click **Detail** at the right of the role to view the inherited roles, resources, and inheritance tree information of this role.

3.1.6.7 View all roles

You can view all the roles in the OAM system on the **All Roles** page.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Role Management > All Roles**.
3. On the **All Roles** page, view all the roles in the system.

You can search roles by **Role Name** on this page.

4. At the right of the role, click **Detail** to view the inherited roles, resources, and inheritance tree information of this role.

3.1.7 Search resources

You can search resources to view the roles to which the resources are assigned.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Search Resource**.
3. Enter the **Resource** and **Action** in the search boxes, and then click **Search** to search roles that meet the conditions.
4. At the right of the search result, click **Detail** to view the inherited roles, resources, and inheritance tree information of the role.

3.1.8 View personal information

You can view your personal information and perform permission tests on the **Personal Information** page.

Procedure

1. [Log on to OAM](#).
2. In the left-side navigation pane, select **Personal Information**.
3. In the **Personal Information** section, you can view your username, user type, created time, AccessKey ID, and AccessKey Secret.



Note:

Click **Display** or **Hide** to display or hide the AccessKey Secret.

4. In the **Test Access** section, test if you have a certain permission.
 - a) Enter the resource information in the **Resource** field.
 - b) Enter the permissions in the **Action** field, such as create, read, and write. Separate multiple permissions with commas (,).

3.1.9 Typical applications

3.1.9.1 Assign a default role to a user

Prerequisites

You have obtained the user ID of Alice.



Note:

Use Alice's account to log on and check the information following **User Name** on the **Personal Information** page to obtain Alice's user ID.

Context

Scenario:

Alice is the DBA of the cloud service and needs the permission to manage all database instances.

Procedure

1. Use a super administrator account to log on to the OAM system.

For how to log on to the OAM system, see [Log on to OAM](#).

2. Assign the `rds_instance administrator` role to Alice.

- a) In the left-side navigation pane, select **Role Management > Owned Roles**.
- b) At the right of the `rds_instance administrator` role, click **Manage**.
- c) Select the **Operator List** tab.
- d) Click **Add Operator**.
- e) In the displayed dialog box, select **AliyunPk** from the **Search** drop-down list and enter Alice's user ID in the search box. Then, click **Detail**.
- f) Set the expiration time.
- g) Click **Add** to assign the `rds_instance administrator` role to Alice.

3.1.9.2 Group and RoleHierarchy

Context

Scenario:

With further development of cloud computing, the database instance scale and O&M workload have significantly increased. As the DBA, Alice often needs to check the system status in RDS Operations and Maintenance System. Fortunately, Alice is recently promoted to the DBA team leader, and Bob, a senior DBA, has joined her team. Dave, a common DBA, has just been recruited. The manager hopes that Alice can control permissions of her team members by herself, saving the manager from the trouble of granting permissions to each employee while preventing system permissions from getting out of control. To achieve this, the group and RoleHierarchy functions can be used.

Procedure

1. Use a super administrator account to log on to the OAM system.

For how to log on to the OAM system, see [Log on to OAM](#).

2. Create the rds_senior DBA role.

For how to create a role, see [Create a role](#).

3. Add role hierarchy for the rds_senior DBA role to make it include the rds_instance administrator and rds_system read-only roles.

For how to add the rds_instance administrator and rds_system read-only roles to the rds_senior DBA role, see [Add inherited roles to a role](#).

4. Alice creates the Common DBA group and Senior DBA group.

a) Use Alice's account to log on to OAM.

b) Create the Common DBA group and Senior DBA group. For more information, see [Create a group](#).

5. Assign the rds_instance administrator role to the Common DBA group and assign the rds_senior DBA role to the Senior DBA group.

a) Use a super administrator account to log on to the OAM system.

b) Assign the rds_instance administrator role to the Common DBA group. For more information, see [Add group roles](#).

c) Assign the rds_senior DBA role to the Senior DBA group. For more information, see [Add group roles](#).

6. Add Alice and Bob to the Senior DBA group and add Dave to the Common DBA group.

a) Use Alice's account to log on to OAM.

b) Add Alice and Bob to the Senior DBA group. For more information, see [Add group members](#).

c) Add Dave to the Common DBA group. For more information, see [Add group members](#).

3.1.9.3 Use custom roles

Context

Carol, from the internal audit team of the company, needs to log on to the systems and view the statistical data in the RDS Operations and Maintenance System and Storage Operations and Maintenance System to check if the earlier data reports are true.

Procedure

1. Use a super administrator account to log on to the OAM system.

For how to log on to the OAM system, see [Log on to OAM](#).

2. Create the Internal audit only role. For more information, see [Create a role](#).
3. Assign RDS permissions to the Internal audit only role. The resource is 26842:rds, the action is ["HOME", "RDS_HOME"], and the grant option is 0. For more information, see [Add resources to a role](#).
4. Assign OSS permissions to the Internal audit only role. The default role OSS_public permissions meets the requirements. Therefore, add this role to the Internal audit only role as the hierarchy role.

Add the OSS_public permissions role to the Internal audit only role as an inherited role. For more information, see [Add inherited roles to a role](#).

5. Assign the Internal audit only role to Carol. For more information, see [Add authorized users to a role](#).

3.1.10 Appendix

3.1.10.1 Default roles and their functions

3.1.10.1.1 OAM default role

Role name	Role description	Resource	Actions	GrantOption
Super administrator	Root permission administrator	*.*	*	10

3.1.10.1.2 ECS Operations and Maintenance System default roles

Role name	Role description	Resource	Actions	GrantOption
ECS_administrator	ECS administrator, with all permissions	26842:ecs	["*"]	0
ECS_read-only	ECS read-only, with all read permissions	26842:ecs	["inner_getAllUrls", "inner_getCurrentUser", "inner_getAccountByIdkp", "inner_getIdkpByAccount", "inner_allE"]	0

Role name	Role description	Resource	Actions	GrantOption
			rrorCode"," inner_getOptions ","vm_describ e","vm_export ","vm_describ eMountedSn apshots"," region_des cribeRegions ","group_quer yVms"," group_queryAcIs ","group_desc ribe","disk_desc ribe","monitor_de viceIOStat"," monitor_vm Monitor"," monitor_de viceIOBlock ","monitor_de viceLatency ","nc_queryAv ailableNcs"," snapshot_d escribe"," vnc_generateUrl ","iso_queryA vailableIsos ","iso_queryM ountedIso"," image_describe"]	

3.1.10.1.3 RDS Operations and Maintenance System default roles

Role name	Role description	Resource	Actions	GrantOption
RDS_super administrator	All RDS permissions, only used for online	26842:rds	["SYSTEM_DOS AVEINSLEVEL ","SYSTEM_EDI TTEMPLATE"," SYSTEM_DOE	9

Role name	Role description	Resource	Actions	GrantOption
	initialization configuration		DITMYCNFTE MPLATE"," SYSTEM_PREF ","SYSTEM_SOF TLIST"," SYSTEM_SOF TWARE"," SYSTEM_IPF ILTER"," SYSTEM_ADD _IPFILTER"," SYSTEM_DEL ETE_IPFILTER ","BOSS_SEND ","SYSTEM_SET TING"," SYSTEM_GRO UP"," SYSTEM_FEA CHDATA"," SYSTEM_OPE RATORS"," SYSTEM_CRE ATE_OPERAT OR"," SYSTEM_TO_ UPDATE_OPE RATOR"," SYSTEM_UPD ATE_OPERAT OR"," SYSTEM_DEL ETE_OPERAT OR"," SYSTEM_GRO UP_SUBSCRI BE_WARN"," SYSTEM_NEW _LEVEL"," SYSTEM_ED IT_LEVEL"," SYSTEM_DO_	

Role name	Role description	Resource	Actions	GrantOption
			NEW_LEVEL"," SYSTEM_DO_ UPDATE_LEVEL ","SYSTEM_DO_ DELETE_LEVEL ","SYSTEM_NEW _HOST_LEVEL ","SYSTEM_EDIT _HOST_LEVEL ","SYSTEM_EDIT _GROUP"," SYSTEM_DO_ EDIT_GROUP"," SYSTEM_DO_ SAVE_HOST_ LEVEL"," SYSTEM_DO_ UPDATE_HOS T_LEVEL"," SYSTEM_DO_ DELETE_HOS T_LEVEL"," SYSTEM_WAT CH"," SYSTEM_UPL OAD_IMAGE"," SYSTEM_MOD IFY_IMAGE"," SYSTEM_MOD IFY_WATCH"," CHECK_ACCO UNT"," REFLUSH_TR ANCES_DENY ","REFLUSH_US ER_CLUSTER"," REFLUSH_US ER_ROLE"," SYSTEM_HOS TBUFFER"," SYSTEM_HOS TBUFFER_DE	

Role name	Role description	Resource	Actions	GrantOption
			LETE"," INSTANCE_S QLWALL"," INSTANCE_S QLWALLCHECK ","INSTANCE_S QLWALLCHEC KS"," INSTANCE_S QLWALLS"," REPORT_EXT RA_PURCHASE ","REPORT_EXT RA_PURCHAS E_PSOT"," INSTANCE_B AKHIS_MODIFY ","SYSTEM_CRE ATE_SITENAME ","SYSTEM_SIT ENAME"," SYSTEM_INS PERF"," DELETE_SIT ENAME_ID"," PROXY_GROU P_HOME"," PROXY_CLUS TER"," TO_CREATE_ PROXY_CLUS TER"," CREATE_PRO XY_CLUSTER ","TO_UPDATE_ PROXY_CLUS TER"," UPDATE_PRO XY_CLUSTER ","TO_CREATE_ PROXY_NODE ","CREATE_PRO	

Role name	Role description	Resource	Actions	GrantOption
			XY_NODE"," TO_UPDATE_ PROXY_NODE ","UPDATE_PRO XY_NODE"," TO_UPDATE_ PROXY_API_ NODE"," UPDATE_PRO XY_API_NODE ","DELETE_PRO XY_NODE"," DELETE_PRO XY_API_NODE"," PROXY_DETAIL ","CREATE_PRO XY_CLUSTER _GROUP"," EDIT_NODE_ TO_GROUP"," TO_EDIT_NO DE_TO_GROU P","NET_VIEW ","NET_VIEW_N ET_TIME"," COMPONENT_ OSS"," COMPONENT_ HA"," COMPONENT_ HA_LOAD"," COMPONENT_ HA_SWITCH_ RECORD"," COMPONENT_ HA_API"," COMPONENT_ HA_EXCEPTION ","COMPONENT_ SWITCH_DETAIL ","COMPONENT_ SWITCH_API	

Role name	Role description	Resource	Actions	GrantOption
			TREND"," COMPONENT BAK"," PROXY_GROU P_OFFLINE"," PROXY_GROU P_ONLINE"," PROXY_GROU P_SLB"," PROXY_GROU P_API"," SLB_VIEW"," MONITOR_HO ME"," MONITOR_DE TAIL_TYPE"," PROXY_VIEW ","MONITOR_IN DEX"," MONITOR_CR EATE_SUBSC RIBER"," MONITOR_RE MOVE_SUBSC RIBER"," SUBSCRIBER _MANAGER"," SUBSCRIBER _CREATE"," SUBSCRIBER _UPDATE"," SUBSCRIBER _DELETE"," MONITOR_ER ROR"," MONITOR_TR END_DETAIL"," CLOUD_HOME _STAT"," SYSTEM_API _MANAGE"," SYSTEM_API	

Role name	Role description	Resource	Actions	GrantOption
			_ADDKEY"," SYSTEM_API _DOADDKEY"," SYSTEM_API _DODELETEKEY ","API_ADD_EC S_IP_FILTER"," API_SHOW_E CS_IP_FILTER"," CLOUD_HOME ","CLOUD_APPL Y_POST"," CLOUD_GROU P_LIST"," CLOUD_INS_ LIST"," CLOUD_GROU P_MANAGER"," CLOUD_GROU P_CREATE"," CLOUD_DO_G ROUP_CREATE ","CLOUD_EDIT _GROUP"," CLOUD_DO_E DIT_GROUP"," CLOUD_APPL Y"," CLOUD_GROU P_ADDINS"," CLOUD_GROU P_INS"," CLOUD_GROU P_INSPROFI LE"," CLOUD_GROU P_INSTANCE _LOCK"," CLOUD_GROU P_INSTANCE _UNLOCK"," CLOUD_GROU	

Role name	Role description	Resource	Actions	GrantOption
			P_CLEARLOG"," CLOUD_GROU P_RESTART"," CLOUD_GROU P_UPDATE_A URARO"," CLOUD_GROU P_BATCH_SW ITH"," CLOUD_GROU P_DOBATCH_ SWITCH"," CLOUD_GROU P_ATTENTION ","CLOUD_MY_G ROUP_ATTEN TION"," USERGROUP_ USER_GROUP ","USERGROUP_ CREATE_USE R_GROUP"," USERGROUP_ EDIT_USER_ GROUP"," USERGROUP_ OF_EDIT_ROLE ","USERGROUP_ OF_DO_EDIT _ROLE"," USERGROUP_ OF_EDIT_CL USTER"," USERGROUP_ OF_SEARCH_ CLUSTER"," USERGROUP_ OF_DO_EDIT _CLUSTER"," USERGROUP_ OF_EDIT_INS"," USERGROUP_	

Role name	Role description	Resource	Actions	GrantOption
			OF_SEARCH_ INS"," USERGROUP_ OF_DO_EDIT _INS"," USERGROUP_ OF_EDIT_USER ","USERGROUP_ OF_SEARCH_ USER"," USERGROUP_ OF_DO_EDIT _USER"," USERGROUP_ DO_EDIT_US ER_GROUP"," USERGROUP_ DELETE_USE R_GROUP"," CUSTINS_LOGS ","DATA_SQLCO MAND"," DATA_SQLCO MAND_SHOWD ATABASE"," DATA_SQLCO MAND_EXECU TE"," DATA_SQLCO MAND_CANCEL ","TABLE_DETA IL"," COLUMN_DET AIL","HOME"," RDS_HOME"," COMPONENT_ HOME"," COMPONENT_ RGWVIEW"," COMPONENT_ PROXYVIEW"," COMPONENT_	

Role name	Role description	Resource	Actions	GrantOption
			SQLVIEW", COMPONENT_ BAKVIEW", COMPONENT_ RGW", COMPONENT_ RGWLIST", COMPONENT_ LVS", COMPONENT_ PROXY", DBS_ACCOUN TS", BAK_HIS_LIST ",BAK_OAS_FE TCH_LIST", BAK_FETCH_ OAS", SWITCH_VIP", SYSTEM_ADD MYCNFTEMPL ATE", SYSTEM_DOD ELETETEMPL ATE", BAK_REVERT", CLUSTER_HOST ",BAK_BINLOG ",BAK_HIS_SET ",BAK_HIS_RE VERT", DBBAK_CREATE ",BAK_INSTAN CE_DBS", RDS_GROUP", GROUP_FINA NCE", GROUP_CREA TE", GROUP_PROF SESSION", GROUP_ENTE	

Role name	Role description	Resource	Actions	GrantOption
			RPRISE", GROUP_ADDINS ", "GROUP_INST ANCE_GID", GROUP_COMM UNICATE", INSTANCE_D BS_LIST", INSTANCE_D ELETEDB_DB SID", INSTANCE_D BS_DETAIL", INSTANCE_D BS_CREATE", INSTANCE_C REATRREADO NLY", INSTANCE_C REATEDISAS TER", GROUP_OTHE R", GROUP_HOME ", "GROUP_INDE X", GROUP_NUMB ER", "GROUP_HA ", "GROUP_VIEW ", "GROUP_LIST ", "GROUP_HOST _LIST", GROUP_DDL", USER_INSPR OFILE", GROUP_REMO VE_INSTANCE", INSTANCE_LIST ", "INSTANCE_C HECK_PASS", INSTANCE_O WNER",	

Role name	Role description	Resource	Actions	GrantOption
			INSTANCE_A UDIT"," INSTANCE_A DDACCOUNT ","INSTANCE_A DDACCOUNT_ VIEW"," INSTANCE_A PPLY_POST"," INSTANCE_U PDATE_POST ","INSTANCE_A PPLY_PROXY _POST"," INSTANCE_A UDIT_POST"," INSTANCE_D OCREATEREA ONLY"," INSTANCE_D OCREATEDIS ASTER"," PROXY_EDIT _POST"," INSTANCE_D ETAIL"," INSTANCE_N OT_NORMAL_ DETAIL"," INSTANCE_C REATE_NOT_ NORMAL"," INSTANCE_E DIT_NOT_NO RMAL"," INSTANCE_D O_EDIT_NOT _NORMAL"," INSTANCE_D ELETE_NOT_ NORMAL"," SWITCH_GUA	

Role name	Role description	Resource	Actions	GrantOption
			RD"," DO_SWITCH_ GUARD"," INSTANCE_DBS ","INSTANCE_D ELETE"," INSTANCE_C REATEBAKRE ADONLYINS"," INSTANCE_M ANAGE_POST ","INSTANCE_I NS_TASK"," INSTANCE_D IAGONSE"," INSTANCE_T RANS_CLUST ERS"," INSTANCE_Z ONE_CLUSTE RS"," INSTANCE_M AGAGE_INS"," INSTANCE_C USTLINK_INS ","INSTANCE_A UDIT_INS"," INSTANCE_E DIT_INS"," INSTANCE_I NTIME_INS"," INSTANCE_K ILL_SESSION ","INSTANCE_P ROXY_LINK"," INSTANCE_D IAGNOSE"," INSTANCE_S TATUS"," INSTANCE_C ONFIG_INS"," INSTANCE_P	

Role name	Role description	Resource	Actions	GrantOption
			REF_INS"," INSTANCE_UPDATE_CONFIG ","INSTANCE_EXPLAIN_INS"," INSTANCE_EXCEPTION_INS ","MONITOR_EXCEPTION_DELETE"," MONITOR_EXCEPTION_UPDATE"," INSTANCE_EXCEPTION_INS_BATCH"," EXCEPTION_UPDATE"," EXCEPTION_BATCHUPDATE ","INSTANCE_MAGAGE_HOST ","INSTANCE_HA_LOGGER"," INSTANCE_SLOW"," INSTANCE_REPORT"," INSTANCE_REPORT_RPT"," INSTANCE_ACCOUNT"," INSTANCE_OPENPAGE"," INSTANCE_LOCK"," INSTANCE_ACCOUNT_LIST"," DBS_ACCOUNT_LIST"," ACCOUNT_LIST ","DBS_LIST","	

Role name	Role description	Resource	Actions	GrantOption
			DBS_NEWACC OUNT"," DBS_ACCOUN T_CONFIG"," DBS_ACCOUN T_PROXY_INFO ","DO_DBS_ACC OUNT_CONFIG ","DBS_ACCOUN T_CHANGE_P ASSWORD"," DO_DBS_ACC OUNT_CHANG E_PASSWORD ","DBS_ACCOUN T_RESET_PA SSWORD"," DO_DBS_ACC OUNT_RESET _PASSWORD"," DBS_ACCOUN T_DELETE"," ADD_DBS_AC COUNT"," TRANS_DBS"," DBS_MODIFY PRIVILEGE"," INSTANCE_U NLOCK"," INSTANCE_C ONFIG_PROXY ","INSTANCE_C ONFIG_SYNC ","INSTANCE_R ESTART"," INSTANCE_C LEARLOG"," INSTANCE_C HANGE"," DBS_ACCOUNT ","INSTANCE_B ACKUP","	

Role name	Role description	Resource	Actions	GrantOption
			INSTANCE_B ACKUP_CREA TE"," INSTANCE_B ACKUP_UPDA TE"," INSTANCE_R EBUILD_HA"," INSTANCE_A PPLY"," INSTANCE_C ONFIGSQLWALL ","INSTANCE_M ULTITRANS"," INSTANCE_D OMULTITRANS ","INSTANCE_C ONFIGPROXY MODE"," INSTANCE_P ASS"," INSTANCE_U NPASS"," INSTANCE_D BCONFIG"," INSTANCE_T UNE"," SQL_DETAIL"," SLOWSQL_DE TAIL"," INSTANCE_S QL_SLOW_LOG ","SLOWLOG_DE TAIL"," MONITOR_WO RNING_DETAIL ","INSTANCE_L OG"," INSTANCE_T RANS"," TRANS_AUDIT"," WARN_MANAG	

Role name	Role description	Resource	Actions	GrantOption
			ER_THRESHO LD", " WARN_MANAG ER_CREATE_ CONTACT", " WARN_MANAG ER_UPDATE_ THRESHOLD", " WARN_MANAG ER_DELETE_ CONTACTS", " INSTANCE_S WITCH_INST ANCE", " INSTANCE_O PARATOR_PE RMISSION", " INSTANCE_L OG_PAGE", " INSTANCE_B ATCH_APPLY ", "INSTANCE_P ROXYLIST", " INSTANCE_S WITCHLINK", " COMPONENT_ SLB_CLUSTER ", "COMPONENT_ RDS_CLUSTER ", "PROXY_TO_U SE_NODE_TE MPLATE", " PROXY_USE_ NODE_TEMPL ATE", " PROXY_TO_U SE_NODE_TE MPLATE", " TO_EDIT_NO DE_TO_GROUP ", "EDIT_NODE_ TO_GROUP", " 	

Role name	Role description	Resource	Actions	GrantOption
			PROXY_USE_ NODE_TEMPL ATE"," SYSTEM_EXC EPTION_LEVEL ","SYSTEM_MOD IFY_EXCEPT ION_LEVEL"," INSTANCE_D O_SWITCHLINK ","HOST_BAKIN FO"," HOST_RTTIME ","CONNECTIVE TY_CHECK"," CONNECTIVE TY_REGION_ DATA"," COMPONENT_ INS_LIST"," CONNECTIVE TY_MAIL"," REFLUSH_AV ZONE_LIST"," INSTANCE_T RANS_UPGRA DE"," INSTANCE_M ULTITRANS_ NEW"," INSTANCE_D OMULTITRAN S_NEW"," TASK_EDIT_ PENGINE_CO NTENT"," REFLUSH_US ERINFO"," DATA_SQLCO MAND"," RESOURCE_O Verview","	

Role name	Role description	Resource	Actions	GrantOption
			HOST_BIANQUE ","COMPONENT_ CUSTINS_NO TEQUEL_SIT ENAME_WITH _SLB"," GROUP_INST ANCE_THRES HOLD"," INSTANCE_M ULTIUPGRADE ","INSTANCE_D OMULTIUPGR ADE"," INSTANCE_D OMULTIUPGR ADE"," INSTANCE_D O_BATCH_HA SWITCH "," INSTANCE_D O_BATCH_HA SWITCH"," CUSTINS_DA TA_LINK"," INSTANCE_M ULTIREFRESH ","INSTANCE_M YSQL_OPERATE ","HOST_INTIME ","INSTANCE_M YSQL_OPERATE ","INSTANCE_U PLOAD_POLI CY"," HOST_RESTART ","ROBOT_LOG ","ROBOT_ROBO T","INSTANCE_M YSQL_SPACE"," INSTANCE_SLA ","INSTANCE_B	

Role name	Role description	Resource	Actions	GrantOption
			ATCH_VERSI ON_UPGRADE ", "HOST_OPERA TE", "TASK_INFO ", "OS_CONFIG ", "UPDATE_OS_ CONFIG", " RESOURCE_S CHEDULE", " OPERATE_WA TCH", " COMPONENT_ SLB_CHECK", " CUSTINS_PA NORAMA", " SYSTEM_CLU STER_CONFIG ", "TABLE_ALTER ", "RDS_SCHEMA _SQL", " POWER_TEST ", "NODE_ADD ", "INSTANCE_F CS_DELETE", " PROXY_CONFIG ", "MIGRATE_CR EATE", " SYSTEM_BU", " ROBOT_TASK _STATISTICS", " CREATE_SPE CIAL_ACCOUNT ", "COMPONENT_ INCONSIST", " COMPONENT_ INCONSIST_ READONLY", " RDS_DATA", " RESOURCE_B USINESS", " HOST_COMMA ND", " 	

Role name	Role description	Resource	Actions	GrantOption
			CREATE_SUP ER_ACCOUNT ", "INSTANCE_B ATCH_PRE_S UPER_PERMI SSION", " PACKAGE_SP EC_OPERATION ", "TASK_TRACE ", "INSTANCE_M ULBAKREBUILD ", "HOST_BATCH _DO_BAK_RE BUILD", " SYSTEM_DUK ANG_CONFIG ", "INSTANCE_O PENSSL", " INSTANCE_C ONFIG_INS_OP ", "BAK_HIS_LI ST_FETCH", " ACCESS_GRA NTACCOUNT ", "INSTANCE_B ATCH_HASWITH ", "COMPONENT_ AUTOTEST", " INSTANCE_R ESET_PASSW ORD", " INSTANCE_T RANS_UPDATE ", "INSTANCE_T RANS_CANCEL ", "INSTANCE_T RANS_APPLY ", "INSTANCE_T RANS_APPLY POST", " INSTANCE_T RANS_CHECK	

Role name	Role description	Resource	Actions	GrantOption
			POST"," INSTANCE_T RANS_DBPOST ","INSTANCE_T RANS_DB"," INSTANCE_T RANS_OPENP AGE"," GET_INSTAN CE_TRANS_H OST"," GET_INSTAN CE_TRANS_C USTINS"," GET_INSTAN CE_TRANS_DB ","INSTANCE_U PDATECONFIG ","INSTANCE_U PDATE_AURA RO"," CLUSTER_LIST ","USSER_PROF ILE_LIST"," USSER_PROF ILE_ALL_LIST ","USSER_ALIY UN_INFO"," CLUSTER_NEW ","CLUSTER_ER ROR"," ERROR_RE_S UBMIT"," CLUSTER_UP CONIFG"," CLUSTER_NO DELIST"," CLUSTER_NO DE"," CLUSTER_ED ITNODE"," CREATE_NOD	

Role name	Role description	Resource	Actions	GrantOption
			E"," UPDATE_NODE ","CLUSTER_CR EATE"," CLUSTER_FL USHWHITE"," FLUSH_SYNC _MODE"," FLUSH_RESO URCE"," CHECK_INSN AME"," CHECK_CONN ADDRCUST"," DEL_NODE_ID ","DEL_CLUSTE R_ID"," FETCH_BAK_ URL"," FETCH_BAK_ BINLOG_URL"," CHECK_DBNA ME"," EXCEPTION_ HOME"," EXCEPTION_ LIST"," RESOURCE_H OME"," HOST_CONFIG ","HOST_UPCON FIG"," RESOURCE_R EGION"," RESOURCE_M ORE"," HOST_CREATE ","HOST_UPDAT E"," RESOURCE_HA ","RESOURCE_H OSTBUFFER","	

Role name	Role description	Resource	Actions	GrantOption
			RESOURCE_H OST"," RESOURCE_IP ","RESOURCE_S ERVICE"," RESOURCE_B AKOWNER_TY PE"," RESOURCE_C REATE_BAKO WNER_TYPE"," RESOURCE_D ELETE_BAKO WNER_TYPE"," RESOURCE_E DIT_BAKOWN ER_TYPE"," RESOURCE_U PDATE_BAKO WNER_TYPE"," CLUSTER_UP DATERES"," LOGGER_HOME ","LOGGER_USE R","LOGGER_HA ","LOGGER_TRA NS"," LOGGER_REC OVER"," LOGGER_REM OTE"," LOGGER_BAC KUP"," LOGGER_API ","INSTANCE_A PILOG"," INSTANCE_A DMINLOG"," LOGGER_RES OURCE"," HOST_HOME"," HOST_INSPREF	

Role name	Role description	Resource	Actions	GrantOption
			", "HOST_SWITCH ", "HOST_BATCH _SWITH", " HOST_BATCH _TRANS_INS", " HOST_PREF", " HOST_INFO", " HOST_INSTA NCE", " HOST_NEW", " HOST_DOSWI TCH", " HOST_TASK", " HOST_TASKS", " HOST_DOBAT CH_SWITCH", " HOST_DOBAT CH_TRANS_INS ", "HOST_EDIT ", "HOST_PREF_ DEATIL", " HOST_DELET E_HOSTID", " HOST_CHECK _HOSTID", " INS_PREF_D EATIL", " CUST_PREF_ DEATIL", " TASK_HOME", " TASK_FAIL", " TRANCE_LIST ", "TASK_RUN", " TASK_STEP", " TASK_CLOSE", " TASK_START", " TASK_FLOW", " TASK_STAT", " TASK_FLOWE XE", " TASK_HISTORY ", "TASK_LOOGE	

Role name	Role description	Resource	Actions	GrantOption
			R"," REPORT_HOME ","REPORT_CLU STER"," REPORT_ZONE ","RESOURCE_H OSTINFO"," RESOURCE_V IPINFO"," REPORT_REG IONNAME"," USER_DELETE ","ROLE_DELET E","DRC_HOME ","DRC_PRECHE CK"," DRC_PRESCH ECK"," DRC_COMMIT ","DRC_LIST"," CHECK_HOME ","SYSTEM_HOM E"," SYSTEM_USER ","SYSTEM_INS IDC"," SYSTEM_INS IDC_LSIT"," SYSTEM_MEA SUREDATA"," SYSTEM_COU NTDATA"," SYSTEM_BOSS ","SYSTEM_PER MISSION"," SYSTEM_UPD ATEPERMISS ION"," SYSTEM_UPD ATEROLE"," SYSTEM_TAN CEDENCY","	

Role name	Role description	Resource	Actions	GrantOption
			SYSTEM_CFR EATE_TANCE DENCY"," SYSTEM_REG ION"," SYSTEM_CFR EATE_REGION ","DELETE_REG ION_ID"," SYSTEM_DEL ETE_TANCED ENCY"," SYSTEM_CRE ATE_HOSTBU FFERSN"," SYSTEM_CRE ATEROLE"," SYSTEM_CRE ATEPERMISS ION"," USER_UPDAT E_ROLE"," USER_UPDAT E_CLUSTER"," GET_INSTAN CE_LEVEL"," ROLE_LIST"," ROLE_NEW"," PERMISSION _NEW"," ROLE_UPDATE ","USER_ROLE_ EDIT"," USER_ADD_R OLECLUSTER"," USER_ADD_R ESOURCE"," SYSTEM_DEL ETE_RESOUR CE"," USER_UPDAT E_RESOURCE","	

Role name	Role description	Resource	Actions	GrantOption
			SYSTEM_SALES ", "INSLEVEL_P ARAMS", " INSLEVEL_A DDPARAMS", " SYSTEM_TEM PLATE", " SYSTEM_NEW TEMPLATE"]	
RDS_instance read-only	RDS end user - instance level - external acceptance	26842:rds	["LOGGER_API ", "INSTANCE_A PILOG", " INSTANCE_A DMINLOG", " LOGGER_RES OURCE", " HOST_HOME", " HOST_INSPREF ", "HOST_PREF ", "INS_PREF_D EATIL", " CUST_PREF_ DEATIL", " TASK_HOME", " TASK_FAIL", " TRANCE_LIST ", "TASK_RUN ", "TASK_STEP ", "TASK_HISTO RY", " REPORT_HOME ", "REPORT_CLU STER", " REPORT_ZONE ", "RESOURCE_H OSTINFO", " RESOURCE_V IPINFO", " DATA_SQLCO MAND", " DATA_SQLCO MAND_SHOWD	0

Role name	Role description	Resource	Actions	GrantOption
			ATABASE"," DATA_SQLCO MAND_EXECU TE"," DATA_SQLCO MAND_CANCEL ","INSTANCE_S WITCH_INST ANCE"," GROUP_INST ANCE_VIEW_ WARN"," INSTANCE_L OG_PAGE"," RESOURCE_O VERVIEW"," INSTANCE_M YSQL_SPACE ","CUSTINS_PA NORAMA"," TABLE_ALTER ","CREATE_SUP ER_ACCOUNT ","HOME"," COMPONENT_ BAKVIEW"," COMPONENT_ RGW"," COMPONENT_ PROXY"," DBS_ACCOUN TS"," BAK_HIS_LIST ","BAK_OAS_FE TCH_LIST"," BAK_FETCH_ OAS"," SWITCH_VIP"," BAK_BINLOG"," INSTANCE_D BS_LIST"," INSTANCE_D	

Role name	Role description	Resource	Actions	GrantOption
			ELETEDB_DB SID"," INSTANCE_D BS_DETAIL"," INSTANCE_D BS_CREATE"," INSTANCE_C REATRREADO NLY"," INSTANCE_C REATEDISAS TER"," GROUP_HOME "," GROUP_NUMB ER","GROUP_HA ","GROUP_LIST ","GROUP_HOST _LIST"," GROUP_DDL"," USER_INSPR OFILE"," GROUP_REMO VE_INSTANCE"," INSTANCE_LIST ","INSTANCE_C HECK_PASS"," INSTANCE_O WNER"," INSTANCE_A DDACCOUNT ","INSTANCE_A DDACCOUNT_ VIEW"," INSTANCE_A PPLY_POST"," INSTANCE_U PDATE_POST ","INSTANCE_A PPLY_PROXY _POST"," INSTANCE_D	

Role name	Role description	Resource	Actions	GrantOption
			OCREATEREA ONLY"," INSTANCE_D OCREATEDIS ASTER"," PROXY_EDIT _POST"," INSTANCE_D ETAIL"," INSTANCE_N OT_NORMAL_ DETAIL"," INSTANCE_E DIT_NOT_NO RMAL"," INSTANCE_D O_EDIT_NOT _NORMAL"," INSTANCE_D ELETE_NOT_ NORMAL"," SWITCH_GUA RD"," DO_SWITCH_ GUARD"," INSTANCE_DBS ","INSTANCE_D ELETE"," INSTANCE_C REATEBAKRE ADONLYINS"," INSTANCE_M ANAGE_POST ","INSTANCE_I NS_TASK"," INSTANCE_D IAGONSE"," INSTANCE_T RANS_CLUST ERS"," INSTANCE_Z ONE_CLUSTE	

Role name	Role description	Resource	Actions	GrantOption
			RS", INSTANCE_C USTLINK_INS ", "INSTANCE_E DIT_INS", INSTANCE_I NTIME_INS", INSTANCE_K ILL_SESSION ", "INSTANCE_P ROXY_LINK", INSTANCE_D IAGNOSE", INSTANCE_S TATUS", INSTANCE_C ONFIG_INS", INSTANCE_P REF_INS", INSTANCE_E XPLAIN_INS", INSTANCE_E XCEPTION_INS ", "MONITOR_EX CEPTION_DE LETE", MONITOR_EX CEPTION_UP DATE", INSTANCE_E XCEPTION_I NS_BATCH", EXCEPTION_ UPDATE", EXCEPTION_ BATCHUPDATE ", "INSTANCE_M AGAGE_HOST ", "INSTANCE_H A_LOGGER", INSTANCE_S LOW",	

Role name	Role description	Resource	Actions	GrantOption
			INSTANCE_R EPORT"," INSTANCE_R EPORT_RPT"," INSTANCE_A CCOUNT"," INSTANCE_L OCK"," INSTANCE_A CCOUNT_LIST"," DBS_ACCOUN T_LIST"," ACCOUNT_LIST ","DBS_LIST"," DBS_NEWACC OUNT"," DBS_ACCOUN T_CONFIG"," DBS_ACCOUN T_PROXY_INFO ","DO_DBS_ACC OUNT_CONFIG ","DBS_ACCOUN T_CHANGE_P ASSWORD"," DO_DBS_ACC OUNT_CHANG E_PASSWORD ","DBS_ACCOUN T_RESET_PA SSWORD"," DO_DBS_ACC OUNT_RESET _PASSWORD"," DBS_ACCOUN T_DELETE"," ADD_DBS_AC COUNT"," TRANS_DBS"," DBS_MODIFY PRIVILEGE"," INSTANCE_U	

Role name	Role description	Resource	Actions	GrantOption
			NLOCK"," INSTANCE_C ONFIG_PROXY ","INSTANCE_C ONFIG_SYNC ","INSTANCE_R ESTART"," INSTANCE_C LEARLOG"," INSTANCE_C HANGE"," DBS_ACCOUNT ","INSTANCE_B ACKUP"," INSTANCE_B ACKUP_CREA TE"," INSTANCE_B ACKUP_UPDA TE"," INSTANCE_R EBUILD_HA"," INSTANCE_A PPLY"," INSTANCE_C ONFIGSQLWALL ","INSTANCE_M ULTITRANS"," INSTANCE_D OMULTITRANS ","INSTANCE_C ONFIGPROXY MODE"," INSTANCE_P ASS"," INSTANCE_U NPASS"," INSTANCE_T UNE"," SQL_DETAIL"," SLOWSQL_DE TAIL","	

Role name	Role description	Resource	Actions	GrantOption
			INSTANCE_S QL_SLOW_LOG ", "SLOWLOG_DE TAIL", " MONITOR_WO RNING_DETAIL ", "INSTANCE_L OG", " INSTANCE_T RANS", " INSTANCE_T RANS_DETAIL ", "INSTANCE_T RANS_UPDATE ", "INSTANCE_T RANS_CANCEL ", "INSTANCE_T RANS_CHECK POST", " INSTANCE_T RANS_DBPOST ", "INSTANCE_T RANS_DB", " INSTANCE_T RANS_OPENP AGE", " GET_INSTAN CE_TRANS_H OST", " GET_INSTAN CE_TRANS_C USTINS", " GET_INSTAN CE_TRANS_DB ", "INSTANCE_U PDATECONFIG ", "INSTANCE_U PDATE_AURA RO", " CLUSTER_LIST ", "USSER_PROF ILE_LIST", " 	

Role name	Role description	Resource	Actions	GrantOption
			USSER_PROF ILE_ALL_LIST ", "USSER_ALIY UN_INFO", " ERROR_RE_S UBMIT", " FLUSH_SYNC _MODE", " FLUSH_RESO URCE", " CHECK_INSN AME", " CHECK_CONN ADDR_CUST", " DEL_NODE_ID ", "DEL_CLUSTE R_ID", " FETCH_BAK_ URL", " FETCH_BAK_ BINLOG_URL", " CHECK_DBNA ME", " EXCEPTION_ HOME", " EXCEPTION_ LIST", " RESOURCE_H OME", " RESOURCE_R EGION", " RESOURCE_M ORE", " RESOURCE_HA ", "RESOURCE_H OSTBUFFER", " LOGGER_REC OVER", " LOGGER_REM OTE"]	
RDS_system read-only	RDS end user - system level	26842:rds	["RESOURCE_B AKOWNER_TY	0

Role name	Role description	Resource	Actions	GrantOption
	- external acceptance		PE"," LOGGER_HOME ","LOGGER_USE R","LOGGER_HA ","LOGGER_TRA NS"," LOGGER_REC OVER"," LOGGER_REM OTE"," LOGGER_BAC KUP"," LOGGER_API ","INSTANCE_A PILOG"," INSTANCE_A DMINLOG"," LOGGER_RES OURCE"," HOST_HOME"," HOST_INSPREF ","HOST_SWITH ","HOST_BATCH _SWITH"," HOST_BATCH _TRANS_INS"," HOST_PREF"," HOST_INFO"," HOST_INSTA NCE"," HOST_NEW"," HOST_TASK"," HOST_TASKS ","HOST_PREF_ DEATIL"," HOST_CHECK _HOSTID"," INS_PREF_D EATIL"," CUST_PREF_ DEATIL"," TASK_HOME","	

Role name	Role description	Resource	Actions	GrantOption
			TASK_FAIL"," TRANCE_LIST ","TASK_RUN"," TASK_STEP"," TASK_CLOSE"," TASK_START"," TASK_FLOW"," TASK_STAT"," TASK_FLOWE XE"," TASK_HISTORY ","TASK_LOOGE R"," REPORT_HOME ","REPORT_CLU STER"," REPORT_ZONE ","RESOURCE_H OSTINFO"," RESOURCE_V IPINFO"," REPORT_REG IONNAME"," DRC_HOME"," DRC_PRECHE CK"," DRC_PRESCH ECK"," DRC_COMMIT ","DRC_LIST"," CHECK_HOME ","SYSTEM_HOM E"," SYSTEM_USER ","SYSTEM_INS IDC"," SYSTEM_INS IDC_LSIT"," SYSTEM_MEA SUREDATA"," SYSTEM_COU NTDATA","	

Role name	Role description	Resource	Actions	GrantOption
			SYSTEM_BOSS ","SYSTEM_PER MISSION"," SYSTEM_TAN CEDENCY"," SYSTEM_CFR EATE_TANCE DENCY"," SYSTEM_REG ION"," SYSTEM_CFR EATE_REGION ","GET_INSTAN CE_LEVEL"," ROLE_LIST"," ROLE_NEW"," PERMISSION _NEW"," SYSTEM_SALES ","INSLEVEL_P ARAMS"," SYSTEM_TEM PLATE"," SYSTEM_NEW TEMPLATE"," SYSTEM_PREF ","SYSTEM_SOF TLIST"," SYSTEM_SOF TWARE"," SYSTEM_IPF ILTER"," BOSS_SEND"," SYSTEM_SET TING"," SYSTEM_GRO UP"," SYSTEM_FEA CHDATA"," SYSTEM_OPE RATORS"," SYSTEM_GRO	

Role name	Role description	Resource	Actions	GrantOption
			UP_SUBSCRI BE_WARN"," SYSTEM_NEW _LEVEL"," SYSTEM_NEW _HOST_LEVEL ","SYSTEM_WAT CH"," SYSTEM_UPL OAD_IMAGE"," SYSTEM_MOD IFY_IMAGE"," SYSTEM_MOD IFY_WATCH"," CHECK_ACCO UNT"," REFLUSH_TR ANCES_DENY ","REFLUSH_US ER_CLUSTER"," REFLUSH_US ER_ROLE"," SYSTEM_HOS TBUFFER"," INSTANCE_S QLWALL"," INSTANCE_S QLWALLCHECK ","INSTANCE_S QLWALLCHEC KS"," INSTANCE_S QLWALLS"," REPORT_EXT RA_PURCHASE ","REPORT_EXT RA_PURCHAS E_PSOT"," INSTANCE_B AKHIS_MODIFY ","SYSTEM_SIT ENAME","	

Role name	Role description	Resource	Actions	GrantOption
			SYSTEM_INS PERF"," PROXY_GROU P_HOME"," PROXY_CLUS TER"," PROXY_DETA IL","NET_VIEW ","NET_VIEW_N ET_TIME"," COMPONENT_ OSS"," COMPONENT_ HA"," COMPONENT_ HA_LOAD"," COMPONENT_ HA_SWITCH_ RECORD"," COMPONENT_ HA_API"," COMPONENT_ HA_EXCEPTION ","COMPONENT_ SWITCH_DETAIL ","COMPONENT_ SWITCH_API _TREND"," COMPONENT_ BAK"," PROXY_GROU P_SLB"," PROXY_GROU P_API"," SLB_VIEW"," MONITOR_HO ME"," MONITOR_DE TAIL_TYPE"," PROXY_VIEW ","MONITOR_IN DEX","	

Role name	Role description	Resource	Actions	GrantOption
			SUBSCRIBER_MANAGER"," MONITOR_ERROR"," MONITOR_TREND_DETAIL"," CLOUD_HOME_STAT"," SYSTEM_API_MANAGE"," API_SHOW_ERROR_IP_FILTER"," CLOUD_HOME","CLOUD_APPLY_POST"," CLOUD_GROUP_LIST"," CLOUD_INSTANCE_LIST"," CLOUD_GROUP_MANAGER"," CLOUD_APPLY"," CLOUD_GROUP_INS"," CLOUD_GROUP_INSPROFILE"," CLOUD_GROUP_CLEARLOG"," CLOUD_GROUP_RESTART"," CLOUD_GROUP_BATCH_SWITCH"," CLOUD_GROUP_ATTENTION","CLOUD_MY_GROUP_ATTENTION"," USERGROUP_USER_GROUP	

Role name	Role description	Resource	Actions	GrantOption
			", "USERGROUP_ OF_SEARCH_ CLUSTER", " USERGROUP_ OF_SEARCH_ INS", " USERGROUP_ OF_SEARCH_ USER", " CUSTINS_LOGS ", "DATA_SQLCO MAND", " DATA_SQLCO MAND_SHOWD ATABASE", " DATA_SQLCO MAND_EXECU TE", " DATA_SQLCO MAND_CANCE L", "HOME", " RDS_HOME", " COMPONENT_ HOME", " COMPONENT_ RGWVIEW", " COMPONENT_ PROXYVIEW", " COMPONENT_ SQLVIEW", " COMPONENT_ BAKVIEW", " COMPONENT_ RGW", " COMPONENT_ RGWLIST", " COMPONENT_ LVS", " COMPONENT_ PROXY", " DBS_ACCOUN TS", " 	

Role name	Role description	Resource	Actions	GrantOption
			BAK_HIS_LIST ",BAK_OAS_FET TCH_LIST", BAK_FETCH_ OAS", SWITCH_VIP", BAK_REVERT", CLUSTER_HOST ",BAK_BINLOG ",BAK_HIS_SET ",BAK_HIS_RE VERT", BAK_INSTAN CE_DBS", RDS_GROUP", GROUP_FINA NCE", GROUP_PROF ESSION", GROUP_ENTE RPRISE", GROUP_INST ANCE_GID", GROUP_COMM UNICATE", INSTANCE_D BS_LIST", INSTANCE_D BS_DETAIL", GROUP_OTHE R", GROUP_HOME ",GROUP_INDE X", GROUP_NUMB ER",GROUP_HA ",GROUP_VIEW ",GROUP_LIST ",GROUP_HOST _LIST", GROUP_DDL", USER_INSPR	

Role name	Role description	Resource	Actions	GrantOption
			OFFILE", INSTANCE_LIST ", "INSTANCE_C HECK_PASS", INSTANCE_O WNER", INSTANCE_A PPLY_POST", INSTANCE_A PPLY_PROXY _POST", INSTANCE_A UDI_POST", INSTANCE_D ETAIL", INSTANCE_N OT_NORMAL_ DETAIL", SWITCH_GUA RD", INSTANCE_DBS ", "INSTANCE_M ANAGE_POST ", "INSTANCE_I NS_TASK", INSTANCE_D IAGONSE", INSTANCE_T RANS_CLUST ERS", INSTANCE_Z ONE_CLUSTE RS", INSTANCE_M AGAGE_INS", INSTANCE_C USTLINK_INS ", "INSTANCE_A UDI_INS", INSTANCE_I NTIME_INS", INSTANCE_K	

Role name	Role description	Resource	Actions	GrantOption
			ILL_SESSION ", "INSTANCE_P ROXY_LINK", " INSTANCE_D IAGNOSE", " INSTANCE_S TATUS", " INSTANCE_C ONFIG_INS", " INSTANCE_P REF_INS", " INSTANCE_E XPLAIN_INS", " INSTANCE_E XCEPTION_INS ", "INSTANCE_E XCEPTION_I NS_BATCH", " INSTANCE_M AGAGE_HOST ", "INSTANCE_H A_LOGGER", " INSTANCE_S LOW", " INSTANCE_R EPORT", " INSTANCE_R EPORT_RPT", " INSTANCE_A CCOUNT", " INSTANCE_O PENPAGE", " INSTANCE_A CCOUNT_LIST", " DBS_ACCOUN T_LIST", " ACCOUNT_LIST ", "DBS_LIST", " DBS_NEWACC OUNT", " DBS_ACCOUN T_CONFIG", " 	

Role name	Role description	Resource	Actions	GrantOption
			DBS_ACCOUNT_PROXY_INFO ", "DBS_ACCOUNT_PROXY_CHANGE_PASSWORD", " DBS_ACCOUNT_RESET_PASSWORD", " TRANS_DB", " DBS_MODIFY_PRIVILEGE", " INSTANCE_CONFIG_PROXY ", "INSTANCE_CONFIG_SYNC ", "INSTANCE_RESTART", " INSTANCE_LEARNLOG", " INSTANCE_CHANGE", " DBS_ACCOUNT_INSTANCE_BACKUP", " INSTANCE_REBUILD_HA", " INSTANCE_APPLY", " INSTANCE_CONFIGSQLWALL ", "INSTANCE_MULTITRANS", " INSTANCE_CONFIGPROXY MODE", " INSTANCE_PASS", " INSTANCE_UNPASS", " INSTANCE_TUNE", " SQL_DETAIL", " 	

Role name	Role description	Resource	Actions	GrantOption
			SLOWSQL_DE TAIL"," INSTANCE_S QL_SLOW_LOG ","SLOWLOG_DE TAIL"," MONITOR_WO RNING_DETAIL ","INSTANCE_L OG"," INSTANCE_T RANS"," TRANS_AUDIT ","INSTANCE_T RANS_DETAIL ","INSTANCE_T RANS_CANCEL ","INSTANCE_T RANS_APPLY ","INSTANCE_T RANS_APPLY POST"," INSTANCE_T RANS_CHECK POST"," INSTANCE_T RANS_DBPOST ","INSTANCE_T RANS_DB"," INSTANCE_T RANS_OPENP AGE"," GET_INSTAN CE_TRANS_H OST"," GET_INSTAN CE_TRANS_C USTINS"," GET_INSTAN CE_TRANS_DB ","CLUSTER_LI ST","	

Role name	Role description	Resource	Actions	GrantOption
			USSER_PROF ILE_LIST"," USSER_PROF ILE_ALL_LIST ","USSER_ALIY UN_INFO"," CLUSTER_NEW ","CLUSTER_ER ROR"," ERROR_RE_S UBMIT"," CLUSTER_UP CONIFG"," CLUSTER_NO DELIST"," CLUSTER_NO DE"," CLUSTER_FL USHWHITE"," FLUSH_SYNC _MODE"," FLUSH_RESO URCE"," CHECK_INSN AME"," DEL_NODE_ID ","DEL_CLUSTE R_ID"," FETCH_BAK_ URL"," FETCH_BAK_ BINLOG_URL"," CHECK_DBNA ME"," EXCEPTION_ HOME"," EXCEPTION_ LIST"," RESOURCE_H OME"," HOST_CONFIG ","HOST_UPCON	

Role name	Role description	Resource	Actions	GrantOption
			FIG"," RESOURCE_R EGION"," RESOURCE_M ORE"," RESOURCE_HA ","RESOURCE_H OSTBUFFER"," RESOURCE_H OST"," RESOURCE_IP ","COLUMN_DET AIL"," WARN_MANAG ER_CONTACT S"," WARN_MANAG ER_THRESHO LD"," HOST_BAKIN FO"," HOST_RTIME"," ROBOT_LOG"," ROBOT_ROBOT ","TABLE_ALTER ","ROBOT_TASK _STATISTICS"," CREATE_SUP ER_ACCOUNT"]	
RDS_instance administrator	RDS DBA - instance level - cannot perform operations on cluster and host information	26842:rds	["HOME"," COMPONENT_ RGW"," COMPONENT_ RGWLIST"," COMPONENT_ PROXY"," DBS_ACCOUN TS"," BAK_HIS_LIST ","BAK_OAS_FE TCH_LIST"," BAK_FETCH_	0

Role name	Role description	Resource	Actions	GrantOption
			OAS"," SWITCH_VIP"," BAK_BINLOG"," INSTANCE_D BS_LIST"," INSTANCE_D ELETEDB_DB SID"," INSTANCE_D BS_DETAIL"," INSTANCE_D BS_CREATE"," INSTANCE_C REATRREADO NLY"," INSTANCE_C REATEDISAS TER"," GROUP_HOME "," GROUP_NUMB ER","GROUP_HA ","GROUP_LIST ","GROUP_HOST _LIST"," GROUP_DDL"," USER_INSPR OFILE"," GROUP_REMO VE_INSTANCE"," INSTANCE_LIST ","INSTANCE_C HECK_PASS"," INSTANCE_O WNER"," INSTANCE_A DDACCOUNT ","INSTANCE_A DDACCOUNT_ VIEW"," INSTANCE_U PDATE_POST	

Role name	Role description	Resource	Actions	GrantOption
			", "INSTANCE_D OCREATEREA ONLY", " INSTANCE_D OCREATEDIS ASTER", " PROXY_EDIT _POST", " INSTANCE_D ETAIL", " INSTANCE_N OT_NORMAL_ DETAIL", " INSTANCE_C REATE_NOT_ NORMAL", " INSTANCE_E DIT_NOT_NO RMAL", " INSTANCE_D O_EDIT_NOT _NORMAL", " INSTANCE_D ELETE_NOT_ NORMAL", " SWITCH_GUA RD", " DO_SWITCH_ GUARD", " INSTANCE_DBS ", "INSTANCE_D ELETE", " INSTANCE_C REATEBAKRE AONLYINS", " INSTANCE_M ANAGE_POST ", "INSTANCE_I NS_TASK", " INSTANCE_D IAGONSE", " INSTANCE_T	

Role name	Role description	Resource	Actions	GrantOption
			RANS_CLUST ERS"," INSTANCE_Z ONE_CLUSTER RS"," INSTANCE_C USTLINK_INS ","INSTANCE_E DIT_INS"," INSTANCE_I NTIME_INS"," INSTANCE_K ILL_SESSION ","INSTANCE_P ROXY_LINK"," INSTANCE_D IAGNOSE"," INSTANCE_S TATUS"," INSTANCE_C ONFIG_INS"," INSTANCE_P REF_INS"," INSTANCE_E XPLAIN_INS"," INSTANCE_E XCEPTION_INS ","MONITOR_EX CEPTION_DE LETE"," MONITOR_EX CEPTION_UP DATE"," INSTANCE_E XCEPTION_I NS_BATCH"," EXCEPTION_ UPDATE"," EXCEPTION_ BATCHUPDATE ","INSTANCE_M AGAGE_HOST	

Role name	Role description	Resource	Actions	GrantOption
			", "INSTANCE_H A_LOGGER", " INSTANCE_S LOW", " INSTANCE_R EPORT", " INSTANCE_R EPORT_RPT", " INSTANCE_A CCOUNT", " INSTANCE_O PENPAGE", " INSTANCE_L OCK", " INSTANCE_A CCOUNT_LIST", " DBS_ACCOUN T_LIST", " ACCOUNT_LIST ", "DBS_LIST", " DBS_NEWACC OUNT", " DBS_ACCOUN T_CONFIG", " DBS_ACCOUN T_PROXY_INFO ", "DO_DBS_ACC OUNT_CONFIG ", "DBS_ACCOUN T_CHANGE_P ASSWORD", " DO_DBS_ACC OUNT_CHANG E_PASSWORD ", "DBS_ACCOUN T_RESET_PA SSWORD", " DO_DBS_ACC OUNT_RESET _PASSWORD", " DBS_ACCOUN T_DELETE", " 	

Role name	Role description	Resource	Actions	GrantOption
			ADD_DBS_AC COUNT"," TRANS_DBS"," DBS_MODIFY PRIVILEGE"," INSTANCE_U NLOCK"," INSTANCE_C ONFIG_PROXY ","INSTANCE_C ONFIG_SYNC ","INSTANCE_R ESTART"," INSTANCE_C LEARLOG"," INSTANCE_C HANGE"," DBS_ACCOUNT ","INSTANCE_B ACKUP"," INSTANCE_B ACKUP_CREA TE"," INSTANCE_B ACKUP_UPDA TE"," INSTANCE_R EBUILD_HA"," INSTANCE_A PPLY"," INSTANCE_C ONFIGSQLWALL ","INSTANCE_M ULTITRANS"," INSTANCE_D OMULTITRANS ","INSTANCE_C ONFIGPROXY MODE"," INSTANCE_P ASS"," INSTANCE_U	

Role name	Role description	Resource	Actions	GrantOption
			NPASS"," INSTANCE_D BCONFIG"," INSTANCE_T UNE"," SQL_DETAIL"," SLOWSQL_DE TAIL"," INSTANCE_S QL_SLOW_LOG ","SLOWLOG_DE TAIL"," MONITOR_WO RNING_DETAIL ","INSTANCE_L OG"," INSTANCE_T RANS"," INSTANCE_T RANS_DETAIL ","INSTANCE_T RANS_UPDATE ","INSTANCE_T RANS_CANCEL ","INSTANCE_T RANS_APPLY ","INSTANCE_T RANS_APPLY POST"," INSTANCE_T RANS_CHECK POST"," INSTANCE_T RANS_DBPOST ","INSTANCE_T RANS_DB"," INSTANCE_T RANS_OPENP AGE"," GET_INSTAN CE_TRANS_H OST","	

Role name	Role description	Resource	Actions	GrantOption
			GET_INSTAN CE_TRANS_C USTINS"," GET_INSTAN CE_TRANS_DB ","INSTANCE_U PDATECONFIG ","INSTANCE_U PDATE_AURA RO"," CLUSTER_LIST ","USSER_PROF ILE_LIST"," USSER_PROF ILE_ALL_LIST ","USSER_ALIY UN_INFO"," ERROR_RE_S UBMIT"," FLUSH_SYNC _MODE"," FLUSH_RESO URCE"," CHECK_INSN AME"," CHECK_CONN ADDR_CUST"," DEL_NODE_ID ","DEL_CLUSTE R_ID"," FETCH_BAK_ URL"," FETCH_BAK_ BINLOG_URL"," CHECK_DBNA ME"," EXCEPTION_ HOME"," EXCEPTION_ LIST"," RESOURCE_H OME","	

Role name	Role description	Resource	Actions	GrantOption
			RESOURCE_R EGION"," RESOURCE_M ORE"," RESOURCE_H A"," RESOURCE_IP ","RESOURCE_S ERVICE"," RESOURCE_B AKOWNER_TY PE"," RESOURCE_C REATE_BAKO WNER_TYPE"," RESOURCE_D ELETE_BAKO WNER_TYPE"," RESOURCE_E DIT_BAKOWN ER_TYPE"," RESOURCE_U PDATE_BAKO WNER_TYPE"," CLUSTER_UP DATERES"," LOGGER_HOME ","LOGGER_USE R","LOGGER_HA ","LOGGER_TRA NS"," LOGGER_REC OVER"," LOGGER_REM OTE"," LOGGER_BAC KUP"," LOGGER_API ","INSTANCE_A PILOG"," INSTANCE_A DMINLOG","	

Role name	Role description	Resource	Actions	GrantOption
			LOGGER_RESOURCE", HOST_HOME", HOST_SWITH", HOST_DOSWI TCH", INS_PREF_D EATIL", CUST_PREF_ DEATIL", TASK_HOME", TASK_FAIL", TRANCE_LIST ",TASK_RUN", TASK_STEP", TASK_START", TASK_FLOW", TASK_STAT", TASK_FLOWE XE", TASK_HISTORY ",TASK_LOOGE R", REPORT_HOME ",REPORT_CLU STER", REPORT_ZONE ",RESOURCE_V IPINFO", REPORT_REG IONNAME", DRC_LIST", GET_INSTAN CE_LEVEL", USER_ADD_R OLECLUSTER", USER_ADD_R ESOURCE", USER_UPDAT E_RESOURCE ",INSLEVEL_P ARAMS",	

Role name	Role description	Resource	Actions	GrantOption
			INSLEVEL_A DDPARAMS"," SYSTEM_WAT CH"," INSTANCE_S QLWALL"," INSTANCE_S QLWALLCHECK ","INSTANCE_S QLWALLCHEC KS"," INSTANCE_S QLWALLS"," REPORT_EXT RA_PURCHASE ","REPORT_EXT RA_PURCHAS E_PSOT"," INSTANCE_B AKHIS_MODIFY ","DELETE_SIT ENAME_ID"," PROXY_GROU P_HOME"," PROXY_CLUS TER"," PROXY_DETA IL","NET_VIEW ","NET_VIEW_N ET_TIME"," COMPONENT_ OSS"," COMPONENT_ HA"," COMPONENT_ HA_LOAD"," COMPONENT_ HA_SWITCH_ RECORD"," COMPONENT_ HA_API"," COMPONENT_	

Role name	Role description	Resource	Actions	GrantOption
			HA_EXCEPTION ","COMPONENT_ SWITCH_DETAIL ","COMPONENT_ SWITCH_API _TREND"," COMPONENT_ BAK"," PROXY_GROU P_OFFLINE"," PROXY_GROU P_ONLINE"," PROXY_GROU P_SLB"," PROXY_GROU P_API"," SLB_VIEW"," MONITOR_HO ME"," MONITOR_DE TAIL_TYPE"," PROXY_VIEW ","MONITOR_IN DEX"," MONITOR_CR EATE_SUBSC RIBER"," MONITOR_RE MOVE_SUBSC RIBER"," SUBSCRIBER _MANAGER"," SUBSCRIBER _CREATE"," SUBSCRIBER _UPDATE"," SUBSCRIBER _DELETE"," MONITOR_ER ROR"," MONITOR_TR END_DETAIL","	

Role name	Role description	Resource	Actions	GrantOption
			CLOUD_HOME _STAT"," API_ADD_EC S_IP_FILTER"," API_SHOW_E CS_IP_FILTER"," CLOUD_HOME ","CLOUD_APPL Y_POST"," CLOUD_GROU P_LIST"," CLOUD_INS_ LIST"," CLOUD_GROU P_MANAGER"," CLOUD_GROU P_CREATE"," CLOUD_DO_G ROUP_CREATE ","CLOUD_EDIT _GROUP"," CLOUD_DO_E DIT_GROUP"," CLOUD_APPL Y"," CLOUD_GROU P_ADDINS"," CLOUD_GROU P_INS"," CLOUD_GROU P_INSPROFI LE"," CLOUD_GROU P_INSTANCE _LOCK"," CLOUD_GROU P_INSTANCE _UNLOCK"," CLOUD_GROU P_CLEARLOG"," CLOUD_GROU P_RESTART","	

Role name	Role description	Resource	Actions	GrantOption
			CLOUD_GROU P_UPDATE_A URARO"," CLOUD_GROU P_BATCH_SW ITH"," CLOUD_GROU P_DOBATCH_ SWITCH"," CLOUD_GROU P_ATTENTION ","CLOUD_MY_G ROUP_ATTEN TION"," CUSTINS_LOGS ","DATA_SQLCO MAND"," DATA_SQLCO MAND_SHOWD ATABASE"," DATA_SQLCO MAND_EXECU TE"," DATA_SQLCO MAND_CANCEL ","TABLE_DETA IL"," COLUMN_DET AIL"," WARN_MANAG ER_CONTACT S"," WARN_MANAG ER_THRESHO LD"," WARN_MANAG ER_CREATE_ CONTACT"," WARN_MANAG ER_UPDATE_ THRESHOLD"," WARN_MANAG	

Role name	Role description	Resource	Actions	GrantOption
			ER_DELETE_CONTACTS"," INSTANCE_CREATE_NOT_NORMAL"," INSTANCE_LOG_PAGE"," COMPONENT_SLB_CLUSTER ","COMPONENT_RDS_CLUSTER ","CUSTINS_DATA_LINK"," INSTANCE_MYSQL_SPACE"," INSTANCE_SLASH","HOST_OPERATE"," CUSTINS_PANORAMA"," TABLE_ALTER"," RDS_SCHEMA_SQL"," POWER_TEST ","MIGRATE_CREATE"," CREATE_SUPER_ACCOUNT ","INSTANCE_CONFIG_INS_OP ","BACK_HIST_FETCH"," ACCESS_GRANTEDACCOUNT"," COMPONENT_AUTOTEST"," INSTANCE_RESET_PASSWORD"]	
RDS_instance approval	RDS_instance approval	26842:rds	["INSTANCE_AUDIT"," INSTANCE_A	0

Role name	Role description	Resource	Actions	GrantOption
			UDIT_POST"," INSTANCE_A UDIT_INS"]	
RDS_system administrator	RDS DBA - system level - cannot authorize, but has almost all other functions	26842:rds	["SYSTEM_EDIT_LEVEL"," SYSTEM_DO_NEW_LEVEL"," SYSTEM_DO_UPDATE_LEVEL ","SYSTEM_DO_DELETE_LEVEL ","SYSTEM_NEW_HOST_LEVEL ","SYSTEM_EDIT_HOST_LEVEL ","SYSTEM_EDIT_GROUP"," SYSTEM_DO_EDIT_GROUP"," SYSTEM_DO_SAVE_HOST_LEVEL"," SYSTEM_DO_UPDATE_HOST_LEVEL"," SYSTEM_DO_DELETE_HOST_LEVEL"," SYSTEM_WATCH"," SYSTEM_UPLOAD_IMAGE"," SYSTEM_MODIFY_IMAGE"," SYSTEM_MODIFY_WATCH"," CHECK_ACCOUNT"," REFLUSH_TRANCES_DENY ","REFLUSH_USER_CLUSTER",	0

Role name	Role description	Resource	Actions	GrantOption
			REFLUSH_US ER_ROLE"," SYSTEM_HOS TBUFFER"," SYSTEM_HOS TBUFFER_DE LETE"," INSTANCE_S QLWALL"," INSTANCE_S QLWALLCHECK ","INSTANCE_S QLWALLCHEC KS"," INSTANCE_S QLWALLS"," REPORT_EXT RA_PURCHASE ","REPORT_EXT RA_PURCHAS E_PSOT"," INSTANCE_B AKHIS_MODIFY ","SYSTEM_CRE ATE_SITENAME ","SYSTEM_SIT ENAME"," SYSTEM_INS PERF"," DELETE_SIT ENAME_ID"," PROXY_GROU P_HOME"," PROXY_CLUS TER"," TO_CREATE_ PROXY_CLUS TER"," CREATE_PRO XY_CLUSTER ","TO_UPDATE_ PROXY_CLUS	

Role name	Role description	Resource	Actions	GrantOption
			TER"," UPDATE_PROXY_CLUSTER ","TO_CREATE_PROXY_NODE ","CREATE_PROXY_NODE"," TO_UPDATE_PROXY_NODE ","UPDATE_PROXY_NODE"," TO_UPDATE_PROXY_API_NODE"," UPDATE_PROXY_API_NODE ","DELETE_PROXY_NODE"," DELETE_PROXY_API_NODE"," PROXY_DETAIL ","CREATE_PROXY_CLUSTER_GROUP"," EDIT_NODE_TO_GROUP"," TO_EDIT_NODE_TO_GROUP"," NET_VIEW ","NET_VIEW_NET_TIME"," COMPONENT_OSS"," COMPONENT_HA"," COMPONENT_HA_LOAD"," COMPONENT_HA_SWITCH_RECORD"," COMPONENT_HA_API","	

Role name	Role description	Resource	Actions	GrantOption
			COMPONENT_ HA_EXCEPTION ","COMPONENT_ SWITCH_DETAIL ","COMPONENT_ SWITCH_API _TREND"," COMPONENT_ BAK"," PROXY_GROU P_OFFLINE"," PROXY_GROU P_ONLINE"," PROXY_GROU P_SLB"," PROXY_GROU P_API"," SLB_VIEW"," MONITOR_HO ME"," MONITOR_DE TAIL_TYPE"," PROXY_VIEW ","MONITOR_IN DEX"," MONITOR_CR EATE_SUBSC RIBER"," MONITOR_RE MOVE_SUBSC RIBER"," SUBSCRIBER _MANAGER"," SUBSCRIBER _CREATE"," SUBSCRIBER _UPDATE"," SUBSCRIBER _DELETE"," MONITOR_ER ROR"," MONITOR_TR	

Role name	Role description	Resource	Actions	GrantOption
			END_DETAIL"," CLOUD_HOME _STAT"," SYSTEM_API _MANAGE"," API_ADD_EC S_IP_FILTER"," API_SHOW_E CS_IP_FILTER"," CLOUD_HOME ","CLOUD_APPL Y_POST"," CLOUD_GROU P_LIST"," CLOUD_INS_ LIST"," CLOUD_GROU P_MANAGER"," CLOUD_GROU P_CREATE"," CLOUD_DO_G ROUP_CREATE ","CLOUD_EDIT _GROUP"," CLOUD_DO_E DIT_GROUP"," CLOUD_APPL Y"," CLOUD_GROU P_ADDINS"," CLOUD_GROU P_INS"," CLOUD_GROU P_INSPROFI LE"," CLOUD_GROU P_INSTANCE _LOCK"," CLOUD_GROU P_INSTANCE _UNLOCK"," CLOUD_GROU	

Role name	Role description	Resource	Actions	GrantOption
			P_CLEARLOG"," CLOUD_GROU P_RESTART"," CLOUD_GROU P_UPDATE_A URARO"," CLOUD_GROU P_BATCH_SW ITH"," CLOUD_GROU P_DOBATCH_ SWITCH"," CLOUD_GROU P_ATTENTION ","CLOUD_MY_G ROUP_ATTEN TION"," USERGROUP_ CREATE_USE R_GROUP"," USERGROUP_ EDIT_USER_ GROUP"," USERGROUP_ OF_EDIT_ROLE ","USERGROUP_ OF_DO_EDIT _ROLE"," USERGROUP_ OF_EDIT_CL USTER"," USERGROUP_ OF_SEARCH_ CLUSTER"," USERGROUP_ OF_DO_EDIT _CLUSTER"," USERGROUP_ OF_EDIT_INS"," USERGROUP_ OF_SEARCH_ INS","	

Role name	Role description	Resource	Actions	GrantOption
			USERGROUP_ OF_DO_EDIT _INS"," USERGROUP_ OF_EDIT_USER ","USERGROUP_ OF_SEARCH_ USER"," USERGROUP_ OF_DO_EDIT _USER"," USERGROUP_ DO_EDIT_US ER_GROUP"," USERGROUP_ DELETE_USE R_GROUP"," CUSTINS_LOGS ","DATA_SQLCO MAND"," DATA_SQLCO MAND_SHOWD ATABASE"," DATA_SQLCO MAND_EXECU TE"," DATA_SQLCO MAND_CANCEL ","TABLE_DETA IL"," COLUMN_DET AIL"," WARN_MANAG ER_CONTACT S"," WARN_MANAG ER_THRESHO LD"," WARN_MANAG ER_CREATE_ CONTACT"," WARN_MANAG	

Role name	Role description	Resource	Actions	GrantOption
			ER_UPDATE_ THRESHOLD"," WARN_MANAG ER_DELETE_ CONTACTS"," INSTANCE_S WITCH_INST ANCE"," INSTANCE_O PARATOR_PE RMISSION"," INSTANCE_C REATE_BY_A MORAYAPI"," INSTANCE_C REATE_NOT_ NORMAL"," GROUP_INST ANCE_VIEW_ WARN"," GROUP_INST ANCE_DELET E_WARN"," INSTANCE_L OG_PAGE"," INSTANCE_B ATCH_APPLY ","INSTANCE_P ROXYLIST"," INSTANCE_S WITCHLINK"," COMPONENT_ SLB_CLUSTER ","COMPONENT_ RDS_CLUSTER ","PROXY_TO_U SE_NODE_TE MPLATE"," PROXY_USE_ NODE_TEMPL ATE"," PROXY_TO_U	

Role name	Role description	Resource	Actions	GrantOption
			SE_NODE_TEMPLATE", TO_EDIT_NODE_TO_GROUP", "EDIT_NODE_TO_GROUP", PROXY_USE_NODE_TEMPLATE", SYSTEM_EXCEPTION_LEVEL", "INSTANCE_DO_SWITCHLINK", "HOST_BACKINFO", HOST_RRTIME", "CONNECTIVITY_CHECK", CONNECTIVITY_REGION_DATA", COMPONENT_INS_LIST", REFLUSH_AV_ZONE_LIST", INSTANCE_TRANS_UPGRADE", INSTANCE_MULTITRANS_NEW", INSTANCE_DOMULTITRANS_NEW", TASK_EDIT_ENGINE_CONTENT", DATA_SQLCOMMAND", RESOURCE_OVERVIEW", HOST_BIANQUE	

Role name	Role description	Resource	Actions	GrantOption
			", "COMPONENT_ CUSTINS_NO TEQUEL_SIT ENAME_WITH _SLB", " GROUP_INST ANCE_THRES HOLD", " INSTANCE_M ULTIUPGRADE ", "INSTANCE_D OMULTIUPGR ADE", " INSTANCE_D O_BATCH_HA SWITH ", " INSTANCE_D O_BATCH_HA SWITH", " CUSTINS_DA TA_LINK", " INSTANCE_M ULTIREFRESH ", "INSTANCE_M YSQL_OPERATE ", "HOST_INTIME ", "INSTANCE_M YSQL_OPERATE ", "INSTANCE_U PLOAD_POLI CY", " HOST_RESTART ", "ROBOT_LOG ", "ROBOT_ROBO T", "INSTANCE_M YSQL_SPACE", " INSTANCE_SLA ", "INSTANCE_B ATCH_VERSI ON_UPGRADE ", "HOST_OPERA TE", "TASK_INFO	

Role name	Role description	Resource	Actions	GrantOption
			";OS_CONFIG ";UPDATE_OS_CONFIG"," RESOURCE_SCHEDULE"," OPERATE_WATCH"," COMPONENT_SLB_CHECK"," CUSTINS_PANORAMA"," SYSTEM_CLUSTER_CONFIG ";TABLE_ALTER ";RDS_SCHEMA_SQL"," POWER_TEST ";NODE_ADD ";INSTANCE_FCS_DELETE"," PROXY_CONFIG ";MIGRATE_CREATE"," SYSTEM_BU"," ROBOT_TASK_STATISTICS"," CREATE_SPECIAL_ACCOUNT ";COMPONENT_INCONSIST"," RDS_DATA"," CREATE_SUPER_ACCOUNT ";INSTANCE_BATCH_PRE_SUPER_PERMISSION"," TASK_TRACE ";INSTANCE_MULTIBAKREBUILD ";HOST_BATCH_DO_BAK_RE	

Role name	Role description	Resource	Actions	GrantOption
			BUILD"," INSTANCE_C ONFIG_INS_OP ","BAK_HIS_LI ST_FETCH"," ACCESS_GRA NTACCOUNT ","INSTANCE_B ATCH_HASWITH ","COMPONENT_ AUTOTEST"," INSTANCE_R ESET_PASSW ORD","HOME"," RDS_HOME"," COMPONENT_ HOME"," COMPONENT_ RGWVIEW"," COMPONENT_ PROXYVIEW"," COMPONENT_ SQLVIEW"," COMPONENT_ BAKVIEW"," COMPONENT_ RGW"," COMPONENT_ RGWLIST"," COMPONENT_ LVS"," COMPONENT_ PROXY"," DBS_ACCOUN TS"," BAK_HIS_LIST ","BAK_OAS_FE TCH_LIST"," BAK_FETCH_ OAS"," SWITCH_VIP"," BAK_REVERT","	

Role name	Role description	Resource	Actions	GrantOption
			CLUSTER_HOST ", "BAK_BINLOG ", "BAK_HIS_SET ", "BAK_HIS_RE VERT", " DBBAK_CREATE ", "BAK_INSTAN CE_DBS", " RDS_GROUP", " GROUP_FINA NCE", " GROUP_CREA TE", " GROUP_PROF ESSION", " GROUP_ENTE RPRISE", " GROUP_ADDINS ", "GROUP_INST ANCE_GID", " GROUP_COMM UNICATE", " INSTANCE_D BS_LIST", " INSTANCE_D ELETEDB_DB SID", " INSTANCE_D BS_DETAIL", " INSTANCE_D BS_CREATE", " INSTANCE_C REATRREADO NLY", " INSTANCE_C REATEDISAS TER", " GROUP_OTHE R", " GROUP_HOME ", "GROUP_INDE X", " 	

Role name	Role description	Resource	Actions	GrantOption
			GROUP_NUMB ER","GROUP_HA ","GROUP_VIEW ","GROUP_LIST ","GROUP_HOST _LIST"," GROUP_DDL"," USER_INSPR OFILE"," GROUP_REMO VE_INSTANCE"," INSTANCE_LIST ","INSTANCE_C HECK_PASS"," INSTANCE_O WNER"," INSTANCE_A DDACCOUNT ","INSTANCE_A DDACCOUNT_ VIEW"," INSTANCE_U PDATE_POST ","INSTANCE_D OCREATEREA ONLY"," INSTANCE_D OCREATEDIS ASTER"," PROXY_EDIT _POST"," INSTANCE_D ETAIL"," INSTANCE_N OT_NORMAL_ DETAIL"," INSTANCE_C REATE_NOT_ NORMAL"," INSTANCE_E DIT_NOT_NO RMAL","	

Role name	Role description	Resource	Actions	GrantOption
			INSTANCE_D O_EDIT_NOT _NORMAL"," INSTANCE_D ELETE_NOT_ NORMAL"," SWITCH_GUA RD"," DO_SWITCH_ GUARD"," INSTANCE_DBS ","INSTANCE_D ELETE"," INSTANCE_C REATEBAKRE AONLYINS"," INSTANCE_M ANAGE_POST ","INSTANCE_I NS_TASK"," INSTANCE_D IAGONSE"," INSTANCE_T RANS_CLUST ERS"," INSTANCE_Z ONE_CLUSTE RS"," INSTANCE_M AGAGE_INS"," INSTANCE_C USTLINK_INS ","INSTANCE_A UDIT_INS"," INSTANCE_E DIT_INS"," INSTANCE_I NTIME_INS"," INSTANCE_K ILL_SESSION ","INSTANCE_P ROXY_LINK","	

Role name	Role description	Resource	Actions	GrantOption
			INSTANCE_D IAGNOSE"," INSTANCE_S TATUS"," INSTANCE_C ONFIG_INS"," INSTANCE_P REF_INS"," INSTANCE_U PDATE_CONFIG ","INSTANCE_E XPLAIN_INS"," INSTANCE_E XCEPTION_INS ","MONITOR_EX CEPTION_DE LETE"," MONITOR_EX CEPTION_UP DATE"," INSTANCE_E XCEPTION_I NS_BATCH"," EXCEPTION_ UPDATE"," EXCEPTION_ BATCHUPDATE ","INSTANCE_M AGAGE_HOST ","INSTANCE_H A_LOGGER"," INSTANCE_S LOW"," INSTANCE_R EPORT"," INSTANCE_R EPORT_RPT"," INSTANCE_A CCOUNT"," INSTANCE_O PENPAGE"," INSTANCE_L	

Role name	Role description	Resource	Actions	GrantOption
			LOCK"," INSTANCE_A CCOUNT_LIST"," DBS_ACCOUN T_LIST"," ACCOUNT_LIST ","DBS_LIST"," DBS_NEWACC OUNT"," DBS_ACCOUN T_CONFIG"," DBS_ACCOUN T_PROXY_INFO ","DO_DBS_ACC OUNT_CONFIG ","DBS_ACCOUN T_CHANGE_P ASSWORD"," DO_DBS_ACC OUNT_CHANG E_PASSWORD ","DBS_ACCOUN T_RESET_PA SSWORD"," DO_DBS_ACC OUNT_RESET _PASSWORD"," DBS_ACCOUN T_DELETE"," ADD_DBS_AC COUNT"," TRANS_DBS"," DBS_MODIFY PRIVILEGE"," INSTANCE_U NLOCK"," INSTANCE_C ONFIG_PROXY ","INSTANCE_C ONFIG_SYNC ","INSTANCE_R ESTART","	

Role name	Role description	Resource	Actions	GrantOption
			INSTANCE_C LEARLOG", INSTANCE_C HANGE", DBS_ACCOUNT ", INSTANCE_B ACKUP", INSTANCE_B ACKUP_CREA TE", INSTANCE_B ACKUP_UPDA TE", INSTANCE_R EBUILD_HA", INSTANCE_C ONFIGSQLWALL ", INSTANCE_M ULTITRANS", INSTANCE_D OMULTITRANS ", INSTANCE_C ONFIGPROXY MODE", INSTANCE_P ASS", INSTANCE_U NPASS", INSTANCE_D BCONFIG", INSTANCE_T UNE", SQL_DETAIL", SLOWSQL_DE TAIL", INSTANCE_S QL_SLOW_LOG ", SLOWLOG_DE TAIL", MONITOR_WO RNING_DETAIL ", INSTANCE_L	

Role name	Role description	Resource	Actions	GrantOption
			OG"," INSTANCE_T RANS"," TRANS_AUDIT ","INSTANCE_T RANS_DETAIL ","INSTANCE_T RANS_UPDATE ","INSTANCE_T RANS_CANCEL ","INSTANCE_T RANS_APPLY ","INSTANCE_T RANS_APPLY POST"," INSTANCE_T RANS_CHECK POST"," INSTANCE_T RANS_DBPOST ","INSTANCE_T RANS_OPENP AGE"," GET_INSTAN CE_TRANS_H OST"," GET_INSTAN CE_TRANS_C USTINS"," GET_INSTAN CE_TRANS_DB ","INSTANCE_U PDATECONFIG ","INSTANCE_U PDATE_AURA RO"," CLUSTER_LIST ","USSER_PROF ILE_LIST"," USSER_PROF ILE_ALL_LIST ","USSER_ALIY	

Role name	Role description	Resource	Actions	GrantOption
			UN_INFO"," CLUSTER_NEW ","CLUSTER_ER ROR"," ERROR_RE_S UBMIT"," CLUSTER_UP CONIFG"," CLUSTER_NO DELIST"," CLUSTER_NO DE"," CLUSTER_ED ITNODE"," CREATE_NOD E"," UPDATE_NODE ","CLUSTER_CR EATE"," CLUSTER_FL USHWHITE"," FLUSH_SYNC _MODE"," FLUSH_RESO URCE"," CHECK_INSN AME"," CHECK_CONN ADDRCUST"," DEL_NODE_ID ","DEL_CLUSTE R_ID"," FETCH_BAK_ URL"," FETCH_BAK_ BINLOG_URL"," CHECK_DBNA ME"," EXCEPTION_ HOME"," EXCEPTION_ LIST","	

Role name	Role description	Resource	Actions	GrantOption
			RESOURCE_H OME"," HOST_CONFIG ","HOST_UPCON FIG"," RESOURCE_R EGION"," RESOURCE_M ORE"," HOST_CREATE ","HOST_UPDAT E"," RESOURCE_HA ","RESOURCE_H OSTBUFFER"," RESOURCE_H OST"," RESOURCE_IP ","RESOURCE_S ERVICE"," RESOURCE_B AKOWNER_TY PE"," RESOURCE_C REATE_BAKO WNER_TYPE"," RESOURCE_D ELETE_BAKO WNER_TYPE"," RESOURCE_E DIT_BAKOWN ER_TYPE"," RESOURCE_U PDATE_BAKO WNER_TYPE"," CLUSTER_UP DATERES"," LOGGER_HOME ","LOGGER_USE R","LOGGER_HA ","LOGGER_TRA NS","	

Role name	Role description	Resource	Actions	GrantOption
			LOGGER_REC OVER"," LOGGER_REM OTE"," LOGGER_BAC KUP"," LOGGER_API ","INSTANCE_A PILOG"," INSTANCE_A DMINLOG"," LOGGER_RES OURCE"," HOST_HOME"," HOST_INSPREF ","HOST_SWITH ","HOST_BATCH _SWITH"," HOST_BATCH _TRANS_INS"," HOST_PREF"," HOST_INFO"," HOST_INSTA NCE"," HOST_NEW"," HOST_DOSWI TCH"," HOST_TASK"," HOST_TASKS"," HOST_DOBAT CH_SWITCH"," HOST_DOBAT CH_TRANS_INS ","HOST_EDIT ","HOST_PREF_ DEATIL"," HOST_DELET E_HOSTID"," HOST_CHECK _HOSTID"," INS_PREF_D EATIL","	

Role name	Role description	Resource	Actions	GrantOption
			CUST_PREF_ DEATIL"," TASK_HOME"," TASK_FAIL"," TRANCE_LIST ","TASK_RUN"," TASK_STEP"," TASK_START"," TASK_FLOW"," TASK_STAT"," TASK_FLOWE XE"," TASK_HISTORY ","TASK_LOOGE R"," REPORT_HOME ","REPORT_CLU STER"," REPORT_ZONE ","RESOURCE_H OSTINFO"," RESOURCE_V IPINFO"," REPORT_REG IONNAME"," DRC_HOME"," DRC_PRECHE CK"," DRC_PRESCH ECK"," DRC_COMMIT ","DRC_LIST"," SYSTEM_HOME ","SYSTEM_INS IDC"," SYSTEM_INS IDC_LSIT"," SYSTEM_MEA SUREDATA"," SYSTEM_COU NTDATA"," SYSTEM_BOSS	

Role name	Role description	Resource	Actions	GrantOption
			", "SYSTEM_PER MISSION", " SYSTEM_UPD ATEPERMISS ION", " SYSTEM_TAN CEDENCY", " SYSTEM_CFR EATE_TANCE DENCY", " SYSTEM_REG ION", " SYSTEM_CFR EATE_REGION ", "DELETE_REG ION_ID", " SYSTEM_DEL ETE_TANCED ENCY", " SYSTEM_CRE ATE_HOSTBU FFERSN", " SYSTEM_CRE ATEPERMISS ION", " USER_UPDAT E_CLUSTER", " GET_INSTAN CE_LEVEL", " PERMISSION _NEW", " USER_ADD_R OLECLUSTER", " USER_ADD_R ESOURCE", " SYSTEM_DEL ETE_RESOUR CE", " USER_UPDAT E_RESOURCE", " SYSTEM_SALES ", "INSLEVEL_P	

Role name	Role description	Resource	Actions	GrantOption
			ARAMS"," INSLEVEL_A DDPARAMS"," SYSTEM_TEM PLATE"," SYSTEM_NEW TEMPLATE"," SYSTEM_DOD ELETEPARAMID ","SYSTEM_DOS AVEINSLEVEL"," SYSTEM_DOE DITMYCNFTE MPLATE"," SYSTEM_PREF ","SYSTEM_SOF TLIST"," SYSTEM_SOF TWARE"," SYSTEM_IPF ILTER"," SYSTEM_ADD _IPFILTER"," SYSTEM_DEL ETE_IPFILTER ","BOSS_SEND ","SYSTEM_SET TING"," SYSTEM_GRO UP"," SYSTEM_FEA CHDATA"," SYSTEM_OPE RATORS"," SYSTEM_CRE ATE_OPERAT OR"," SYSTEM_TO_ UPDATE_OPE RATOR"," SYSTEM_UPD ATE_OPERAT	

Role name	Role description	Resource	Actions	GrantOption
			OR"," SYSTEM_DELETE_OPERATOR"," SYSTEM_GROUP_SUBSCRIBE_WARN"]	
ROLE_CONTROLLER	RDS control duty	26842:rds	["TASK_START_STEP"," TASK_CLOSE"]	0

Of which:

- RDS_instance read-only: Has the read permission to the database instance.
- RDS_system read-only: Has the read-only permission to RDS Operations and Maintenance System, including the homepage dashboard, cluster information, and host management information.
- RDS_instance administrator: Has the read and write permissions to the database instance and can configure the database instance.
- RDS_system administrator: Has the read and write permissions to RDS Operations and Maintenance System and can configure the service nodes and resources.

3.1.10.1.4 Storage Operations and Maintenance System default roles

Role name	Role description	Resource	Actions	GrantOption
OSS_user administrator	OSS user data management and monitoring	26842:oss	["get_quota_quota"," get_vip_vip_list"," get_quota_run_monitor"," get_ocm_bucket"," get_quota_datasize"," get_quota_bucket_resource"," get_user_info"," get_quota_overview","	0

Role name	Role description	Resource	Actions	GrantOption
			get_quota_sla"," get_ocm_buckets ","post_vip_v ip_list"," delete_vip _vip_list"]	
OSS_cluster administrator	OSS cluster data management and monitoring	26842:oss	["get_quota_ region_storage ","get_quota_ region_buc ket_stat"," get_quota_ region_object ","get_quota_ region_monitor ","get_quota_ region_stat"," get_quota_ region_overview ","get_quota_ region_clu ster_type_stat ","get_quota_ region_tod ay_cluster _type_overview ","get_quota_ region_inventory ","get_quota_ region_mns _active"," get_quota_ top_min_time ","get_quota_ top_storage ","get_quota_ top_storag e_increment ","get_quota_ top_request ","get_quota_ top_sys_error	0

Role name	Role description	Resource	Actions	GrantOption
			", "get_quota_top_pub_traffic_out", " get_quota_top_pub_traffic_in ", "get_quota_top_pri_traffic_out ", "get_quota_top_pri_traffic_in ", "get_quota_top_cdn_in", " get_quota_top_cdn_out ", "get_disk_status_summary", " get_disk_status ", "get_disk_usage_summary", " get_disk_usage_history", " get_disk_usage ", "get_disk_usage_details ", "post_pop_cluster_inventory"]	
OSS_public permissions	Basic permissions for the OSS platform, required for authorization	26842:oss	["get_env_get_env", "get_location_tree", " get_location_tree2", " get_location_all", " get_audit_op_log"]	0

Of which:

- OSS_user administrator: Queries resource usage by UID, account, and bucket, makes statistics of data such as basic resource attributes, and learns about the trend.
- OSS_cluster administrator: Queries the resource usage of a bucket running on a cluster, the cluster running status, and physical resource monitoring.

- OSS_public permissions: Provides the query function of backend log audit and basic public permissions.

3.1.10.1.5 SLB/VPC Operations and Maintenance System default roles

Default roles and GrantOption

Role name	Role description	Resource	Actions	GrantOption
SLB_administrator	Performs operations on all Server Load Balancer data	26842:slb	["read","create","delete","update"]	0
VPC_administrator	Performs operations on all VPC data	26842:vpc	["read","create","delete","update"]	0
SLB_read-only	Performs operations on all Server Load Balancer data	26842:slb	["read"]	0
VPC_read-only	Performs operations on all VPC data	26842:vpc	["read"]	0

Of which:

- SLB_administrator: Has permissions to update the Server Load Balancer cluster version, kernel, and cluster information.
- SLB_read-only: Has permissions to search Server Load Balancer resources, query cluster information, and view all information.
- VPC_administrator: Has permissions to add non-read-only interfaces such as BFlag resources.
- VPC_read-only: Has permissions to view read-only interfaces such as VPC information.

Default roles and RoleHierarchy

Role name	Role description	RoleHierarchy
VNET_super administrator	Performs operations on all SLB/VPC Operations and Maintenance System data.	[SLB_administrator, VPC_administrator]

Role name	Role description	RoleHierarchy
VNET_global read-only	Reads all SLB/VPC Operations and Maintenance System data.	[SLB_read-only, VPC_read-only]

3.1.10.1.6 Apsara Infrastructure Management Framework default roles

Role name	Role description	Resource	Actions	GrantOption
Tianji_Project read-only	Has the read-only permission to Apsara Infrastructure Management Framework projects, which allows you to view the configurations and status information of all projects and clusters	*:tianji:projects	["read"]	0
Tianji_Project administrator	Has all the permissions to Apsara Infrastructure Management Framework projects, which allows you to view and modify the configurations and status information of all projects and clusters	*:tianji:projects	["*"]	0
Tianji_Service read-only	Has the read-only permission to Apsara Infrastructure Management Framework services, which allows you to view the	*:tianji:services	["read"]	0

Role name	Role description	Resource	Actions	GrantOption
	configurations and template information of all services			
Tianji_Service administrator	Has all the permissions to Apsara Infrastructure Management Framework services, which allows you to view and modify the configurations and template information of all services	*:tianji:services	["*"]	0
Tianji_IDC administrator	Has all the permissions to Apsara Infrastructure Management Framework data centers, which allows you to view and modify the data center information	*:tianji:idcs	["*"]	0
Tianji_administrator	Has all the permissions to Apsara Infrastructure Management Framework, which allows you to perform operations on all Apsara Infrastructure Management Framework configurations	*:tianji	["*"]	0

3.1.10.1.7 Webapp-rule default roles

Role name	Role description	Resource	Actions	GrantOption
Webapp-rule O&M administrator	Has all the permissions to Webapp-rule projects, which allows you to view, modify, add, and delete all configurations and status information	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 configurations and status information	26842:webapp-rule:*	["read"]	0

3.1.10.1.8 Workflow (grandcanal) console default roles

Role name	Role description	Resource	Actions	GrantOption
grandcanal.ADMIN	Workflow console administrator, who can query the workflow and activity details, and retry, roll back, stop, 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

3.1.10.1.9 baseService-yaochi-console default roles

Role name	Role description	Resource	Actions	GrantOption
yaochi-console-admin (Business Foundation System console management)	Has the add, delete, update , and query permissions to the baseService-yaochi-console , including business (BID) management , cloud product code management , business cloud product management, physical location management, business location management , and product service account management	26842:yaochi-console:*	["read", "write"]	0
yaochi-console-reader (Business Foundation System console read-only)	Has the read-only permission to the baseService-yaochi-console, which only allows you to view business (BID) management , cloud product code management , business cloud product management, physical location management, business location management	26842:yaochi-console:*	["read"]	0

Role name	Role description	Resource	Actions	GrantOption
	, and product service account information			

3.1.10.1.10 BCC default roles

Role name	Role description	Resource	Actions	GrantOption
bcc_admin	Super administrator in the BCC backend	*:bcc	*	0
bcc_admin_odps	MaxCompute administrator in the BCC backend	26842:bcc:/api/product/odps/	*	0
bcc_admin_dataworks	DataWorks administrator in the BCC backend	26842:bcc:/api/product/dataworks/	*	0
bcc_admin_streamcompute	StreamCompute administrator in the BCC backend	26842:bcc:/api/product/streamcompute/	*	0
mcadmin	MaxCompute substation administrator	26842:bcc:/api/bccapi/sysadmin/	*	0
		26842:bcc:/api/ias/	*	0
		26842:bcc:/api/tflow/	*	0
		26842:bcc:/api/bccapi/odps/	*	0
scadmin	StreamCompute substation administrator	26842:bcc:/api/bccapi/sysadmin/	*	0
		26842:bcc:/api/ias/	*	0
		26842:bcc:/api/tflow/	*	0
		26842:bcc:/api/bccapi/galaxy/	*	0

Role name	Role description	Resource	Actions	GrantOption
dwadmin	DataWorks substation administrator	26842:bcc:/api/bccapi/sysadmin/	*	0
		26842:bcc:/api/ias/	*	0
		26842:bcc:/api/tflow/	*	0
		26842:bcc:/api/bccapi/base/	*	0
bcc_admin_dataapp	BCC data application administrator	26842:bcc:/api/product/iplus/	*	0
		26842:bcc:/api/product/datav/		
		26842:bcc:/api/product/dtboost/		
		26842:bcc:/api/product/pai/		
		26842:bcc:/api/product/quickbi/		
bcc_admin_biggraph	BCC graph calculation administrator	26842:bcc:/api/product/biggraph/	*	0

**Note:**

The mcadmin, scadmin, and dwadmin roles are administrators of BCC O&M substations MaxCompute, StreamCompute, and DataWorks. They have all menu permissions and the corresponding interface resource permissions to their substations.

Where,

- **MaxCompute O&M substation administrator**

The initialized role name of the MaxCompute O&M substation administrator is mcadmin. This role has all menu permissions and interface call permissions to the MaxCompute substation.

The mcadmin role has permissions to all menus in the left-side navigation pane and all interface resources. The interface call is reflected in each menu. The chart and list data loaded

by menu functions will call `26842:bbc:/api/bccapi/sysadmin/` and `26842:bbc:/api/bccapi/odps/` respectively.

- **StreamCompute O&M substation administrator**

The initialized role name of the StreamCompute O&M substation administrator is `scadmin`. This role has all menu permissions and interface call permissions to the StreamCompute substation

The `scadmin` role has permissions to all menus in the left-side navigation pane and all interface resources. The interface call is reflected in each menu. The chart and list data loaded by menu functions will call `26842:bbc:/api/bccapi/sysadmin/` and `26842:bbc:/api/bccapi/galaxy/` respectively.

- **DataWorks O&M substation administrator**

The initialized role name of the DataWorks O&M substation administrator is `dwadmin`. This role has all menu permissions and interface call permissions to the DataWorks substation.

The `dwadmin` role has permissions to all menus in the left-side navigation pane and all interface resources. The interface call is reflected in each menu. The chart and list data loaded by menu functions will call `26842:bbc:/api/bccapi/sysadmin/` and `26842:bbc:/api/bccapi/base/` respectively.

3.1.10.1.11 Tlog default role

Role name	Role description	Resource	Actions	GrantOption
Tlog administrator	Has all Tlog permissions, which allows you to perform operations on all Tlog configurations	<code>26842:tlogconsole:*</code>	<code>["*"]</code>	0

3.1.10.1.12 Butler default roles

Role name	Role description	Resource	Actions	GrantOption
butler-guest	Common Butler user, with the read-only permission	<code>26842:butler:*</code>	<code>["query"]</code>	0

Role name	Role description	Resource	Actions	GrantOption
butler-admin	Butler administrator, with all permissions	26842:butler:*	["*"]	0

3.1.10.1.13 Data Replication System default roles

Role name	Role description	Resource	Actions	GrantOption
jingwei-develop	Developer permissions, which allow you to perform common user operations on the Data Replication System console, such as creating, viewing, deleting, starting, and stopping resources (tasks and services)	26842:drds:jingwei:/createGuide.htm	["READ"]	0
		26842:drds:jingwei:/serviceList.htm		
		26842:drds:jingwei:/db2DbServiceDirect.htm		
		26842:drds:jingwei:/taskDetail.htm		
		26842:drds:jingwei:/statTrend.htm		
		26842:drds:jingwei:/fullCopyService.htm		
		26842:drds:jingwei:/taskWorker.htm		
		26842:drds:jingwei:/taskWorker.htm		
		26842:drds:jingwei:/taskJstack.htm		
		26842:drds:jingwei:/		

Role name	Role description	Resource	Actions	GrantOption
		taskWorkerLog.htm		
		26842:drds:jingwei:/db2Db.htm		
		26842:drds:jingwei:/tableSpread.htm		
jingwei-admin	The highest permissions, that is, administrator permissions, which allow you to perform all operations on the Data Replication System console	26842:drds:jingwei:*	["*"]	0

3.1.10.1.14 Tianjimon default role

Role name	Role description	Resource	Actions	GrantOption
Tianjimon O&M	Has all Tianjimon permissions, which allows you to perform basic monitoring and O&M	26842:tianjimon:*	["*"]	0

3.1.10.1.15 Rtools default role

Role name	Role description	Resource	Actions	GrantOption
Rtools administrator	Has all permissions to the Rtools console	26842:drds:rtools:.*	*	0

3.1.10.1.16 MetaCenter default roles

Role name	Role description	Resource	Actions	GrantOption
MetaCenter administrator	Has all permissions to the MetaCenter console	26842:drds:mc:*	*	0
Dayu administrator	Has all Dayu permissions, which allows you to perform operations on all Dayu configurations	26842:drds:dayu:*	*	0

3.1.10.1.17 Dayu default role

Role name	Role description	Resource	Actions	GrantOption
Dayu administrator	Has all Dayu permissions, which allows you to perform operations on all Dayu configurations	26842:drds:dayu:*	*	0

3.1.10.2 Operation permissions of O&M platforms

3.1.10.2.1 ECS Operations and Maintenance System permission list

Resource	Action	Description
26842:ecs	inner_getAllUrls	Basic platform interface
26842:ecs	inner_getCurrentUser	Basic platform interface
26842:ecs	inner_getAccountByldkp	Basic platform interface
26842:ecs	inner_getldkpByAccount	Basic platform interface
26842:ecs	inner_allErrorCode	Basic platform interface
26842:ecs	inner_getOptions	Basic platform interface
26842:ecs	network_allocateIpAddress	Allocates Internet IP addresses

Resource	Action	Description
26842:ecs	network_releaselpAddress	Releases Internet IP addresses
26842:ecs	vm_restart	Restarts an ECS instance
26842:ecs	vm_liveMigrate	Performs a live migration for an ECS instance
26842:ecs	vm_describe	Queries an ECS instance list
26842:ecs	vm_migrate	Migrates an ECS instance in shutdown mode
26842:ecs	vm_describeMountedSnapshots	Queries a mounted snapshot
26842:ecs	vm_resetPassword	Resets the password of an ECS instance
26842:ecs	vm_start	Starts an ECS instance
26842:ecs	vm_stop	Stops an ECS instance
26842:ecs	vm_rename	Changes an ECS instance name
26842:ecs	region_describeRegions	Queries a region list
26842:ecs	group_revoke	Cancels inbound rules of a security group
26842:ecs	group_queryVms	Queries ECS instances in a security group
26842:ecs	group_queryAcls	Queries security group rules
26842:ecs	group_describe	Queries a security group list
26842:ecs	group_authorizeEgress	Authorizes outbound rules of a security group
26842:ecs	group_authorize	Authorizes inbound rules of a security group
26842:ecs	group_revokeEgress	Cancels outbound rules of a security group
26842:ecs	group_leave	Removes instances from a security group
26842:ecs	group_create	Creates a security group

Resource	Action	Description
26842:ecs	group_join	Adds instances to a security group
26842:ecs	group_delete	Deletes a security group
26842:ecs	disk_describe	Queries a disk list
26842:ecs	disk_replaceSystemDisk	Changes a system disk
26842:ecs	disk_attach	Mounts a disk
26842:ecs	disk_detach	Unmounts a disk
26842:ecs	disk_reset	Resets a disk
26842:ecs	nc_queryAvailableNcs	Queries a list of available physical machines
26842:ecs	snapshot_describe	Queries a snapshot list
26842:ecs	snapshot_attach	Mounts a snapshot
26842:ecs	snapshot_detach	Unmounts a snapshot
26842:ecs	snapshot_create	Creates a snapshot
26842:ecs	snapshot_delete	Deletes a snapshot
26842:ecs	vnc_generateUrl	Generates a VNC URL
26842:ecs	image_describe	Queries an image list
26842:ecs	image_create	Creates an image
26842:ecs	image_delete	Deletes an image

3.1.10.2.2 RDS Operations and Maintenance System permission list

Resource	Action	Description
26842:rds	HOME	/
26842:rds	RDS_HOME	/rds/home
26842:rds	COMPONENT_HOME	/component/home
26842:rds	COMPONENT_RGWVIEW	/component/rgwview
26842:rds	COMPONENT_PROXYVIEW	/component/proxysview
26842:rds	COMPONENT_SQLVIEW	/component/sqlview
26842:rds	COMPONENT_BAKVIEW	/component/bakview

Resource	Action	Description
26842:rds	COMPONENT_RGW	/component/rgw
26842:rds	COMPONENT_RGWLIST	/component/rgwlist
26842:rds	COMPONENT_LVS	/component/lvs
26842:rds	COMPONENT_PROXY	/component/proxy
26842:rds	DBS_ACCOUNTS	/dbs/accounts/{insId}
26842:rds	BAK_HIS_LIST	/bakhis/list/{insId}
26842:rds	BAK_OAS_FETCH_LIST	/bakhis/oasfetchlist/{insId}
26842:rds	BAK_FETCH_OAS	/bakhis/fetchoas/{hisId}
26842:rds	SWITCH_VIP	/vip/switch
26842:rds	SYSTEM_ADDMYCNFTEMPLATE	/system/addmycnfTemplate
26842:rds	SYSTEM_DODELETETEMPLATE	/system/dodeletetemplate/{templd}
26842:rds	BAK_REVERT	/bakhis/revert
26842:rds	CLUSTER_HOST	/select/clusterhost
26842:rds	BAK_BINLOG	/bakhis/binlog/{instanceId}
26842:rds	BAK_HIS_SET	/bakhis/bakset/{hisId}/{insId}
26842:rds	BAK_HIS_REVERT	/bak/revert
26842:rds	DBBAK_CREATE	/dbbak/create
26842:rds	BAK_INSTANCE_DBS	/instance/dbsbak/{insId}
26842:rds	RDS_GROUP	/rds/group
26842:rds	GROUP_FINANCE	/group/finance
26842:rds	GROUP_CREATE	/group/create
26842:rds	GROUP_PROFESSION	/group/profession/{groupId}
26842:rds	GROUP_ENTERPRISE	/group/enterprise/{groupId}
26842:rds	GROUP_ADDINS	/group/addins
26842:rds	GROUP_INSTANCE_GID	/group/instance/{groupId}
26842:rds	GROUP_COMMUNICATE	/group/communicate
26842:rds	INSTANCE_DBS_LIST	/instance/dbs/list/{instanceId}

Resource	Action	Description
26842:rds	INSTANCE_DELETEDB_DB SID	/instance/deletedb/{instanceId}
26842:rds	INSTANCE_DBS_DETAIL	/instance/dbs/detail/{dbId}
26842:rds	INSTANCE_DBS_CREATE	/instance/dbs/create
26842:rds	INSTANCE_CREATEREADONLY	/instance/createreadonly/{instanceId}
26842:rds	INSTANCE_CREATEDISASTER	/instance/createdisaster/{instanceId}
26842:rds	GROUP_OTHER	/group/other
26842:rds	GROUP_HOME	Group Management (menu)
26842:rds	GROUP_INDEX	/group/index
26842:rds	GROUP_NUMBER	/group/home/{groupId}
26842:rds	GROUP_HA	/group/ha/{groupId}
26842:rds	GROUP_VIEW	/group/view/{groupId}
26842:rds	GROUP_LIST	/group/list/{groupId}
26842:rds	GROUP_HOST_LIST	/group/hostlist/{groupId}
26842:rds	GROUP_DDL	/group/ddl/{groupId}
26842:rds	USER_INSPROFILE	/user/insprofile/{userId}
26842:rds	GROUP_REMOVE_INSTANCE	/group/remove/{groupId}/{insId}
26842:rds	INSTANCE_LIST	Instance Management (menu)
26842:rds	INSTANCE_CHECK_PASS	/ins/check
26842:rds	INSTANCE_OWNER	/instance/owner
26842:rds	INSTANCE_AUDIT	/instance/audit
26842:rds	INSTANCE_ADDACCOUNT	/instance/addAccount
26842:rds	INSTANCE_ADDACCOUNT_VIEW	/dbs/addaccount/{insId}
26842:rds	INSTANCE_APPLY_POST	/instance/applypost
26842:rds	INSTANCE_UPDATE_POST	/instance/updatepost
26842:rds	INSTANCE_APPLY_PROXY_POST	/instance/proxy/applypost

Resource	Action	Description
26842:rds	INSTANCE_AUDIT_POST	/instance/auditpost
26842:rds	INSTANCE_DOCREATEREADONLY	/instance/docreatereadonly
26842:rds	INSTANCE_DOCREATEDISASTER	/instance/docreatedisaster
26842:rds	PROXY_EDIT_POST	/proxy/editpost
26842:rds	INSTANCE_DETAIL	/instance/detail/{instanceId}
26842:rds	INSTANCE_NOT_NORMAL_DETAIL	/instance/notnormaldetail
26842:rds	INSTANCE_CREATE_NOT_NORMAL	/instance/createnotnormal/{instanceId}
26842:rds	INSTANCE_EDIT_NOT_NORMAL	/instance/editnotnormal/{id}
26842:rds	INSTANCE_DO_EDIT_NOT_NORMAL	/instance/doeditnotnormal
26842:rds	INSTANCE_DELETE_NOT_NORMAL	/instance/deletenotnormal/{id}
26842:rds	SWITCH_GUARD	/host/switchguard/{guardInsId}
26842:rds	DO_SWITCH_GUARD	/host/doswitchguard/{guardInsId}
26842:rds	INSTANCE_DBS	/instance/dbs/{instanceId}
26842:rds	INSTANCE_DELETE	/instance/delete/{instanceId}
26842:rds	INSTANCE_CREATEBAKREADONLYINS	/instance/createbakreadonly/{instanceId}
26842:rds	INSTANCE_MANAGE_POST	/instance/managepost/{clusterId}
26842:rds	INSTANCE_INS_TASK	/instance/instask/{instanceId}
26842:rds	INSTANCE_DIAGONSE	/instance/diagonse/{instanceId}
26842:rds	INSTANCE_TRANS_CLUSTERS	/instance/transcluster/{instanceId}
26842:rds	INSTANCE_ZONE_CLUSTERS	/instance/zonecluster/{instanceId}
26842:rds	INSTANCE_MAGAGE_INS	/instance/manage

Resource	Action	Description
26842:rds	INSTANCE_CUSTLINK_INS	/instance/custlink/{instanceId}
26842:rds	INSTANCE_AUDIT_INS	/instance/insaudit/{instanceId}
26842:rds	INSTANCE_EDIT_INS	/instance/insedit/{instanceId}
26842:rds	INSTANCE_INTIME_INS	/instance/intime/{instanceId}
26842:rds	INSTANCE_KILL_SESSION	/instance/killsession/{instanceId}
26842:rds	INSTANCE_PROXY_LINK	/instance/proxylink/{instanceId}
26842:rds	INSTANCE_DIAGNOSE	/instance/diagnose/{instanceId}
26842:rds	INSTANCE_STATUS	/instance/status/{instanceId}
26842:rds	INSTANCE_CONFIG_INS	/instance/insconfig/{instanceId}
26842:rds	INSTANCE_PREF_INS	/instance/custpref/{instanceId}
26842:rds	INSTANCE_UPDATE_CONFIG	/instance/update/config/{instanceId}
26842:rds	INSTANCE_EXPLAIN_INS	/instance/explain/{instanceId}
26842:rds	INSTANCE_EXCEPTION_INS	/ins/exception/{exceptionId}
26842:rds	MONITOR_EXCEPTION_DELETE	/delete/exception/{exceptionId}
26842:rds	MONITOR_EXCEPTION_UPDATE	/update/exception
26842:rds	INSTANCE_EXCEPTION_INS_BATCH	/ins/batchexception/{exceptions}
26842:rds	EXCEPTION_UPDATE	/exception/update
26842:rds	EXCEPTION_BATCHUPDATE	/exception/batchupdate
26842:rds	INSTANCE_MAGAGE_HOST	/instance/manage/host
26842:rds	INSTANCE_HA_LOGGER	/instance/halogger/{instanceId}
26842:rds	INSTANCE_SLOW	/instance/slow/{instanceId}
26842:rds	INSTANCE_REPORT	/instance/report/{instanceId}
26842:rds	INSTANCE_REPORT_RPT	/instance/reportrpt/{instanceId}
26842:rds	INSTANCE_ACCOUNT	/instance/account/{instanceId}
26842:rds	INSTANCE_OPENPAGE	/instance/openpage/{pageType}/{instanceId}

Resource	Action	Description
26842:rds	INSTANCE_LOCK	/instance/lock/{instanceId}
26842:rds	INSTANCE_ACCOUNT_LIST	/instance/account/list/{instanceId}
26842:rds	DBS_ACCOUNT_LIST	/dbs/account/list/{instanceId}/{dbId}
26842:rds	ACCOUNT_LIST	/account/list
26842:rds	DBS_LIST	/dbs/list
26842:rds	DBS_NEWACCOUNT	/dbs/newaccount/{instanceId}/{dbId}
26842:rds	DBS_ACCOUNT_CONFIG	/dbs/account/config/{instanceId}/{accountId}
26842:rds	DBS_ACCOUNT_PROXY_INFO	/dbs/account/proxy/{instanceId}/{accountId}
26842:rds	DO_DBS_ACCOUNT_CONFIG	/dbs/account/update/{instanceId}/{dbId}/{accountId}
26842:rds	DBS_ACCOUNT_CHANGE_PASSWORD	/dbs/account/changepasswod/{instanceId}/{accountId}
26842:rds	DO_DBS_ACCOUNT_CHANGE_PASSWORD	/dbs/account/dochangepasswd/{instanceId}/{accountId}
26842:rds	DBS_ACCOUNT_RESET_PASSWORD	/dbs/account/resetpasswd/{instanceId}/{accountId}
26842:rds	DO_DBS_ACCOUNT_RESET_PASSWORD	/dbs/account/doreset/{instanceId}/{accountId}
26842:rds	DBS_ACCOUNT_DELETE	/dbs/account/delete/{instanceId}/{accountId}
26842:rds	ADD_DBS_ACCOUNT	/dbs/account/add/{instanceId}/{dbId}
26842:rds	TRANS_DBS	/dbs/trans
26842:rds	DBS_MODIFYPRIVILEGE	/dbs/modifyprivilege/{dbId}/{accountId}/{custinsId}/{accountTyp}
26842:rds	INSTANCE_UNLOCK	/instance/unlock/{instanceId}
26842:rds	INSTANCE_CONFIG_PROXY	/instance/config/{instanceId}

Resource	Action	Description
26842:rds	INSTANCE_CONFIG_SYNC	/instance/sync/{instanceId}
26842:rds	INSTANCE_RESTART	/instance/restart/{instanceId}
26842:rds	INSTANCE_CLEARLOG	/instance/clearlog/{instanceId}
26842:rds	INSTANCE_CHANGE	/instance/change/{instanceId}
26842:rds	DBS_ACCOUNT	/dbs/account/{instanceId}
26842:rds	INSTANCE_BACKUP	/instance/backup/{instanceId}
26842:rds	INSTANCE_BACKUP_CREATE	/instance/backup/create
26842:rds	INSTANCE_BACKUP_UPDATE	/instance/backup/update
26842:rds	INSTANCE_REBUILD_HA	/instance/rebuildha
26842:rds	INSTANCE_APPLY	/instance/apply
26842:rds	INSTANCE_CONFIGSQLWALL	/instance/configsqlwall
26842:rds	INSTANCE_MULTITRANS	/instance/multitrans
26842:rds	INSTANCE_DOMULTITRANS	/instance/domultitrans
26842:rds	INSTANCE_CONFIGPROXYMODE	/instance/configProxyMode
26842:rds	INSTANCE_PASS	/instance/pass/{instanceId}
26842:rds	INSTANCE_UNPASS	/instance/unpass/{instanceId}
26842:rds	INSTANCE_DBCONFIG	/instance/dbconfig/{pageType}/{instanceId}
26842:rds	INSTANCE_TUNE	/instance/tune/{opType}/{instanceId}
26842:rds	SQL_DETAIL	/sql/detail
26842:rds	SLOWSQL_DETAIL	/slowsql/detail
26842:rds	INSTANCE_SQL_SLOW_LOG	/instance/slowsql/{custinsId}
26842:rds	SLOWLOG_DETAIL	/slowLog/detail/{instanceId}/{analysId}
26842:rds	MONITOR_WARNING_DETAIL	/monitor/warndetail

Resource	Action	Description
26842:rds	INSTANCE_LOG	/instance/log/{opType}/{instanceId}
26842:rds	INSTANCE_TRANS	/instance/trans/{opType}/{instanceId}
26842:rds	TRANS_AUDIT	/trance/audit
26842:rds	INSTANCE_TRANS_DETAIL	/instance/trans/detail/{opType}/{transId}
26842:rds	INSTANCE_TRANS_UPDATE	/instance/trans/update/{transId}
26842:rds	INSTANCE_TRANS_CANCEL	/instance/trans/cancel/{transId}
26842:rds	INSTANCE_TRANS_APPLY	/instance/trans/apply/{instanceId}
26842:rds	INSTANCE_TRANS_APPLY POST	/instance/trans/applypost
26842:rds	INSTANCE_TRANS_CHECK POST	/instance/trans/checkpost
26842:rds	INSTANCE_TRANS_DBPOST	/instance/trans/dbpost
26842:rds	INSTANCE_TRANS_DB	/instance/trans/db/{instanceId}
26842:rds	INSTANCE_TRANS_OPENPAGE	/instance/trans/openpage/{pageType}/{transId}
26842:rds	GET_INSTANCE_TRANS_HOST	/select/trans/host
26842:rds	GET_INSTANCE_TRANS_CUSTINS	/select/trans/custins/{instanceId}
26842:rds	GET_INSTANCE_TRANS_DB	/select/trans/db
26842:rds	INSTANCE_UPDATECONFIG	/instance/updateconfig/{paramId}
26842:rds	INSTANCE_UPDATE_AURA RO	/instance/auraro/{custinsId}
26842:rds	CLUSTER_LIST	/cluster/list
26842:rds	USSER_PROFILE_LIST	/user/profile/{userId}
26842:rds	USSER_PROFILE_ALL_LIST	/user/profilelist/{userId}
26842:rds	USSER_ALIYUN_INFO	/user/aliyuninfo

Resource	Action	Description
26842:rds	CLUSTER_NEW	/cluster/new
26842:rds	CLUSTER_ERROR	/cluster/error
26842:rds	ERROR_RE_SUBMIT	/error/resubmit
26842:rds	CLUSTER_UPCONIFG	/cluster/upconfig
26842:rds	CLUSTER_NODELIST	/cluster/nodelist/{clusterId}
26842:rds	CLUSTER_NODE	/cluster/node
26842:rds	CLUSTER_EDITNODE	/cluster/editnode/{nodeId}
26842:rds	CREATE_NODE	/node/create
26842:rds	UPDATE_NODE	/node/update
26842:rds	CLUSTER_CREATE	/cluster/create
26842:rds	CLUSTER_FLUSHWHITE	/cluster/flushwhite
26842:rds	FLUSH_SYNC_MODE	/flush/syncmode
26842:rds	FLUSH_RESOURCE	/flush/resource
26842:rds	CHECK_INSNAME	/check/insName
26842:rds	CHECK_CONNADDRRCUST	/check/connAddrCust
26842:rds	DEL_NODE_ID	/del/node/{nodeId}
26842:rds	DEL_CLUSTER_ID	/del/cluster/{clusterId}
26842:rds	FETCH_BAK_URL	/bak/url
26842:rds	FETCH_BAK_BINLOG_URL	/bak/binlogurl
26842:rds	CHECK_DBNAME	/check/dbName
26842:rds	EXCEPTION_HOME	/exception/home
26842:rds	EXCEPTION_LIST	/exception/list/{targetType}
26842:rds	RESOURCE_HOME	/resource/home
26842:rds	HOST_CONFIG	/host/config/{hostIds}
26842:rds	HOST_UPCONFIG	/host/upconfig
26842:rds	RESOURCE_REGION	/resource/region
26842:rds	RESOURCE_MORE	/resource/more
26842:rds	HOST_CREATE	/host/create
26842:rds	HOST_UPDATE	/host/update

Resource	Action	Description
26842:rds	RESOURCE_HA	/resource/ha
26842:rds	RESOURCE_HOSTBUFFER	/resource/hostbuffer
26842:rds	RESOURCE_HOST	Host Management (menu)
26842:rds	RESOURCE_IP	/resource/ip
26842:rds	RESOURCE_SERVICE	/resource/service
26842:rds	RESOURCE_BAKOWNER_TYPE	/resource/bakownertype
26842:rds	RESOURCE_CREATE_BAKOWNER_TYPE	/resource/create/bakownertype
26842:rds	RESOURCE_DELETE_BAKOWNER_TYPE	/resource/delete/bakownertype
26842:rds	RESOURCE_EDIT_BAKOWNER_TYPE	/resource/edit/bakownertype
26842:rds	RESOURCE_UPDATE_BAKOWNER_TYPE	/resource/update/bakownertype
26842:rds	CLUSTER_UPDATERES	/cluster/updateres
26842:rds	LOGGER_HOME	/logger/home
26842:rds	LOGGER_USER	/logger/user
26842:rds	LOGGER_HA	/logger/ha
26842:rds	LOGGER_TRANS	/logger/trans
26842:rds	LOGGER_RECOVER	/logger/recover
26842:rds	LOGGER_REMOTE	/logger/remote
26842:rds	LOGGER_BACKUP	/logger/backup
26842:rds	LOGGER_API	/logger/api
26842:rds	INSTANCE_APILOG	/instance/apilog/{custinsId}
26842:rds	INSTANCE_ADMINLOG	/instance/adminlog/{custinsId}
26842:rds	LOGGER_RESOURCE	/logger/resource/{logId}
26842:rds	HOST_HOME	/host/home/{hostId}
26842:rds	HOST_INSPREF	/host/inspref/{insId}/{custInsId}
26842:rds	HOST_SWITCH	/host/switch/{insId}
26842:rds	HOST_BATCH_SWITCH	/host/batchswitch/{insIds}

Resource	Action	Description
26842:rds	HOST_BATCH_TRANS_INS	/host/batchTransIns/{insIds}
26842:rds	HOST_PREF	/host/pref/{hostId}
26842:rds	HOST_INFO	/host/info/{hostId}
26842:rds	HOST_INSTANCE	/host/instance/{hostId}
26842:rds	HOST_NEW	/host/new
26842:rds	HOST_DOSWITCH	/host/doswitch/{hostId}
26842:rds	HOST_TASK	/host/task/{hostId}
26842:rds	HOST_TASKS	/host/hosttask
26842:rds	HOST_DOBATCH_SWITCH	/host/doBatchswitch/{hostId}
26842:rds	HOST_DOBATCH_TRANS_I NS	/host/doBatchTransIns/{ custInsIds}
26842:rds	HOST_EDIT	/host/edit/{hostId}
26842:rds	HOST_PREF_DEATIL	/host/pref/detail/{hostId}
26842:rds	HOST_DELETE_HOSTID	/host/delete/{hostId}
26842:rds	HOST_CHECK_HOSTID	/host/check/{hostId}
26842:rds	INS_PREF_DEATIL	/ins/pref/detail/{insId}
26842:rds	CUST_PREF_DEATIL	/cust/pref/detail/{insId}
26842:rds	TASK_HOME	/task/home
26842:rds	TASK_FAIL	Task Management (menu)
26842:rds	TRANCE_LIST	/trance/list
26842:rds	TASK_RUN	/task/run
26842:rds	TASK_STEP	/task/step/{taskId}
26842:rds	TASK_CLOSE	/task/close
26842:rds	TASK_START	/task/start
26842:rds	TASK_FLOW	/task/flow/{taskId}
26842:rds	TASK_STAT	/task/stat
26842:rds	TASK_FLOWEXE	/task/flowexe/{taskId}
26842:rds	TASK_HISTORY	/task/history/{taskId}
26842:rds	TASK_LOOGER	/task/logger

Resource	Action	Description
26842:rds	REPORT_HOME	Resource Management (menu)
26842:rds	REPORT_CLUSTER	/report/cluster
26842:rds	REPORT_ZONE	/report/zone
26842:rds	RESOURCE_HOSTINFO	/resource/hostinfo
26842:rds	RESOURCE_VIPINFO	/resource/vipinfo
26842:rds	REPORT_REGIONNAME	/report/regionName/{regionName}
26842:rds	USER_DELETE	/user/delete/{userId}
26842:rds	ROLE_DELETE	/role/delete/{roleId}
26842:rds	DRC_HOME	/drc/home
26842:rds	DRC_PRECHECK	/drc/preCheck
26842:rds	DRC_PRESCHECK	/drc/presCheck
26842:rds	DRC_COMMIT	/drc/commit
26842:rds	DRC_LIST	/drc/func/{opType}
26842:rds	CHECK_HOME	Inspection Information (menu)
26842:rds	SYSTEM_HOME	/system/home
26842:rds	SYSTEM_USER	/system/user
26842:rds	SYSTEM_INSIDC	/system/insidc
26842:rds	SYSTEM_INSIDC_LSIT	/system/insidcs
26842:rds	SYSTEM_MEASUREDATA	/system/measuredata
26842:rds	SYSTEM_COUNTDATA	/system/count
26842:rds	SYSTEM_BOSS	/system/boss/{recordId}
26842:rds	SYSTEM_PERMISSION	/system/permission/{roleId}
26842:rds	SYSTEM_UPDATEPERMISSION	/system/updatePermission
26842:rds	SYSTEM_UPDATEROLE	/system/updateRole
26842:rds	SYSTEM_TANCEDENCY	/system/tancedency
26842:rds	SYSTEM_CFCREATE_TANCEDENCY	/system/create/tancedency
26842:rds	SYSTEM_REGION	/system/region

Resource	Action	Description
26842:rds	SYSTEM_CFCREATE_REGION	/system/create/region
26842:rds	DELETE_REGION_ID	/delete/region/{locationMetaId}
26842:rds	SYSTEM_DELETE_TANCED ENCY	/system/delete/tancedency/{id}
26842:rds	SYSTEM_CREATE_HOSTBU FFERSN	/system/create/hostbuffersn
26842:rds	SYSTEM_CREATEROLE	/system/createRole
26842:rds	SYSTEM_CREATEPERMISS ION	/system/createPermission
26842:rds	USER_UPDATE_ROLE	/update/role
26842:rds	USER_UPDATE_CLUSTER	/update/usercluster
26842:rds	GET_INSTANCE_LEVEL	/select/inslevel
26842:rds	ROLE_LIST	/role/list
26842:rds	ROLE_NEW	/role/new
26842:rds	PERMISSION_NEW	/permission/new
26842:rds	ROLE_UPDATE	/role/update/{roleId}
26842:rds	USER_ROLE_EDIT	/role/edit/{userId}
26842:rds	USER_ADD_ROLECLUSTER	/add/rolecluster/{userId}
26842:rds	USER_ADD_RESOURCE	/addkey/resource
26842:rds	SYSTEM_DELETE_RESOUR CE	/delete/resource/{resId}
26842:rds	USER_UPDATE_RESOURCE	/updatekey/resource
26842:rds	SYSTEM_SALES	System Management (menu)
26842:rds	INSLEVEL_PARAMS	/inslevel/params/{paramsId}
26842:rds	INSLEVEL_ADDPARAMS	/inslevel/addparams/{levelId}
26842:rds	SYSTEM_TEMPLATE	/system/template
26842:rds	SYSTEM_NEWTEMPLATE	/system/newtemplate
26842:rds	SYSTEM_DODELETEPARAM ID	/system/dodeleteparamid/{ paramsId}
26842:rds	SYSTEM_DOSAVEINSLEVEL	/system/dosaveinsLevel/{ paramsId}

Resource	Action	Description
26842:rds	SYSTEM_EDITTEMPLATE	/system/edittemplate/{templd}
26842:rds	SYSTEM_DOEDITMYCNFTE MPLATE	/system/doEditmycnfTemplate
26842:rds	SYSTEM_PREF	/system/pref
26842:rds	SYSTEM_SOFTLIST	/system/softlist
26842:rds	SYSTEM_SOFTWARE	/system/software
26842:rds	SYSTEM_IPFILTER	/system/ipfilter
26842:rds	SYSTEM_ADD_IPFILTER	/system/addIpFilter
26842:rds	SYSTEM_DELETE_IPFILTER	/system/deleteIpFilter/{ruleId}
26842:rds	BOSS_SEND	/boss/send/{recordId}
26842:rds	SYSTEM_SETTING	/system/setting
26842:rds	SYSTEM_GROUP	/system/group
26842:rds	SYSTEM_FEACHDATA	/system/feachdata
26842:rds	SYSTEM_OPERATORS	/system/operators
26842:rds	SYSTEM_CREATE_OPERATOR	/system/create/operator
26842:rds	SYSTEM_TO_UPDATE_OPERATOR	/system/toupdate/operator
26842:rds	SYSTEM_UPDATE_OPERATOR	/system/update/operator
26842:rds	SYSTEM_DELETE_OPERATOR	/system/delete/operator
26842:rds	SYSTEM_GROUP_SUBSCRIBE_WARN	/system/groupsubscribe/warn
26842:rds	SYSTEM_NEW_LEVEL	/system/newlevel
26842:rds	SYSTEM_EDIT_LEVEL	/system/editlevel/{levelId}
26842:rds	SYSTEM_DO_NEW_LEVEL	/system/donewlevel
26842:rds	SYSTEM_DO_UPDATE_LEVEL	/system/doupdatelevel
26842:rds	SYSTEM_DO_DELETE_LEVEL	/system/dodeletelevel/{levelId}

Resource	Action	Description
26842:rds	SYSTEM_NEW_HOST_LEVEL	/system/newHostLevel
26842:rds	SYSTEM_EDIT_HOST_LEVEL	/system/editHostLevel/{levelId}
26842:rds	SYSTEM_EDIT_GROUP	/system/editgroup/{groupId}
26842:rds	SYSTEM_DO_EDIT_GROUP	/system/doeditgroup
26842:rds	SYSTEM_DO_SAVE_HOST_LEVEL	/system/donewhostlevel
26842:rds	SYSTEM_DO_UPDATE_HOST_LEVEL	/system/doupdatehostlevel
26842:rds	SYSTEM_DO_DELETE_HOST_LEVEL	/system/dodeletehostlevel/{levelId}
26842:rds	SYSTEM_WATCH	/system/watch
26842:rds	SYSTEM_UPLOAD_IMAGE	/system/uploadimage
26842:rds	SYSTEM_MODIFY_IMAGE	/system/modifyimage
26842:rds	SYSTEM_MODIFY_WATCH	/system/modifywatch
26842:rds	CHECK_ACCOUNT	/check/account/{instanceId}/{dbId}
26842:rds	REFLUSH_TRANCES_DENY	/reflush/trance
26842:rds	REFLUSH_USER_CLUSTER	/reflush/usercluster
26842:rds	REFLUSH_USER_ROLE	/reflush/userrole
26842:rds	SYSTEM_HOSTBUFFER	/system/hostbuffer
26842:rds	SYSTEM_HOSTBUFFER_DELETE	/system/delete/hostbuffer/{id}
26842:rds	INSTANCE_SQLWALL	/instance/sqlwall
26842:rds	INSTANCE_SQLWALLCHECK	/instance/sqlwallCheck
26842:rds	INSTANCE_SQLWALLCHECKS	/instance/sqlwallChecks
26842:rds	INSTANCE_SQLWALLS	/instance/sqlwalls
26842:rds	REPORT_EXTRA_PURCHASE	/report/purchase

Resource	Action	Description
26842:rds	REPORT_EXTRA_PURCHASE_PSOT	/report/purchase/post
26842:rds	INSTANCE_BAKHIS_MODIFY	/bakhis/modify/{custinsId}
26842:rds	SYSTEM_CREATE_SITENAME	/system/create/sitename
26842:rds	SYSTEM_SITENAME	/system/sitename
26842:rds	SYSTEM_INSPERF	/system/insperf
26842:rds	DELETE_SITENAME_ID	/delete/sitename/{id}
26842:rds	PROXY_GROUP_HOME	/proxy/group/home
26842:rds	PROXY_CLUSTER	Important Components (menu)
26842:rds	TO_CREATE_PROXY_CLUSTER	/proxy/tocreate/proxycluster
26842:rds	CREATE_PROXY_CLUSTER	/proxy/create/proxycluster
26842:rds	TO_UPDATE_PROXY_CLUSTER	/proxy/toupdate/proxycluster
26842:rds	UPDATE_PROXY_CLUSTER	/proxy/update/proxycluster
26842:rds	TO_CREATE_PROXY_NODE	/proxy/tocreate/proxynode
26842:rds	CREATE_PROXY_NODE	/proxy/create/proxynode
26842:rds	TO_UPDATE_PROXY_NODE	/proxy/toupdate/proxynode
26842:rds	UPDATE_PROXY_NODE	/proxy/update/proxynode
26842:rds	TO_UPDATE_PROXY_API_NODE	/proxy/toupdate/proxyapinode
26842:rds	UPDATE_PROXY_API_NODE	/proxy/update/proxyapinode
26842:rds	DELETE_PROXY_NODE	/proxy/delete/proxynode
26842:rds	DELETE_PROXY_API_NODE	/proxy/delete/proxyapinode
26842:rds	PROXY_DETAIL	/proxy/proxydetail
26842:rds	CREATE_PROXY_CLUSTER_GROUP	/proxy/create/proxyclustergroup
26842:rds	EDIT_NODE_TO_GROUP	/proxy/editnodetogroup
26842:rds	TO_EDIT_NODE_TO_GROUP	/proxy/to/editnodetogroup
26842:rds	NET_VIEW	/net/view

Resource	Action	Description
26842:rd	NET_VIEW_NET_TIME	/net/viewtime
26842:rd	COMPONENT_OSS	/component/oss
26842:rd	COMPONENT_HA	/component/ha
26842:rd	COMPONENT_HA_LOAD	/component/haload
26842:rd	COMPONENT_HA_SWITCH_RECORD	/component/haswitchrecord
26842:rd	COMPONENT_HA_API	/component/haapi
26842:rd	COMPONENT_HA_EXCEPTION	/component/haexception
26842:rd	COMPONENT_SWITCH_DETAIL	/component/switch/detail
26842:rd	COMPONENT_SWITCH_API_TREND	/component/switchapi/trend
26842:rd	COMPONENT_BAK	/component/bak
26842:rd	PROXY_GROUP_OFFLINE	/proxy/group/offline
26842:rd	PROXY_GROUP_ONLINE	/proxy/group/online
26842:rd	PROXY_GROUP_SLB	/proxy/group/slb
26842:rd	PROXY_GROUP_API	/proxy/group/api
26842:rd	SLB_VIEW	/slb/view/{bakOwnerId}/{custId}
26842:rd	MONITOR_HOME	/monitor/home/{opType}
26842:rd	MONITOR_DETAIL_TYPE	/monitor/detail/{opType}
26842:rd	PROXY_VIEW	/proxy/view/{bakOwnerId}/{custId}
26842:rd	MONITOR_INDEX	Monitoring Dashboard (menu)
26842:rd	MONITOR_CREATE_SUBSCRIBER	/monitor/create/subscriber
26842:rd	MONITOR_REMOVE_SUBSCRIBER	/monitor/remove/subscriber
26842:rd	SUBSCRIBER_MANAGER	/subscriber/manager
26842:rd	SUBSCRIBER_CREATE	/subscriber/create
26842:rd	SUBSCRIBER_UPDATE	/subscriber/update

Resource	Action	Description
26842:rds	SUBSCRIBER_DELETE	/subscriber/delete
26842:rds	MONITOR_ERROR	/monitor/error
26842:rds	MONITOR_TREND_DETAIL	/monitor/trenddetail/{opType}
26842:rds	CLOUD_HOME_STAT	/report/cloud/stat
26842:rds	SYSTEM_API_MANAGE	/system/keymanage
26842:rds	SYSTEM_API_ADDKEY	/system/addkey
26842:rds	SYSTEM_API_DOADDKEY	/system/doaddkey
26842:rds	SYSTEM_API_DODELETEKEY	/system/dodeletekey/{id}
26842:rds	API_ADD_ECS_IP_FILTER	/api/addecsipfilter
26842:rds	API_SHOW_ECS_IP_FILTER	/api/showecsipfilter
26842:rds	CLOUD_HOME	/cloud/home
26842:rds	CLOUD_APPLY_POST	/instance/cloudpost
26842:rds	CLOUD_GROUP_LIST	/cloud/group/list
26842:rds	CLOUD_INS_LIST	/cloud/inst/list
26842:rds	CLOUD_GROUP_MANAGER	/cloud/group/manager
26842:rds	CLOUD_GROUP_CREATE	/cloud/creategroup
26842:rds	CLOUD_DO_GROUP_CREATE	/cloud/docreategroup
26842:rds	CLOUD_EDIT_GROUP	/cloud/editgroup/{groupId}
26842:rds	CLOUD_DO_EDIT_GROUP	/cloud/doeditgroup
26842:rds	CLOUD_APPLY	/cloud/apply
26842:rds	CLOUD_GROUP_ADDINS	/cloud/group/addins
26842:rds	CLOUD_GROUP_INS	/cloud/group/ins/{groupId}
26842:rds	CLOUD_GROUP_INSPROFILE	/cloud/group/insprofile/{groupId}
26842:rds	CLOUD_GROUP_INSTANCE_LOCK	/cloud/group/lockinst/{groupId}
26842:rds	CLOUD_GROUP_INSTANCE_UNLOCK	/cloud/group/unlockinst/{groupId}
26842:rds	CLOUD_GROUP_CLEARLOG	/cloud/group/clearlog/{groupId}

Resource	Action	Description
26842:rds	CLOUD_GROUP_RESTART	/cloud/group/restart/{groupId}
26842:rds	CLOUD_GROUP_UPDATE_AURARO	/cloud/group/auraro/{groupId}
26842:rds	CLOUD_GROUP_BATCH_SWITCH	/cloud/group/batchswitch/{groupId}
26842:rds	CLOUD_GROUP_DOBATCH_SWITCH	/cloud/group/doBatchswith/{groupId}
26842:rds	CLOUD_GROUP_ATTENTION	/cloud/group/attenGroup/{groupId}
26842:rds	CLOUD_MY_GROUP_ATTENTION	/cloud/home/myAttenGroup
26842:rds	USERGROUP_USER_GROUP	/usergroup/usergroup
26842:rds	USERGROUP_CREATE_USER_GROUP	/usergroup/createusergroup
26842:rds	USERGROUP_EDIT_USER_GROUP	/usergroup/editusergroup/{groupId}
26842:rds	USERGROUP_OF_EDIT_ROLE	/usergroup/editroleofusergroup/{groupId}
26842:rds	USERGROUP_OF_DO_EDIT_ROLE	/usergroup/doeditroleofusergroup
26842:rds	USERGROUP_OF_EDIT_CLUSTER	/usergroup/editclusterofusergroup/{groupId}
26842:rds	USERGROUP_OF_SEARCH_CLUSTER	/usergroup/searchclusterofusergroup/{groupId}
26842:rds	USERGROUP_OF_DO_EDIT_CLUSTER	/usergroup/doeditclusterofusergroup
26842:rds	USERGROUP_OF_EDIT_INS	/usergroup/searchinsofusergroup
26842:rds	USERGROUP_OF_SEARCH_INS	/usergroup/searchinsofusergroup/{page}
26842:rds	USERGROUP_OF_DO_EDIT_INS	/usergroup/doeditinsofusergroup

Resource	Action	Description
26842:rds	USERGROUP_OF_EDIT_USER	/usergroup/searchuserofusergroup
26842:rds	USERGROUP_OF_SEARCH_USER	/usergroup/searchuserofusergroup/{page}
26842:rds	USERGROUP_OF_DO_EDIT_USER	/usergroup/doedituserofusergroup
26842:rds	USERGROUP_DO_EDIT_USER_GROUP	/usergroup/doeditusergroup
26842:rds	USERGROUP_DELETE_USER_GROUP	/usergroup/deleteusergroup/{groupid}
26842:rds	CUSTINS_LOGS	/instance/custinslog
26842:rds	DATA_SQLCOMAND	/data/sqlcommand/{custId}
26842:rds	DATA_SQLCOMAND_SHOWDATABASE	/data/sqlCommand/showDataBases/{custId}
26842:rds	DATA_SQLCOMAND_EXECUTE	/data/sqlCommand/execute
26842:rds	DATA_SQLCOMAND_CANCEL	/data/sqlCommand/cancel
26842:rds	TABLE_DETAIL	/instance/tabledetail
26842:rds	COLUMN_DETAIL	/instance/columndetail/{instanceId}
26842:rds	WARN_MANAGER_THRESHOLD	/instance/warn/threshold
26842:rds	WARN_MANAGER_CREATE_CONTACT	/instance/warn/createcontact
26842:rds	WARN_MANAGER_UPDATE_THRESHOLD	/instance/warn/updatecontact
26842:rds	WARN_MANAGER_DELETE_CONTACTS	/instance/warn/deletecontact
26842:rds	INSTANCE_SWITCH_INSTANCE	/instance/switch/{instanceId}
26842:rds	INSTANCE_OPERATOR_PERMISSION	Instance operations on the instance details page, including restarting an instance

Resource	Action	Description
		, active/standby switchover, disabling HA, enabling HA, rebuilding a standby database, deleting an instance, creating a read-only instance, creating a standby read-only instance, and creating a disaster recovery instance
26842:rds	INSTANCE_CREATE_BY_AMORAYAPI	Creates an instance by using an Amoray API
26842:rds	INSTANCE_CREATE_NOT_NORMAL	Creates a nonstandard instance
26842:rds	GROUP_INSTANCE_VIEW_WARN	Views the instance group alarm contacts
26842:rds	GROUP_INSTANCE_DELETE_WARN	Deletes the instance group alarm contacts
26842:rds	INSTANCE_LOG_PAGE	Instance Management - Historical Availability - View Error Logs (Paging)
26842:rds	INSTANCE_BATCH_APPLY	Welcome - Instance Application in Batches
26842:rds	INSTANCE_PROXYLIST	/instance/proxylist/
26842:rds	INSTANCE_SWITCHLINK	/instance/switchLink
26842:rds	COMPONENT_SLB_CLUSTER	Important Components - SLB O&M Management - SLB Cluster
26842:rds	COMPONENT_RDS_CLUSTER	Important Components - SLB O&M Management - RDS Cluster
26842:rds	PROXY_TO_USE_NODE_TEMPLATE	Important Components - Proxy Cluster Information - Feature Enabling/Disabling Page
26842:rds	PROXY_USE_NODE_TEMPLATE	Important Components - Proxy Cluster Information - Feature Enabling/Disabling Page - Enabling

Resource	Action	Description
26842:rds	HOST_BAKINFO	Host Management - Host Backup Information
26842:rds	HOST_RTTIME	Host Management - Host Response Time
26842:rds	CONNECTIVITY_CHECK	Important Components - Connectivity Check
26842:rds	CONNECTIVITY_MAIL	System Management - Subscription Management - Send Resource Information
26842:rds	DATA_SQLCOMAND	Instance Management - Instance Diagnosis - Execute SQL
26842:rds	RESOURCE_OVERVIEW	Resource Management - Regional Resources - Resource Overview
26842:rds	HOST_BIANQUE	Instance Management - Basic Information - Performance Graph
26842:rds	GROUP_INSTANCE_THRES HOLD	System Management - Group Management - Alarm
26842:rds	CUSTINS_DATA_LINK	Instance Management - Data Link
26842:rds	INSTANCE_MULTIREFRESH	Instance Management - Instance Management in Batches - Refresh Instance Parameters in Batches
26842:rds	INSTANCE_MYSQL_OPERA TE	Views the MySQL space size
26842:rds	HOST_INTIME	Real-time host information
26842:rds	INSTANCE_MYSQL_OPERA TE	MySQL instance operations
26842:rds	INSTANCE_UPLOAD_POLI CY	Enables backup or not
26842:rds	HOST_RESTART	HOST_RESTART
26842:rds	ROBOT_LOG	Robot management

Resource	Action	Description
26842:rds	ROBOT_ROBOT	Robot switch control
26842:rds	INSTANCE_MYSQL_SPACE	Views the MySQL space size
26842:rds	INSTANCE_SLA	Instance SLA
26842:rds	TASK_INFO	Task information
26842:rds	OS_CONFIG	Views and deletes Linux kernel parameter configurations
26842:rds	UPDATE_OS_CONFIG	Adds and modifies Linux kernel parameter configurations
26842:rds	OPERATE_WATCH	Operation announcements and duty sheets
26842:rds	CUSTINS_PANORAMA	Instance panorama
26842:rds	COMPONENT_INCONSIST	Integration test
26842:rds	RDS_DATA	RDS homepage summary data
26842:rds	ROBOT_LOG	Robot logs
26842:rds	HOST_COMMAND	Host commands
26842:rds	CREATE_SUPER_ACCOUNT	Creates a super account
26842:rds	PACKAGE_SPEC_OPERATION	Package modification authorization key
26842:rds	TASK_TRACE	Tracks failed tasks
26842:rds	INSTANCE_OPENSSL	Enables SSL
26842:rds	INSTANCE_CONFIG_INS_OP	Modifies the whitelist
26842:rds	BAK_HIS_LIST_FETCH	Obtains the download link of the backup set
26842:rds	ACCESS_GRANTACCOUNT	Authorization page for instance account access
26842:rds	INSTANCE_BATCH_HSWITH	Instance HA switchover in batches
26842:rds	COMPONENT_AUTOTEST	Automated test

3.1.10.2.3 Storage Operations and Maintenance System permission list

Resource	Action	Description
26842:oss	get_env_get_env	Basic platform interface
26842:oss	get_location_tree	Basic interface used to obtain region, cluster, and group information
26842:oss	get_location_tree2	Basic interface used to obtain region, cluster, and group information
26842:oss	get_location_all	Basic interface used to obtain region, cluster, and group information
26842:oss	get_quota_quota	Obtains the basic user quota data
26842:oss	get_vip_vip_list	Obtains user VIP information
26842:oss	get_quota_run_monitor	Obtains monitoring data
26842:oss	get_ocm_bucket	Obtains basic attribute information of buckets
26842:oss	get_quota_datasize	Obtains the storage size
26842:oss	get_quota_bucket_resource	Obtains a bucket list
26842:oss	get_user_info	Obtains user information
26842:oss	get_quota_overview	Obtains monitoring data
26842:oss	get_quota_sla	Obtains SLA data
26842:oss	get_ocm_buckets	Obtains the bucket list information
26842:oss	post_vip_vip_list	Adds user VIP information
26842:oss	delete_vip_vip_list	Deletes user VIP information
26842:oss	post_pop_cluster_inventory	Obtains the cluster inventory information
26842:oss	get_quota_region_storage	Obtains the cluster storage information
26842:oss	get_quota_region_bucket_stat	Obtains the cluster bucket list
26842:oss	get_quota_region_object	Obtains the cluster object list

Resource	Action	Description
26842:oss	get_quota_region_monitor	Obtains monitoring data
26842:oss	get_quota_region_stat	Obtains monitoring data
26842:oss	get_quota_region_overview	Obtains monitoring data
26842:oss	get_quota_region_cluster_type_stat	Obtains the cluster type
26842:oss	get_quota_region_today_cluster_type_overview	Obtains the cluster day data
26842:oss	get_quota_region_inventory	Obtains the cluster type
26842:oss	get_quota_region_mns_active	Obtains the cluster MNS data
26842:oss	get_quota_top_min_time	Obtains the cluster usage ranking data.
26842:oss	get_quota_top_storage	Obtains the cluster storage ranking data
26842:oss	get_quota_top_storage_increment	Obtains the cluster traffic ranking data
26842:oss	get_quota_top_request	Obtains the ranking data for the number of cluster requests
26842:oss	get_quota_top_sys_error	Obtains the ranking data for the cluster internal errors
26842:oss	get_quota_top_pub_traffic_out	Obtains the cluster traffic ranking data
26842:oss	get_quota_top_pub_traffic_in	Obtains the cluster traffic ranking data
26842:oss	get_quota_top_pri_traffic_out	Obtains the cluster traffic ranking data
26842:oss	get_quota_top_pri_traffic_in	Obtains the cluster traffic ranking data
26842:oss	get_quota_top_cdn_in	Obtains the cluster traffic ranking data
26842:oss	get_quota_top_cdn_out	Obtains the cluster traffic ranking data
26842:oss	get_disk_status_summary	Obtains the disk status
26842:oss	get_disk_status	Obtains the disk status

Resource	Action	Description
26842:oss	get_disk_usage_summary	Obtains the disk usage status
26842:oss	get_disk_usage_history	Obtains the historical disk status
26842:oss	get_disk_usage	Obtains the disk status
26842:oss	get_disk_usage_details	Obtains the disk status
26842:oss	get_audit_op_log	Queries operation logs

3.1.10.2.4 SLB/VPC Operations and Maintenance System permission list

Resource	Action	Description
26842:slb:*	read	Queries common Server Load Balancer data
26842:slb:slb/tools/collect-version-status	create	slb/tools/collect-version-status
26842:slb:slb/tools/collect-kernel-status	create	slb/tools/collect-kernel-status
26842:slb:slb/tools/collect-specifications-status	create	slb/tools/collect-specifications-status
26842:slb:slb/deployment/createClusterDeployTask	create	Creates a cluster deployment task
26842:slb:slb/deployment/deleteClusterDeployTask	delete	Deletes a cluster deployment task
26842:slb:slb/deployment/renameClusterDeployTask	update	Renames a cluster deployment task
26842:slb:slb/deployment/updateNetworkInfo	update	Updates the network information obtained during deployment
26842:slb:slb/deployment/updateAppInfo	update	Updates the application information obtained during deployment
26842:slb:slb/deployment/updateInfo	update	slb/deployment/updateInfo
26842:vpc:*	read	Queries the VPC data
26842:vpc:vpc-base-service/bflag/create	create	Creates a bflag resource

Resource	Action	Description
26842:vpc:capture/add-capture-task	create	capture/add-capture-task
26842:vpc:vpc-base-service/bflag/delete	delete	Deletes a bflag resource
26842:vpc:vpc-base-service/bflag/update	update	Updates a bflag resource
26842:vpc:vpc-inner/flow/compensate	update	vpc-inner/flow/compensate
26842:vpc:vpc-inner/flow/disable	update	vpc-inner/flow/disable
26842:vpc:vpc-inner/flow/update	update	vpc-inner/flow/update
26842:vpc:vpc-inner/flow/resend	update	vpc-inner/flow/resend

3.1.10.2.5 Apsara Infrastructure Management Framework permission list

Resource	Action	Description
*:tianji:services:[sname]:tjmontemplates:[tmplname]	delete	DeleteServiceTjmonTpl
*:tianji:services:[sname]:tjmontemplates:[tmplname]	write	PutServiceTjmonTpl
*:tianji:services:[sname]:templates:[tmplname]	write	PutServiceConfTpl
*:tianji:services:[sname]:templates:[tmplname]	delete	DeleteServiceConfTpl
*:tianji:services:[sname]:serviceinstances:[sname]:tjmontemplate	read	GetServiceInstanceTjmonTpl
*:tianji:services:[sname]:serviceinstances:[sname]:tsessions	terminal	CreateTsSessionByService
*:tianji:services:[sname]:serviceinstances:[sname]:template	write	SetServiceInstanceTpl

Resource	Action	Description
*:tianji:services:[sname]:serviceinstances:[sname]:template	delete	DeleteServiceInstanceTpl
*:tianji:services:[sname]:serviceinstances:[sname]:template	read	GetServiceInstanceTpl
*:tianji:services:[sname]:serviceinstances:[sname]:tags:[tag]	delete	DeleteServiceInstanc eProductTagInService
*:tianji:services:[sname]:serviceinstances:[sname]:tags:[tag]	write	AddServiceInstancePr oductTagInService
*:tianji:services:[sname]:serviceinstances:[sname]:serverroles:[serverrole]:resources	read	GetServerroleResourc eInService
*:tianji:services:[sname]:serviceinstances:[sname]:serverroles:[serverrole]:machines:[machine]	write	OperateSRMachineInService
*:tianji:services:[sname]:serviceinstances:[sname]:serverroles:[serverrole]:machines:[machine]	read	GetMachineSRInfoInService
*:tianji:services:[sname]:serviceinstances:[sname]:serverroles:[serverrole]:machines:[machine]	delete	DeleteSRMachineActio nInService
*:tianji:services:[sname]:serviceinstances:[sname]:serverroles:[serverrole]:machines	read	GetMachinesSRInfoInService
*:tianji:services:[sname]:serviceinstances:[sname]:serverroles:[serverrole]:machines	delete	DeleteSRMachinesActi onInService
*:tianji:services:[sname]:serviceinstances:[sname]	write	OperateSRMachinesInService

Resource	Action	Description
].serverroles:[serverrole]: machines		
*:tianji:services:[sname]: serviceinstances:[sname]: serverroles:[serverrole]:apps:[app]:resources	read	GetAppResourceInService
*:tianji:services:[sname]: serviceinstances:[sname]: serverroles:[serverrole]:apps :[app]:machines:[machine]: tianjilogs	read	TianjiLogsInService
*:tianji:services:[sname]: serviceinstances:[sname]: serverroles	read	GetServiceInstanceSe rverrolesInService
*:tianji:services:[sname]: serviceinstances:[sname]: schema	write	SetServiceInstanceSchema
*:tianji:services:[sname]: serviceinstances:[sname]: schema	delete	DeleteServiceInstanceSchema
*:tianji:services:[sname]: serviceinstances:[sname]: rollings:[version]	write	OperateRollingJobInService
*:tianji:services:[sname]: serviceinstances:[sname]: rollings	read	ListRollingJobInService
*:tianji:services:[sname]: serviceinstances:[sname]: resources	read	GetInstanceResourceInService
*:tianji:services:[sname]: serviceinstances:[sname]: machines:[machine]	read	GetMachineAllSRInfoInService
*:tianji:services:[sname]: serviceinstances:[sname]	write	DeployServiceInstanc eInService
*:tianji:services:[sname]: serviceinstances:[sname]	read	GetServiceInstanceConf

Resource	Action	Description
*:tianji:services:[sname]: serverroles:[serverrole]: machines:[machine]:apps:[app] :files:name	read	GetMachineAppFileListInService
*:tianji:services:[sname]: serverroles:[serverrole]: machines:[machine]:apps:[app] :files:download	read	GetMachineAppFileDownloadInService
*:tianji:services:[sname]: serverroles:[serverrole]: machines:[machine]:apps:[app] :files:content	read	GetMachineAppFileContentInService
*:tianji:services:[sname]: serverroles:[serverrole]: machines:[machine]:apps:[app] :filelist	read	GetMachineFileListInService
*:tianji:services:[sname]: serverroles:[serverrole]: machines:[machine]:apps:[app] :dockerlogs	read	DockerLogsInService
*:tianji:services:[sname]: serverroles:[serverrole]: machines:[machine]:apps:[app] :debuglog	read	GetMachineDebugLogInService
*:tianji:services:[sname]: serverroles:[serverrole]: machines:[machine]:apps	read	GetMachineAppListInService
*:tianji:services:[sname]: serverroles:[serverrole]:apps:[app]:dockerinspect	read	DockerInspect
*:tianji:services:[sname]: schemas:[schemaname]	write	PutServiceSchema
*:tianji:services:[sname]: schemas:[schemaname]	delete	DeleteServiceSchema
*:tianji:services:[sname]: resources	read	GetResourceInService
*:tianji:services:[sname]	delete	DeleteService

Resource	Action	Description
*:tianji:services:[sname]	write	CreateService
*:tianji:projects:[pname]: machinebuckets:[bname]: machines:[machine]	read	GetMachineBucketMachineInfo
*:tianji:projects:[pname]: machinebuckets:[bname]: machines	read	GetMachineBucketMachines
*:tianji:projects:[pname]: machinebuckets:[bname]	write	CreateMachineBucket
*:tianji:projects:[pname]: machinebuckets:[bname]	write	OperateMachineBucketMachines
*:tianji:projects:[pname]: machinebuckets:[bname]	delete	DeleteMachineBucket
*:tianji:projects:[pname]: machinebuckets:[bname]	read	GetMachineBucketMachinesLegacy
*:tianji:projects:[pname]: machinebuckets	read	GetMachineBucketList
*:tianji:projects:[pname]: projects:[pname]:clusters:[cname]:tsessions:[tsessionn ame]:tses	terminal	UpdateTsSessionTssByCluster
*:tianji:projects:[pname]: projects:[pname]:clusters:[cname]:tsessions	terminal	CreateTsSessionByCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:tjmontemplate	read	GetServiceInstanceTjmonTplInCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:template	delete	DeleteServiceInstanceTplInCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:template	write	SetServiceInstanceTplInCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:template	read	GetServiceInstanceTplInCluster

Resource	Action	Description
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:tags:[tag]	write	AddServiceInstanceProductTagInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:tags:[tag]	delete	DeleteServiceInstanceProductTagInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:resources	read	GetServerroleResourceInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:name	read	GetMachineAppFileList
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:download	read	GetMachineAppFileDownload
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:files:content	read	GetMachineAppFileContent
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:filelist	read	GetMachineFileList
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:machines:[machine]:apps:[app]:dockerlogs	read	DockerLogsInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[read	GetMachineDebugLog

Resource	Action	Description
serverrole]:machines:[machine]:apps:[app]:debuglog		
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:serverroles:[serverrole]:machines:[machine]:apps	read	GetMachineAppList
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:serverroles:[serverrole]:machines:[machine]	read	GetMachineSRInfoInCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:serverroles:[serverrole]:machines:[machine]	write	OperateSRMachineInCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:serverroles:[serverrole]:machines:[machine]	delete	DeleteSRMachineActio nInCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:serverroles:[serverrole]:machines	write	OperateSRMachinesInCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:serverroles:[serverrole]:machines	delete	DeleteSRMachinesActi onInCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:serverroles:[serverrole]:machines	read	GetAllMachineSRInfoInCluster
*:tianji:projects:[pname]: clusters:[cname]:serviceins tances:[sname]:serverrole	read	GetAppResourceInCluster

Resource	Action	Description
s:[serverrole]:apps:[app]:resources		
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:machines:[machine]:tianjilogs	read	TianjiLogsInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles:[serverrole]:apps:[app]:dockerinspect	read	DockerInspectInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:serverroles	read	GetServiceInstanceServerrolesInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:schema	delete	DeleteServiceInstanceSchemaInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:schema	write	SetServiceInstanceSchemaInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]:resources	read	GetInstanceResourceInCluster
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]	delete	DeleteServiceInstance
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]	write	CreateServiceInstance
*:tianji:projects:[pname]:clusters:[cname]:serviceinstances:[siname]	read	GetServiceInstanceConfInCluster
*:tianji:projects:[pname]:clusters:[cname]:rollings:[version]	write	OperateRollingJob

Resource	Action	Description
*:tianji:projects:[pname]:clusters:[cname]:rollings	read	ListRollingJob
*:tianji:projects:[pname]:clusters:[cname]:resources	read	GetResourceInCluster
*:tianji:projects:[pname]:clusters:[cname]:quota	write	SetClusterQuotas
*:tianji:projects:[pname]:clusters:[cname]:machinesinfo	read	GetClusterMachineInfo
*:tianji:projects:[pname]:clusters:[cname]:machines:[machine]	read	GetMachineAllSRInfo
*:tianji:projects:[pname]:clusters:[cname]:machines:[machine]	write	SetMachineAction
*:tianji:projects:[pname]:clusters:[cname]:machines:[machine]	delete	DeleteMachineAction
*:tianji:projects:[pname]:clusters:[cname]:machines	write	OperateClusterMachines
*:tianji:projects:[pname]:clusters:[cname]:difflist	read	GetVersionDiffList
*:tianji:projects:[pname]:clusters:[cname]:diff	read	GetVersionDiff
*:tianji:projects:[pname]:clusters:[cname]:deploylogs:[version]	read	GetDeployLogInCluster
*:tianji:projects:[pname]:clusters:[cname]:deploylogs	read	GetDeployLogListInCluster
*:tianji:projects:[pname]:clusters:[cname]:builds:[version]	read	GetBuildJob
*:tianji:projects:[pname]:clusters:[cname]:builds	read	ListBuildJob
*:tianji:projects:[pname]:clusters:[cname]	write	OperateCluster

Resource	Action	Description
*:tianji:projects:[pname]:clusters:[cname]	delete	DeleteCluster
*:tianji:projects:[pname]:clusters:[cname]	read	GetClusterConf
*:tianji:projects:[pname]:clusters:[cname]	write	DeployCluster
*:tianji:projects:[pname]	write	CreateProject
*:tianji:projects:[pname]	delete	DeleteProject
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]:rackunits:[rackunit]	write	CreateRackunit
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]:rackunits:[rackunit]	write	SetRackunitAttr
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]:rackunits:[rackunit]	delete	DeleteRackunit
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]	write	SetRackAttr
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]	write	CreateRack
*:tianji:idcs:[idc]:rooms:[room]:racks:[rack]	delete	DeleteRack
*:tianji:idcs:[idc]:rooms:[room]	write	CreateRoom
*:tianji:idcs:[idc]:rooms:[room]	delete	DeleteRoom
*:tianji:idcs:[idc]:rooms:[room]	write	SetRoomAttr
*:tianji:idcs:[idc]	delete	Deleteldc
*:tianji:idcs:[idc]	write	SetIdcAttr
*:tianji:idcs:[idc]	write	CreateIdc

3.1.10.2.6 Webapp-rule permission list

Resource	Action	Description
26842:webapp-rule:*	write	Adds, deletes, and updates configuration resources
26842:webapp-rule:*	read	Queries configuration resources

3.1.10.2.7 Workflow (grandcanal) console permission list

Resource	Action	Description
26842:grandcanal	read	Queries the workflow activity details and abstract
26842:grandcanal	write	Restarts, retries, rolls back, and stops a workflow

3.1.10.2.8 baseService-yaochi-console permission list

Resource	Action	Description
26842:yaochi-console:*	write	Adds, deletes, updates, and queries configuration resources
26842:yaochi-console:*	read	Reads configuration resources

3.1.10.2.9 BCC permission list

Resource	Action	Description
26842:bcc:/api/product/odps/	*	Has all operation permissions to MaxCompute in the BCC backend
26842:bcc:/api/product/apsara/	*	Has all operation permissions to Apsara in the BCC backend
26842:bcc:/api/product/dataworks/	*	Has all operation permissions to DataWorks in the BCC backend
26842:bcc:/api/product/streamcompute/	*	Has all operation permissions to StreamCompute in the BCC backend
26842:bcc:/api/product/minirds/	*	Has all operation permissions to MINIRDS in the BCC backend
26842:bcc:/api/product/minilvs/	*	Has all operation permissions to MINILVS in the BCC backend
26842:bcc:/api/bccapi/sysadmin/	*	BCC backend interface
26842:bcc:/api/ias/	*	Intelligent diagnosis interface

Resource	Action	Description
26842:bcc:/api/tflow/	*	Process interface
26842:bcc:/api/bccapi/odps/	*	MaxCompute management interface
26842:bcc:/api/bccapi/base/	*	DataWorks management interface
26842:bcc:/api/bccapi/galaxy/	*	StreamCompute management interface

3.1.10.2.10 Tlog permission list

Resource	Action	Description
26842:tlogconsole:BizGroup	read	BizGroupRead
26842:tlogconsole:BizGroup	save	BizGroupSave
26842:tlogconsole:BizGroup	delete	BizGroupDelete
26842:tlogconsole:Collecting Point	get	CollectingPointGet
26842:tlogconsole:Collecting Point	save	CollectingPointSave
26842:tlogconsole:Collecting Point	delete	CollectingPointDelete

3.1.10.2.11 Butler permission list

Resource	Action	Description
26842:butler:Cmdb	query	queryCmdb
	update	updateCmdb
26842:butler:Collect	query	queryCollect
	update	updateCollect
26842:butler:Docker	query	queryDocker
	update	updateDocker
26842:butler:Env	query	queryEnv
	update	updateEnv
26842:butler:Img	query	queryImage
	update	updateImage

Resource	Action	Description
26842:butler:Metric	query	queryMetric
	update	updateMetric
26842:butler:Patrol	query	queryPatrol
	update	updatePatrol
26842:butler:Schedule	query	querySchedule
	update	updateSchedule
26842:butler:Olap	query	queryOlap
	update	updateOlap
26842:butler:Alarm	query	queryAlarm
	update	updateAlarm

3.1.10.2.12 Data Replication System permission list

Resource	Action	Description
26842:drds:jingwei:/createGuide.htm	READ	Create a Service page
26842:drds:jingwei:/serviceList.htm	READ	Service List page
26842:drds:jingwei:/db2DbServiceDirect.htm	READ	Service Details page
26842:drds:jingwei:/taskDetail.htm	READ	Task Details page
26842:drds:jingwei:/statTrend.htm	READ	Statistical Trend page
26842:drds:jingwei:/fullCopyService.htm	READ	Full Migration page
26842:drds:jingwei:/taskWorker.htm	READ	Task Server page
26842:drds:jingwei:/taskWorker.htm	READ	Task Server page
26842:drds:jingwei:/taskJstack.htm	READ	Jstack page

Resource	Action	Description
26842:drds:jingwei:/taskWorkerLog.htm	READ	Task Server - View Logs
26842:drds:jingwei:/db2Db.htm	READ	DB Synchronization Mode page
26842:drds:jingwei:/tableSpread.htm	READ	Small Table Broadcast page
26842:drds:jingwei:/workerList.htm	READ	Server List page
26842:drds:jingwei:/monitorBoard.htm	READ	Monitoring Dashboard - Latency Dashboard
26842:drds:jingwei:/exceptionBoard.htm	READ	Monitoring Dashboard - Exception Dashboard
26842:drds:jingwei:/taskBoard.htm	READ	Monitoring Dashboard - Task Dashboard page
26842:drds:jingwei:/envManage.htm	READ	System Management - Environment Management page
26842:drds:jingwei:/clusterManage.htm	READ	System Management - Cluster Management page
26842:drds:jingwei:/userManager.htm	READ	System Management - User Management page
26842:drds:jingwei:/trashList.htm	READ	System Management - Recycle Bin page
26842:drds:jingwei:/eventLogList.htm	READ	System Management - Operation Logs page
26842:drds:jingwei:/zkNodeManage.htm	READ	System Management - zk Node Management page
26842:drds:jingwei:/metaqMsg.htm	READ	System Management - metaq Message Query page
26842:drds:jingwei:/akskListBu.c.htm	READ	System Management - API Authorization page
26842:drds:jingwei:/worker.htm	READ	Server Information page
26842:drds:jingwei:/resourceConfig.htm	READ	Modify Resource Scheduling Mode page

Resource	Action	Description
26842:drds:jingwei:/cleanStoppedTaskConfig.htm	READ	Modify a Stopped Scheduling Task page

3.1.10.2.13 Tianjimon permission list

Resource	Action	Description
26842:tianjimon:monitor-manage	manage	Monitoring O&M

3.1.10.2.14 Rtools permission list

Resource	Action	Description
26842:drds:rtools:tddl	all	Publishes TDDL configurations in the Rtools console
26842:drds:rtools:jade	all	Queries and modifies configurations in the Rtools console
26842:drds:rtools:geminis	all	The gemini-related permissions in the Rtools console
26842:drds:rtools:system	all	Other permissions in the Rtools console

3.1.10.2.15 MetaCenter permission list

Resource	Action	Description
26842:drds:mc:app	all	Application-related permissions in the MetaCenter console
26842:drds:mc:rule	all	Rule-related permissions in the MetaCenter console
26842:drds:mc:topology	all	Topology-related permissions in the MetaCenter console
26842:drds:mc:permission	all	Interface call permissions in the MetaCenter console
26842:drds:mc:system	all	Other permissions in the MetaCenter console

3.1.10.2.16 Dayu permission list

Resource	Action	Description
26842:drds:dayu:system	all	Dayu console permissions

3.2 Common O&M operations

3.2.1 Log on to OPS

This section describes how to log on to the OPS server from Apsara Infrastructure Management Framework.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Operations > Cluster Operations**.
3. On the **Cluster Operations** page, enter **tianji** in the **Cluster** search box to perform a fuzzy search.
4. At the right of the cluster, select **Monitoring > Cluster Operation and Maintenance Center**.
5. On the **Cluster Operation and Maintenance Center** page, select **ops** from the **Service** drop-down list.

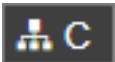

The server information of OPS is displayed.

6. At the right of an OPS server, click **Terminal**.

3.2.2 Log on to ECSAG

This section describes how to log on to the ECSAG server from Apsara Infrastructure Management Framework.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Click the  tab in the upper-left corner. Enter **ecs** in the search box to perform a fuzzy search.
All ECS clusters are displayed.
3. Place your cursor on  at the right of the ECS-IO8-xxx cluster and then select **Cluster Operation and Maintenance Center**.

4. On the **Cluster Operation and Maintenance Center**, select **ecs-init** from the **Service** drop-down list and select **EcsAg#** from the **Service Role** drop-down list.
5. At the right of an ECSAG server, click **Terminal**.

3.2.3 Log on to XGW

This section describes how to log on to the XGW server from Apsara Infrastructure Management Framework.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Operations > Cluster Operations**.
3. On the **Cluster Operations** page, enter vpc in the **Cluster** search box to perform a fuzzy search.
4. At the right of the cluster, select **Monitoring > Cluster Operation and Maintenance Center**.
5. On the **Cluster Operation and Maintenance Center** page, click **Terminal** at the right of an XGW server.

3.2.4 View Docker container status

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Operations > Cluster Operations**.
3. On the **Cluster Operations** page, select **Monitoring > Cluster Operation and Maintenance Center** at the right of the ads-xxxxxxx-xxx cluster.

Abnormal Service indicates abnormal services and the number of these services.
4. On the **Cluster Operation and Maintenance Center** page, click **Details** of an abnormal server under **Final Status** to view the container status.
5. In the displayed server details dialog box, click **Monitoring** at the right of a service to view the monitoring items of the server role.

3.2.5 View service status

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Reports > System Reports**.

3. On the **System Reports** page, perform a fuzzy search for the service inspection report.
4. Open the **Service Inspector Report** to view the service status.

3.2.6 View cluster status

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Operations > Cluster Operations**.
3. On the **Cluster Operations** page, view the cluster status.

3.2.7 View the status of project component

This section describes how to view Docker, service, and project alarms.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Reports > System Reports**.
3. On the **System Reports** page, perform a fuzzy search for current status of project component.
4. Open the **State of Project Component**.

3.2.8 View Docker host status

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Reports > System Reports**.
3. On the **System Reports** page, perform a fuzzy search for machine view.
4. Open the **Machine Info Report** to view the machine status.

3.2.9 View Docker host and container distribution

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Reports > System Reports**.
3. On the **System Reports** page, perform a fuzzy search for virtual machine mapping.
4. Open the **Virtual Machines Map**.
5. On the **Virtual Machines Map** page, view the mapping between virtual machines and virtual machines actually deployed.

Select a virtual machine from the **machine** drop-down list and click **Filter** to view the specific hostname.

3.2.10 View monitoring status (formerly Alimonitor)

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Reports > System Reports**.
3. On the **System Reports** page, perform a fuzzy search for machine view.
4. Open the **Machine Info Report**. On the **Machine Info Report** page, view the monitoring status of machines.

3.2.11 View resource status (formerly CMDB)

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Reports > System Reports**.
3. On the **System Reports** page, perform a fuzzy search for resource application report.
4. Open the **Resource Apply Report**.
5. On the **Resource Apply Report** page, view the resource information.

3.2.12 View the number of physical machines for each project

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Reports > System Reports**.
3. On the **System Reports** page, perform a fuzzy search for machine view.
4. Open the **Machine Info Report**.
5. On the **Machine Info Report** page, select a project to view the number of machines.

3.2.13 View server SN based on IP address

This section describes how to view the server SN based on the IP address.

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Operations > Server Operations**.

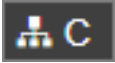

3. On the **Server Operations** page, enter an IP address in the search box. For example, 10.XX.XX.XX.

The hostname, cluster, and project of the server using this IP address are displayed.

4. Select **Operations > Cluster Operations**.
5. On the **Cluster Operations** page, select the project name obtained in 3 from the **Project** drop-down list. At the right of the cluster, select **Monitoring > Cluster Operation and Maintenance Center**.
6. On the **Cluster Operation and Maintenance Center** page, enter the hostname obtained in 3 in the **Server Search** field under **Server List**.
7. Click **Confirm**.
8. Click the server hostname to view the detailed server information, including the SN.

3.2.14 Check whether a physical machine of a V3 Apsara Infrastructure Management Framework cluster is a control server or OPS 1-4

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Click the  tab in the upper-left corner. Enter tianji in the search box to perform a fuzzy search.
3. Place your cursor on  at the right of the cluster and then select **Cluster Configuration File**.
4. Find the host in the *machine_group.conf* file and check whether the host is a control server or OPS 1-4.

3.2.15 View deployment conditions

Procedure

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Tasks > Deployment Summary**.
3. On the **Deployment Summary** page, click **Deployment Details**.
4. View the deployment status and detailed information of each service.