# Alibaba Cloud
# Apsara Stack Enterprise

## Maintenance Guide

Version: 1807

Issue: 20180731

MORE THAN JUST CLOUD | Alibaba Cloud

# Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 instructio ns, 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 `cd /d C:/windows` command to enter the Windows system folder. |
| *`Italics`* | It is used for parameters and variables. | `bae log list --instanceid` *`Instance_ID`* |
| [] or [a\|b] | It indicates that it is a optional value, and only one item can be selected. | `ipconfig` *`[-all\|-t]`* |
| {} or {a\|b} | It indicates that it is a required value, and only one item can be selected. | `switch` *`{stand \| slave}`* |

# 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 Platform maintenance.....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 Configurations.....23
2.1.9.1 Overview.....23
2.1.9.2 Modify a configuration item of a product.....24

2.1.9.3 Restore the modified configuration item....24
2.1.10 System management....25
2.1.10.1 Overview....25
2.1.10.2 Department management....25
2.1.10.3 Role management....26
2.1.10.4 Logon policy management....27
2.1.10.5 User management....28
2.1.10.6 Two-factor authentication....29
2.1.10.7 Application whitelist....32
2.1.10.8 Operation logs....33
2.1.10.9 Server password management....34
2.1.10.10 Offline backup....35
2.2 Tianji maintenance....38
2.2.1 Overview....38
2.2.1.1 What is Apsara Infrastructure Management Framework?....38
2.2.1.2 Basic concepts....39
2.2.2 Homepage overview....41
2.2.3 System management....43
2.2.3.1 Permission management....43
2.2.3.2 Data source management....43
2.2.4 Project management....43
2.2.5 Cluster management....43
2.2.5.1 Cluster dashboard....43
2.2.5.2 Cluster Operation and Maintenance Center....47
2.2.5.3 Service final status....49
2.2.5.4 Cluster configuration....50
2.2.5.5 Operation logs....50
2.2.6 Modify a monitor template....50
2.2.7 Ticket management....51
2.2.7.1 Manage permissions of a ticket....51
2.2.7.2 Create a ticket....52
2.2.7.2.1 Manually open a ticket....52
2.2.7.2.1.1 Process description....52
2.2.7.2.1.2 Procedure....52
2.2.7.2.2 Apsara Infrastructure Management Framework opens a ticket after self-check....54
2.2.8 Machine management....54
2.2.8.1 Add a machine....54
2.2.8.2 Modify machine buckets....55
2.2.8.3 Delete a machine....55
2.2.9 Task management....56
2.2.9.1 Task query....56
2.2.9.2 Deployment overview....56
2.2.9.2.1 Deployment progress....56

2.2.9.2.2 Deployment details....57
2.2.10 Alarm center....59
2.2.11 Report management....60
2.2.11.1 Product component information....60
2.2.11.2 Product component current status....60
2.2.11.3 Machine view....62
2.2.11.4 Machine role action report....63
2.2.11.5 Machine clone report....64
2.2.11.6 Service inspection report....65
2.2.11.7 Resource application report....65
2.2.11.8 Rolling job query....66
2.2.11.9 VM mapping....67
2.2.11.10 Service dependency....68
2.2.11.11 Service registration variables....68
2.2.11.12 Network topology check....68
2.2.11.13 Machine RMA pending approval list....69
2.2.11.14 Automatic recovery – Installation pending approval list....70
2.2.11.15 Cluster on/off monitoring report....70
2.2.11.16 Apsara Stack service alert status dashboard....71
2.2.11.17 Thermometer....71
2.2.11.18 Project-based O&M....72
2.2.11.19 AGG node O&M....72
2.2.11.20 Source node O&M....73
2.2.11.21 Container monitoring - cluster....74
2.2.11.22 Container monitoring - single machine....74
2.2.11.23 JVM monitoring - cluster....74
2.2.11.24 JVM monitoring - single machine....75
2.2.11.25 Reference error check of service exposure variables....75
**3 Appendix....76**
3.1 Maintenance role authorization....76
3.1.1 OAM introduction....76
3.1.2 Basic concepts....76
3.1.3 Log on to OAM....77
3.1.4 Quick start....78
3.1.4.1 Create a group....78
3.1.4.2 Add group members....78
3.1.4.3 Add a group role....79
3.1.4.4 Create a role....79
3.1.4.5 Add an inherited role to a role....80
3.1.4.6 Add resources to a role....80
3.1.4.7 Add authorized users to a role....81
3.1.5 Manage a group....83
3.1.5.1 Modify group information....83
3.1.5.2 View group role details....83

3.1.5.3 Delete a group....84
3.1.5.4 View assigned groups....84
3.1.6 Manage roles....84
3.1.6.1 Query roles....84
3.1.6.2 Modify role information....85
3.1.6.3 View the role inheritance tree....85
3.1.6.4 Transfer a role....85
3.1.6.5 Delete a role....86
3.1.6.6 View assigned roles....86
3.1.6.7 View all roles....86
3.1.7 Search resources....87
3.1.8 View personal information....87
3.1.9 Typical applications....87
3.1.9.1 Assign a default role to a user....87
3.1.9.2 Use groups and RoleHierarchy....88
3.1.9.3 Use custom roles....89

# 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 Platform maintenance

## 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:

| Function | Description |
| --- | --- |
| *O&M dashboard* | The O&M dashboard displays the product version, inventory statistics, inventory usage trend, O&M process task statistics, 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 informatio n, 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. |
| *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. |

| Function | Description |
| --- | --- |
| *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 redirecting to the O&M interface 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.

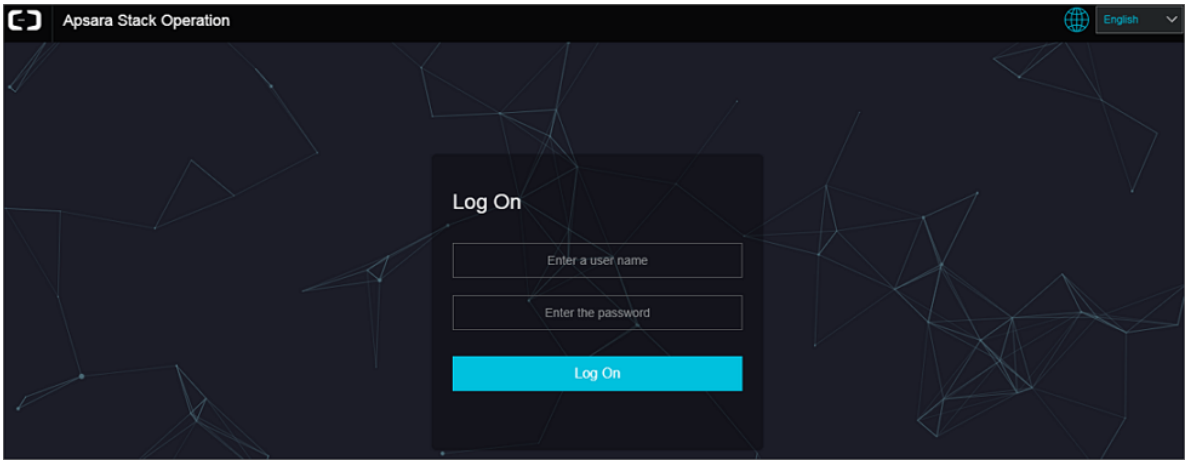
**Prerequisites**

- 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 Configurations

# 2.1.9.1 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.

## 2.1.9.2 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.

## 2.1.9.3 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.

# 2.1.10 System management

## 2.1.10.1 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.

## 2.1.10.2 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**.

## 2.1.10.3 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**.

## 2.1.10.4 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.

# 2.1.10.5 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 polices 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.

## 2.1.10.6 Two-factor authentication

To improve the security for user logon, 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 logon 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 logon, 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 logon 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 logon 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 the authentication server provided by the third-party manufacturer to verify the encrypted information or certificate provided upon logon. 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 authentica tion 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.

## 2.1.10.7 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**.

## 2.1.10.8 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**.

# 2.1.10.9 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**.

## 2.1.10.10 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 nvwa 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 2-2: Description of backup service**

| Function menu | Description |
| --- | --- |
| Backup Configuration | 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.<br>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**.<br>In the upper-right corner of the page, click **Modify** to modify configurations. |
| Backup Details | Displays the current backup status. The backup details include **Product**, **Backup 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. |

| Function menu | Description |
| --- | --- |
| 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 2-3: Description of service configuration**

| Function menu | Description |
| --- | --- |
| Backup Service Configuration | Provides backup server configurations.<br>• 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.<br>• 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.<br>• Backup retention: The file storage time on the backup server. The backup file that exceeds the time will be deleted.<br>Click **Modify** under **Actions** to modify configurations. |

| Function menu | Description |
| --- | --- |
| Product Management | Provides basic management of backup products, including:<br>1. 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**.<br>2. 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.<br>You can configure the search conditions and then click **Search** to obtain backup details. |

- **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 Tianji maintenance

# 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 life cycles and various static resources, including programs, configurat ions, 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 Infrastruc

ture Management Framework-based services in a large-scale distributed environment, greatly improving the operation and maintenance efficiency and system availability.

**Core features**

- IDC network initialization
- Server installation and maintenance process management
- Cloud product deployment, resizing, and upgrade
- Cloud product configuration management
- Automatic resource application for cloud products
- Automatic repairing of software and hardware faults
- Basic monitoring and service monitoring of software and hardware

## 2.2.1.2 Basic concepts

**Project**

A project corresponds to a product as a set of clusters in Apsara Infrastructure Management Framework.

A group of clusters can provide service capabilities for external entities.

**Cluster**

It is logically a set of physical machines that provide services and software used to deploy products.

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

**Service**

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

The service name is globally unique. It is recommended that a service name uses a combination of lower-case letters with the business unit (BU) name as a prefix, for example, aliyunoss.

A 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 related service capabilities. For example, Pangu, Fuxi, and Nuwa 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 onto a server indicates that the server provides the corresponding function. Multiple server roles, for example, PanguMaster and TianjiClient, can be deployed on the same server.

It is recommended that a server role be named using **`Upper Camel Case`** and suffixed by #, for example, PanguMaster#. To support the multi-tenant, the full name of a server role contains the service name prefix as the naming space, for example, pangu.PanguMaster.

**Server role instance**

It is 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, which 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 editions in a cluster. Different instances of the same server role are indicated by the pound key (#) and a suffix, for example, PanguLib#56 and PanguLib#57.

**Application**

An application corresponds to a process-level service component contained by 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 on every server.

An application is named using *`Lower case with _`*. 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 configuration, upgrades services, and modifies the cluster configurations based on the configuration contents. This process is called rolling.

**Service configuration template**

When service are deployed in clusters, some configurations are the same. 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.

**Association service template**

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

**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**

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

  O&M covers the following four aspects:

  - Project O&M: Manages projects using the project permission.
  - Cluster O&M: Performs O&M management on clusters using the project permission. For example, you can check the cluster status.
  - Service O&M: Manages services using the service permission. For example, you can perform tianjiMon template management.
  - Machine O&M: Maintains and manages all machines in Apsara Infrastructure Management Framework. For example, you can directly log on to the terminal service of a machine, add a machine to Apsara Infrastructure Management Framework, and migrate buckets.

- Task: After you modify configurations, tasks such as rolling will be generated. With the Task menu, you can access the current task page or history task page.
- Report: Allows you to access the portal report platform. Data can be displayed in tables, graphics, or texts.
- Management: Includes portal permission management, data source management, and custom portal management.
- Alert: Includes status monitoring and alert policies.

**Navigation bar**

On the navigation bar, you can directly view the logical structure of Apsara Infrastructure Management Framework model.

- 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 of each service.
- Report: Supports fuzzy query of reports and allows you to view the report details.

By selecting nodes at different levels on 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**

If you do not need to use the navigation bar when performing some O&M operations, click this button to fold the navigation bar and increase the space of the content area.

**Portal special function button**

- Synchronization time: Indicates the generation time of the data that is currently displayed on the portal.
- Final state time: Indicates the statistical 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. Apsara Infrastructure Management Framework as an asynchronous system is subject to delay. This delay helps explain the data results displayed on the portal and determine whether the current system has any fault.

## 2.2.3 System management

## 2.2.3.1 Permission management

Select **Management** > **Permission Management** to go to the O&M management platform (OAM). For more information about specific operations, see *Cite LeftOAM User GuideCite Right*.

## 2.2.3.2 Data source management

The data source Apsara Infrastructure Management Framework DB exists by default. All users have the read-only permission, which can be modified. Users do not need to apply for any permission for the data source. In addition, the data source serves the purpose of a report platform. Currently, the report platform is used as an auxiliary method for troubleshooting on Apsara Infrastructure Management Framework, so 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. Click **`Delete`** under**Actions** to delete the corresponding project.
5. Click **`Details`**under **Actions** to view all clusters of the project and switch to the **Cluster Operations** page.

## 2.2.5 Cluster management

## 2.2.5.1 Cluster dashboard

On Apsara Infrastructure Management Framework, select the **Cluster** tab and click **Dashboard** next to the cluster. The **Cluster Dashboard** page is displayed.

The cluster dashboard provides the basic cluster information, final status information, rolling job information, dependencies, resource information, VMs, and monitoring information. *Table 2-4: Parameters on the cluster dashboard page* describes the parameters on the page.

**Table 2-4: Parameters on the cluster dashboard page**

| Module | Parameter description |
| --- | --- |
| Basic Cluster Information | • Product name.<br>• Cluster name.<br>• Final-status version: Latest version of the cluster. |

| Module | Parameter description |
| --- | --- |
| | • Cluster reaching final status: Specifies whether the cluster reaches the final status.<br>• Machine not reaching final status: Number of machines not reaching the final status in the cluster.<br>• Real clone or not: Specifies whether system clone is performed when a machine is added to the cluster.<br>• Expected machine count: Number of machines that are expected in the cluster.<br>• Actual machine count: Number of machines that are currently in the cluster.<br>• Non-good machine count: Number of machines in non-good status in the cluster.<br>• Actual service count: Number of services actually deployed in the cluster.<br>• Actual server role count: Number of server roles deployed in the cluster.<br>• Cluster running status: Specifies whether the cluster is started or shut down. |
| Machine Status Statistics | Measures the status of machines in the cluster. |
| Service Machine Final-status Data Statistics | Specifies the final status of service machines in the cluster. |
| Load-System | Cluster system load chart. |
| CPU-System | CPU load chart. |
| Mem-Sytem | Memory load chart. |
| Disk_usage-System | Hard disk usage load chart. |
| Traffic-System | System traffic chart. |
| TCP state-system | TCP request status chart. |
| TCP retrains-System | TCP retransmission volume information. |
| Disk_IO-System | Hard disk read/write information. |
| Service Instances | Displays the service instances currently deployed in the cluster and the related final status information.<br>• Service instance: Service deployed in the cluster. |

| Module | Parameter description |
| --- | --- |
| | • Reaching final status or not: Specifies whether the service reaches the final status.<br>• Expected server role count: Number of server roles that are expected in a service instance.<br>• Final-status server role count: Number of server roles that have reached the final status in a service instance.<br>• Deprecating server role count: Number of server roles that are being deprecated in a service instance.<br>• Choose **Action** > **Details** to go to the service instance dashboard page. |
| Upgrade Task | Displays the change tasks related to the cluster.<br>• Cluster: Cluster name.<br>• Type: Type of the upgrade task. The options include app (version upgrade) and config ( configuration change).<br>• Git version: Changed version to which the upgrade task belongs.<br>• Description: Change description.<br>• Upgrade result: Result of the upgrade task.<br>• Submitted by: Person who submits the change.<br>• Submission time: Time for submitting the change.<br>• Start time: Time for starting the rolling.<br>• End time: Time for stopping the upgrade.<br>• Elapsed time: Time used for the upgrade.<br>• Operation: Click **Details** to go to the upgrade task details page. |
| Cluster Resource Application Status | • version: Changed version.<br>• msg: Exception information.<br>• begintime: Start time of change analysis.<br>• endtime: End time of change analysis.<br>• buildstatus: Change analysis result. |

| Module | Parameter description |
| --- | --- |
| | • resourceprocessstatus: Application status of the resource in the version. |
| Cluster Resource | • service<br>• serverrole: Name of the server role.<br>• app: App of the server role.<br>• name: Resource name.<br>• type: Resource type.<br>• status: Resource application status.<br>• error_message: Exception information.<br>• parameters: Resource parameter.<br>• result: Resource application result.<br>• res: Resource ID.<br>• reprocess_status: Status of interaction with Yaochi during VIP resource application.<br>• reprocesss_msg: Error messages of interaction with Yaochi during VIP resource application.<br>• reprocess_result: Result of interaction with Yaochi during VIP resource application.<br>• refer_process_list: Version that uses the resource. |
| VM Mapping | Displays the information about VMs in the cluster. Data is available only when VMs are deployed in the cluster.<br>• VM: Host name of the VM.<br>• Currently deployed VM: Host name of the physical machine of the currently deployed VM.<br>• Expected deployed VM: Host name of the physical machine of the expected VM. |
| Dependency | Displays the dependencies of the service instances and server roles in the cluster, as well as the final status information about the dependent service or role.<br>• Service: Service name.<br>• Server role: Server role name.<br>• Dependent service: Service on which the server role depends. |

| Module | Parameter description |
| --- | --- |
| | • Dependent server role: Server role on which the server role depends.<br>• Not reaching final status: Number of the clusters in which the dependent server role does not reach the final status.<br>• 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**:

- On the **Cluster** tab, click **Cluster Operation and Maintenance Center** corresponding to the cluster.
- Select **Operations** > **Cluster Operations**, and then select **Monitoring** > **Cluster Operation and Maintenance Center** corresponding to the cluster.
- On the **Cluster Dashboard** page, select **Operations Menu** > **Cluster Operation and Maintenance Center**.

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

*Table 2-5: Parameters on the Cluster O&M Center page* describes parameters on the Cluster O&M Center page.

**Table 2-5: Parameters on the Cluster O&M Center page**

| Parameter | Description |
| --- | --- |
| Total Machines | Indicates the total number of machines in the cluster. |
| Scale Up/Down | Indicates that the machine or server role is going online or offline. |
| Exception Machines | Indicates the number of abnormal machines that encounter each type of the following fault:<br>• Ping failure: A ping_monitor error is reported, and the Apsara Infrastructure Management Framework master cannot successfully ping the machine.<br>• No heartbeat: The tj-client on the machine does not periodically report data to indicate the status of this machine. This problem may be caused by a tj-client or network fault. |

| Parameter | Description |
| --- | --- |
| | • Status error: The monitor reports an error or a fault of the critical or fatal level for the machine. You need to check the alert information and accordingly handle the fault. |
| Exception Service | Apsara Infrastructure Management Framework determines whether a service reaches the final state according to the following criteria:<br>• The server role on the machine is in GOOD state.<br>• The actual version of each application of the server role on the machine must be consistent with the HEAD version.<br>• 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 state is unknown. This process is called by Portal as the change preparation process. The service final state cannot be determined during the preparation process or upon a preparation failure. |
| Server Roles Not in Final State | Displays all server roles that do not reach the final state in the cluster. You can click the number to expand a list, and click a record in the list to filter machines. |
| Running Tasks | Displays the number of rolling tasks if any. |
| HEAD Version Submission Time | Displays the time that the HEAD version is submitted. You can click the time to view the submission details. |
| Modify Preparation Status | Indicates the build status of the HEAD version. |
| Services | You can select a service deployed in the cluster from the drop-down list . |
| Server Role | You can select a server role of a service in the cluster from the drop-down list.<br>**Note:**<br>After you select a service and server role, the list below displays the states of server roles on the machines. |
| Machines | You can view all machines in the cluster, or filter out the machine where the corresponding server role is located by specifying the service and server role.<br>• Machine: If you click Machine, a query dialog box is displayed, where you can filter machines in batches.<br>• Click the host name of a machine. The machine information page is displayed, where you can view the physical information of the |

| Parameter | Description |
| --- | --- |
| | machine. You can also click **DashBoard** to view the machine details.<br>• If you click **Details** in the **Machine Final Status**column, you can view the state and exception information of services on the machine.<br>— Normal<br>— Machine Scale-Down: The machine is being removed from the cluster for scale-down purpose.<br>— Machine Scale-Up: The machine is being added to the cluster for scale-up purpose.<br>— SR Scale-Down: A server role is being deleted from the machine for scale-down purpose.<br>• If you click **Details** in the **Machine Running State**column, you can view the machine running state and exception information.<br>• If you click **Error**, **Warning**, or **Normal** in the **Monitoring Info.** column, you can view the machine monitoring items and server role monitoring items.<br>• If you click **Terminal** in the **Action** column, you can log on to the machine and perform related operations. |

## 2.2.5.3 Service final status

**Procedure**

1. Select **Operations** > **Cluster Operations**.
2. Select **Monitoring** > **Service Final Status Query** in the operation column of the target cluster.

   The **Service Final Status Query** page is displayed.

   *Table 2-6: Parameters on the Final Status Comparison page* describes parameters on the page.

   **Table 2-6: Parameters on the Final Status Comparison page**

| 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 | Indicates that the current rolling task of the cluster may not be of the HEAD version. If there is any task, the task information is displayed. |

| Parameter | Description |
| --- | --- |
| Cluster Machine Status Statistic | Indicates the status of all machines in the cluster. You can click **View Details** to view the detailed information about all machines. |
| Cluster Service Version Final Status | Indicates whether the server role version is consistent on machines and whether the status is GOOD. |
| Server Role Version Final Status Info. | Displays the number of machines 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** under **Actions**.

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

## 2.2.5.5 Operation logs

**Procedure**

1. Select **Operations** > **Cluster Operations**.
2. Select **Monitoring** > **Operation Logs** in the operation column of the target cluster. 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
     - Expand 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 difference content is displayed in the difference file list.

## 2.2.6 Modify a monitor template

**Procedure**

1. Log on to Apsara Infrastructure Management Framework.
2. Select **Operations** > **Service Operations**.
3. Click **Management** of the service for which the monitor template should be modified, for example, tianji.
4. Select the **Monitoring Instance** tab, and view the service instances for which alerts are generated.

   You can view the deployment state and deployment log.
5. To modify a monitor template, view the monitor template used by the service instance on the **Monitoring Instance** page, and select the **Monitoring Template** tab.
6. You are advised to modify the monitor template of the *sub* type, and click **Edit**.
7. On the **Alarm Items** tab, select the alert item to be modified, and click **Edit**. The **Template Settings** page is displayed.
8. Set the monitor parameters according to the actual conditions.
9. Click **Preview Changes** to view the changes.
10. Click **OK** to save the changes.

    Wait for about 10 minutes. The monitor instance will be automatically deployed, the check state will change to **`Successful`**, and the deployment time will be 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 permissions of a ticket

The administrator can authorize each role to process the tickets. This section describes how to manage the ticket permissions.

**Context**

Users can have the following roles:

- PE: User who manually opens and checks a ticket.
- IDC SA: User who diagnoses faults based on a manually opened ticket and fills in the fault details.
- IDC onsite engineer: User who repairs the machines.
- IDC admin: Administrator of the IDC, 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 permission management 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. Click **Modify Permission** next to the current logon account. The **Add User** page is displayed.
4. Select a role as required.
   - To open a ticket, select PE.
   - To process a ticket, select IDC SA.
   - To repair a machine, select IDC onsite engineer.

# 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 is as follows:

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

   When opening a ticket, switch the role of the logon account to PE or log on to the system as PE .
2. The IDC SA checks the event ticket opened by the demand side, verifies the fault, and fills in the fault details.

   When checking the event ticket, switch the role of the logon account to IDC SA or log on to the system as IDC SA.
3. The IDC onsite engineer troubleshoots the fault and completes the repair process.

   When troubleshooting, switch the role of the logon account to IDC onsite engineer or log on to the system as an IDC onsite engineer.

# 2.2.7.2.1.2 Procedure

**Procedure**

1. Log on to Apsara Infrastructure Management Framework.

2. Switch the role to PE and choose **Management** > **Ticket Management**. The **Ticket Management** page is displayed.
3. Click **Create Ticket**. The event ticket settings page is displayed.
4. Set the fault information.
5. Click **Confirm**.
6. Switch the role to IDC SA and choose **Management** > **Ticket Management**. The **Ticket Management** page is displayed.
7. On the **Pending Tickets** tab, select tickets and click **Claim Multiple Tickets**.
8. On the **Received Tickets** tab, check whether the details of each event ticket are reasonable.
   - If not reasonable, select the event ticket and click **Cancel**. The event ticket ends.
   - If reasonable, select the event ticket and click **OK** to go to the next step.

     The **Create Ticket** page 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 PE and choose **Reports** > **All Reports**.
12. Search **`Machine RMA pending approval list`** in fuzzy mode and click **Machine RMA pending approval list**. The **Machine RMA Pending Approval 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 IDC onsite engineer and choose **Management** > **Ticket Management**. The **Ticket Management** page is displayed.
17. Select the pending ticket and click **Received Tickets**.
18. The IDC onsite engineer performs troubleshooting based on the ticket.
19. After the repair, click the **Received Tickets** tab on the **Ticket Management**page and 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 PE and choose **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 IDC onsite engineer repairs the faulty machine. After the repair, the engineer 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 Machine management

## 2.2.8.1 Add a machine

**Procedure**

1. On the Apsara Infrastructure Management Framework page, 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. Follow the prompts on the page to set the target project and bucket and upload the configuration file.

   The configuration file contains the list of the machines to be uploaded. Click **Download Schema** to obtain the machine list table in `.xlsx` format. You can use this table to supplement the machine list.

   **Note:**

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

Generally, the machine list is not resized using the portal. If the portal is used, Apsara Infrastructure Management Framework provides the list of all required attributes for the onsite engineers.

5. Click **Confirm Online**.

## 2.2.8.2 Modify machine buckets

**Procedure**

1. On the Apsara Infrastructure Management Framework page, select **Operations** > **Server Operations**.
2. Click **Server Bucket Change**.
3. In the displayed dialog box, select the target project and bucket.
4. Enter the machine names on the left side of the page on each line.

   If the current user is the owner or user of the project where the machine to be modified resides, go to Step *5*.

   If the current user is not the owner or user of the project, move the cursor over **`Modify`**, click **View Authorizer**, and contact the authorizer to grant the relevant permission of the target project to the current user.
5. Click **Confirm**.

## 2.2.8.3 Delete a machine

**Procedure**

1. On the Apsara Infrastructure Management Framework page, select **Operations** > **Server Operations**. The **Server Operations** page is displayed.
2. Click **Server Online/Offline**.
3. Click the **Remove Server** tab.
4. Enter the list of the host names of the machines to be deprecated and verify that the information is correct.
5. Click **Clear Servers**.

# 2.2.9 Task management

## 2.2.9.1 Task query

Tasks include running tasks and previous tasks. This section describes how to query details of tasks.

**Procedure**

1. On the Apsara Infrastructure Management Framework platform, 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 state: State of the running task. You can click **View Tasks** to view the running details.
   - Rolling time: 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 query tasks by cluster name, type, upgrade result, Git version, start time, and end time.

## 2.2.9.2 Deployment overview

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

### 2.2.9.2.1 Deployment progress

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

- View the deployment state of each project and time required to reach the state.
  - Grey: To be deployed. It indicates that some services of the project depend on SRs or service instances that are being deployed, and other service instances or roles under the project have already been deployed.
  - Blue: Deploying. It indicates that the project has not reached the final state for one time yet.
  - Green: Reaching the final state. It indicates that all clusters under the project have reached the final state.
  - Orange: Not reaching the final state. After the project reaches the final state for the first time , a certain SR has not reached the final state due to some reason.

- Setting of clone_mode (global installation switch):
  - normal: Clone is allowed.
  - block: Clone is prohibited.
- Setting of dependency_check_level (global dependency switch):
  - normal: The dependency of all configurations is checked.
  - ignore: The dependency is not checked.
  - ignore_service: The service-level dependency (including the dependency of SRs of the service) is not checked, and only the SR-level dependency is checked.

## 2.2.9.2.2 Deployment details

Select **Tasks** > **Deployment Summary**.

On the **Deployment Summary** page, click **Deployment Details**. The **Deployment Details** page is displayed.

*Table 2-7: Parameters on the Deployment Details page* describes parameters on the Deployment Details page.

**Table 2-7: Parameters on the Deployment Details page**

| Parameter | Description |
| --- | --- |
| Status Statistics | General deployment statistics: It indicates the number of projects that are currently available. Click each status, and the projects in this status are displayed. There are five deployment statuses:<br>• Reaching the final status: It indicates that all clusters under the project have reached the final status.<br>The icon is a green tick.<br>• Deploying: It indicates that the project has not reached the final status for one time yet.<br>The icon is a blue in-progress symbol.<br>• To be deployed: It indicates that some services of the project depend on SRs or service instances that are being deployed, and other service instances or roles under the project have already been deployed. |

| Parameter | Description |
| --- | --- |
| | The icon is a grey pause symbol.<br>• Not reaching the final status: It indicates that a certain SR has not reached the final status due to some reason after the project reaches the final status for the first time.<br>The icon is a red tick.<br>• Inspection alarm: It indicates that an error is detected on a service instance under the project during the inspection.<br>The icon is a yellow exclamation mark. |
| Start Time | Time when Apsara Infrastructure Management Framework deployment starts. |
| Total Progress | It indicates the ratio of SRs under all projects that reach the final status to SRs under all projects. |
| Deployment Status | The time of each of the following statuses indicates the deployment duration: Reaching the final status, To be deployed, Deploying, and Inspection alarm.<br>The time of Not reaching the final status indicates duration before the final status is reached.<br>You can click the time to view the detailed information. |
| Deployment Progress | It indicates the ratio of clusters, services, or SRs under a project that reach the final status to the total clusters, services, or SRs.<br>You can click **Details** to view the deployment statuses of clusters, services, and SRs. The deployment statuses are indicated by icons, which are the same as those used for status statistics. |
| Resource Application Progress | "Total" indicates the total number of resources related to a project.<br>• Done: Number of resources that have been successfully applied for. |

| Parameter | Description |
| --- | --- |
| | • Doing: Number of resources that are being applied for or retried. The number of retries (if any) is displayed next to the number of resources.<br>• Block: Number of resources of which the applications are blocked by other resources.<br>• Failed: Number of resources of which applications fail. |
| Inspection Error | It indicates the number of inspection alarms generated for the current project. |
| Alarm Info. | It indicates the number of alarms generated for the machine monitor and the machine SR monitors in the current project. |
| Dependency | Click the icon. The following dependency information of a project is displayed: services that depend on other services, and current deployment statuses of services that are depended on. |

## 2.2.10 Alarm center

**Monitoring status**

Select **Monitoring** > **Alarm Status**.

On the **Alarm Status** page, select clusters and services from the drop-down lists and set the start time and end time to view the status of all the clusters and services 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 Product component information

Provides the running status of services and server roles (SRs) on the machine under each cluster of the product.

- Product: Product name.
- Cluster: Cluster name.
- Service: Service name.
- Server role: Server role name.
- SR State: Running state of an SR on the machine.
- SR Action: Action of the SR on the machine.Data is available only when Apsara Infrastructure Management Framework requests the SR to perform certain actions, such as rolling and restart .
- Machine: Host name of the machine.
- IP: IP address of the machine.
- Machine State: Running state of the machine.
- Machine Action: Action that Apsara Infrastructure Management Framework requests the machine to perform, such as clone.

### 2.2.11.2 Product component current status

Provides the status of all SRs in an abnormal state on the machine, and monitoring information (i.e. alert information written by the SR to the Apsara Infrastructure Management Framework monitor) of SRs and machine.

- Product state components in an abnormal state: Only the SRs that are not in GOOD state and SRs to be upgraded are displayed.
  - project: Product name.
  - cluster: Cluster name.
  - service
  - serverrole: Name of the server role.
  - machine: Machine name.
  - need_upgrade: Indicates whether the current version is the HEAD version.

- serverrole_start: SR state.
- machine_state: Machine state.

- SR alert information: Select a row from the product state components in an abnormal state, and you can filter out the monitoring information (non-good and info) of the selected SR from the table.
  - cluster: Cluster name.
  - service
  - sr; Server role.
  - machine: Machine name.
  - monitor: Monitor name of the sever role.
  - level: Alert level.
  - description: Monitor report content.
  - $updatetime: Monitor update time.
- Machine alert information: Select a row from the product state components in an abnormal state, and you can filter out the monitoring information (non-good and info) of the selected machine from the table.
  - cluster: Cluster name.
  - machine: Machine name.
  - monitor: Machine alert information.
  - level: Alert level.
  - description: Alert information.
  - updatetime: Update time.
- Inspection information: Select a row from the product state components in an abnormal state, and you can filter out the monitoring information (non-good and info) of the selected machine from the table.
  - cluster: Cluster name.
  - service
  - sr; Server role.
  - monitor: Inspection report name.
  - level
  - description: Content of the inspection report.
  - updatetime: Update time.

# 2.2.11.3 Machine view

Displays the machine-related information.

- Machine state: Displays the all machines currently managed by Apsara Infrastructure Management Framework and states of these machines.In the global filter on top of the page, you can select a machine and click the Filter button on the right to filter data.
  - machine: Machine name.
  - ip: IP address of the machine.
  - state: Machine state.
  - actionname: Action currently performed by the machine.
  - actionstatus: Action state.
  - statedescription: Machine state description.
- List of expected SRs on the machine {{Machine selected in Machine State}}: SR that should be installed on the selected machine.
  - Machine: Machine name.
  - Server role: Server role name.
- {{Machine selected in Machine State}} Non-normal monitoring item state: Monitoring information of the selected machine.
  - machine: Machine name.
  - monitor: Monitoring item.
  - level: Level of the monitoring item.
  - description: Content of the monitoring item.
  - last_modified_time: Last modification time of the monitoring item.
- Actual version and state of the SR on the machine {{Machine selected in Machine State}}: State of the SR on the selected machine.
  - machine: Machine name.
  - serverrole: SR name.
  - state: SR state.
  - expectedversion: Expected version of the SR on the machine.
  - actualversion: Actual version of the SR on the machine.
  - statedescription: Reason of the state change.
  - errormessage: SR error message.

- Monitoring state of {{Value of the **machine** column on the selected row in the **Machine{{machine}} actual SR version and status** table}} and {{Value of the **serverrole** column on the selected row in the **{Machine{machine}} actual SR version and status** table}}. It displays the monitor information of the selected SR in the **Machine {{machine}} actual SR version and status** table. Only the non-good monitor information is displayed.
  - machine: Machine information.
  - serverrole: Name of the server role.
  - monitor: Monitoring item of the SR.
  - description: Information about the monitoring item.
  - level: Monitoring level.
  - last_modified_time: Monitor update time.

## 2.2.11.4 Machine role action report

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

- Machine role action state: Only machines with actions are displayed.
  - Product: Product name.
  - Cluster: Cluster name.
  - Machine: Host name of the machine.
  - ip: IP address of the machine.
  - Machine State: Running state of the machine.
  - Machine Action: Action that Apsara Infrastructure Management Framework requests the machine to perform, such as clone.
  - SR: Service name plus the SR name.
  - Role State: Running state of the SR.
  - Role Action: action of the SR on the machine, such as rolling, restart, and offline.
- Action status of the SR on the VM of the host ({{machine}}).

If you select any row in the machine role action state table, the host name in the selected row can be used as a filter condition to filter out information about VMs running on the selected machine. Data is available only when the selected machine is a host.

- VM: Host name of the VM.
- ip: IP address of the VM.
- Machine State: Running state of the VM.
- Machine Action: Action performed by the machine, such as clone.
- SR: SR running on the VM.
- Role State: Running state of the SR.
- Role Action: action of the SR on the machine, such as rolling, restart, and offline.

## 2.2.11.5 Machine clone report

Displays the machine clone state information.

- Machine clone progress
  - project: Product name.
  - cluster: Cluster name.
  - machine: Machine name.
  - state: Machine state.
  - Clone Progress: Progress of the current clone process.
- Machine clone state
  - project: Product name.
  - cluster: Cluster name.
  - machine: Machine name.
  - actionname: Apsara Infrastructure Management Framework action currently performed by the machine.
  - actionstatus: Action state.
  - state: Machine state.
  - level: Whether the clone action performed by the machine is normal.
  - clone state: Current state of the clone action performed by the machine.

## 2.2.11.6 Service inspection report

For a cluster in the global filter, you can obtain the service inspection report of this cluster by filtering the inspection report table.

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

- project: Product name.
- cluster: Cluster name.
- service
- description: Content of the inspection report
- level: Inspection report level.

## 2.2.11.7 Resource application report

In the global filter, you can select a cluster and click **Filter** to filter out the resource application data of this cluster from the table below.

- Change mapping table, from which resource change applications in the cluster can be detected.
  - project: Product name.
  - cluster: Cluster name.
  - version: Changed version.
  - resourceprocessstatus: Application status of the resource in the version.
  - msg: Exception information.
  - begintime: Start time of change analysis.
  - endtime: End time of change analysis.
- List of resources corresponding to changes
  - res: Version of the change.
  - type: Resource type.
  - name: Resource name.
  - owner: Application to which the resource belongs.
  - parameters: Resource parameters.
  - ins: Resource instance name.
  - instance_id: ID of the resource instance.
- List of resources corresponding to changes, indicating the states of resources in the cluster.

- project: Product name.
- cluster: Cluster name.
- service
- serverrole: Name of the server role.
- app: App of the server role.
- name: Resource name.
- type: Resource type.
- status: Resource application status.
- parameters: Resource parameter.
- result: Resource application result.
- res: Resource ID.
- reprocess_status: Status of interaction with Yaochi during VIP resource application.
- reprocesss_msg: Error messages of interaction with Yaochi during VIP resource application.
- reprocess_result: Result of interaction with Yaochi during VIP resource application.
- refer_process_list: Version that uses the resource.
- error_message: Exception information.

## 2.2.11.8 Rolling job query

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

- You need to select Rolling. The table displays only the rolling jobs that are currently running.If no job is in Running state, no data is displayed in this table.
  - Cluster: Cluster name.
  - Git version: Version, the change of which triggers the rolling job.
  - Description: Change description entered by a user when the user submits a change.
  - Start Time: Start time of the job.
  - End Time: End time of the job.
  - Submitter: ID of the user who submits the change.
  - State: Job running state.
  - submittime: Time that the change is submitted.
- Rolling-associated SR list: Select Rolling, and then select a rolling job. In this table, you can filter out information about the rolling states of SRs related to the selected job.If no rolling job is selected, the states of SRs in all the historical rolling jobs are displayed.

- Server Role: Name of the server role.
- State: Rolling state of the SR.
- Error Message: Error message of the rolling job.
- Git_version: Version to which the change belongs.
- Start Time: Rolling start time.
- End Time: Rolling end time.
- Approval Rate: Ratio of machines, rolling of which is approved in the rolling process.
- Failure Rate: Ratio of machines that encounter rolling failures.
- Success Rate: Ratio of machines that succeed in rolling.

- SRI upgrade info: Source version and target version of each application under the SR in the rolling process.
  - app: Name of the application under the SR that should participate in rolling.
  - sri_name: SR to which the application belongs.
  - from_build: Source version of the upgrade.
  - to_build: Target version of the upgrade.
- SRI state of each machine in the cluster: Select an SR from the rolling-associated SR list, and you can filter out the state of this SR deployed on the machine.
  - machine: Name of the machine on which the SR is deployed.
  - expectedversion: Target version of the rolling process.
  - actualversion: Current version.
  - state: SR state.
  - actionname: Apsara Infrastructure Management Framework action currently performed by the SR.
  - actionstatus: Action state.

## 2.2.11.9 VM mapping

For a cluster in the global filter, you can obtain information about VMs in this cluster by filtering the VM mapping table.

VM mapping table: Displays the information about VMs in the cluster. Data is available in this table only when VMs are deployed in the cluster.

- project: Product name.
- cluster: Cluster name.

- VM: Host name of the VM.
- Actually Deployed VM: Host name of the physical machine of the currently deployed VM.
- Expected deployed VM: Host name of the physical machine of the expected VM.

## 2.2.11.10 Service dependency

Presents the dependency among server roles (SRs). In the global filter, you can select a cluster and filter the table to obtain the desired cluster data.

- Product: Product name.
- Cluster: Cluster name.
- Service: Service name.
- Server role: Server role name.
- Dependent service: Service on which the server role depends.
- Dependent server role: 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 Service registration variables

Displays values of all service registration variables.

Service registration variables include:

- service
- service_registration: Service registration variable.
- cluster: Cluster name.
- $updatetime: Update time.

## 2.2.11.12 Network topology check

Checks whether any wirecheck alarms are generated for the network devices or machines.

- Network device topology check: Checks whether any wirecheck alarms are generated for the network devices.
  - cluster: Cluster name.
  - n: Name of the network device.
  - level: Alert level.

- description: Alert information.

- Server topology check: Checks whether any wirecheck alarms are generated for servers (machines).
  - cluster: Cluster name.
  - machine: Machine (server) name.
  - level
  - description: Alert description.

## 2.2.11.13 Machine RMA pending approval list

Some Apsara Infrastructure Management Framework actions of the machines and server roles (SRs) can be triggered by users in a way similar to restart, but this type of action must be reviewed and approved.This report is used to process the actions that must be reviewed and approved.

- machine
  - Project: Product name.
  - Cluster: Cluster name.
  - Hostname: Host name of the machine.
  - IP: IP address of the machine.
  - State: Machine running state.
  - Action Name: Action on the machine.
  - Action Status: State of the action on the machine.
  - Operation: Approval button.
- machine_serverrole
  - Project: Product name.
  - Cluster: Cluster name.
  - Hostname: Host name of the machine.
  - IP: IP address of the machine.
  - Serverrole: Name of the server role.
  - State: SR running state.
  - Action Name: Action on the SR.
  - Action Status: State of the action on the SR.
  - Operation: Approval button.

- machine_component
  - Project: Product name.
  - Cluster: Cluster name.
  - Hostname: Host name of the machine.
  - Component: Hard disk on the machine.
  - State: Hard disk running state.
  - Action Name: Action on the hard disk.
  - Action Status: State of the action on the hard disk.
  - Operation: Approval button.

## 2.2.11.14 Automatic recovery – Installation pending approval list

The structure of this table is consistent with that of the RMA pending approval list, except that this view is used to approve the machine installation.

## 2.2.11.15 Cluster on/off monitoring report

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.
  - Product: Product name.
  - Cluster: Cluster name.
  - On/Off State: On/off action that is being performed by the cluster.
- {{Select a cluster from the cluster running state table}} SR On/Off State: On/off state of the SR of the cluster selected from the report on the left.
  - Cluster: Cluster name.
  - SR: SR information.
  - On/Off State: On/off state of the SR.
- {{Select an SR from table 2}} machine state: Displays the machine running state of the selected SR.
  - Cluster: Cluster name.
  - Server role: Server role name.
  - Machine: Machine name.

  - SR State: Running state of the SR.
  - actionname: Action currently performed by the SR.
  - actionstatus: Action state.
  - errormessage: SR error message.
- {{Select a cluster from the cluster running state table}} machine state: Displays the machine running state of the selected cluster.
  - Cluster: Cluster name.
  - Machine: Machine name.
  - IP: IP address of the machine.
  - Machine State: Running state of the machine.
  - actionname: Action currently performed by the machine.
  - action_status: Machine action state.
  - error_message: Exception information.

## 2.2.11.16 Apsara Stack service alert status dashboard

Provides statistics of the alert amount and level of Monitoring System.

- Alert Amount per Hour: Amount of alerts reported by Monitoring System.
- Service Health Status Distribution: ServiceTest#SR monitoring and alert statistics.
- SR Health Status Distribution: post_check monitor monitoring and alert statistics.
- Hardware Health Status Distribution-ServerRole：Monitoring of the machine monitoring item independent_domain_check_syslog_sh.

## 2.2.11.17 Thermometer

Displays the cluster and machine load statistics in the environment.

- Physical machine CPU distribution.

  The load distribution of physical machines is displayed. A darker color indicates a higher load.
- Cluster load ranking:

  Cluster list sorted by load.
- Cluster CPU usage ranking
- Cluster memory usage ranking

## 2.2.11.18 Project-based O&M

Displays the monitoring attributes based on projects monitored by Monitoring System.

- Project read-data count
  - Time: Data update time.
  - project: Project name.
  - readCount: Amount of read data of the project.
- Shard sequence: Shard information list.
  - Time: Recording time.
  - project: Project name.
  - key: Shard name.
  - readCount: Amount of read data of the shard.
  - uuid：Shard ID.
  - latency: Shard processing delay.
- partition
  - Time: Data update time.
  - project: Project name.
  - key: Partition name.
  - readCount: Amount of read data of the partition.
  - uuid：Partition ID.
  - discardÇount: Amount of discarded data.
- Traffic: Amount of read data of the project.
- Latency: Project read delay.
- readCount: Statistics of read data of the project.
- ots: Output amount of the project compute node.
- Compute unit: Statistics of the compute unit.
- Exception: Exception statistics.

## 2.2.11.19 AGG node O&M

Displays the information about the compute nodes of Monitoring System.

- Compute node ranking
  - Time: Data update time.

  - address
  - readCount: Number of times data is read.
  - uuid: Compute node ID.
  - cacheCount: Data cache count.
- CU comparison
  - Time: Data recording time.
  - address: Node address.
  - computerUnit: Number of compute units.
- In/out flow: Statistics of incoming and outgoing traffic of the compute node.
- computeUnit: Compute units of the compute node.
- Exception: Computing failure statistics.
- Partition list
  - Time: Data update time.
  - uuid：Partition ID.
  - key: Partition name.
  - computerUnit: Compute units of the partition.
- Partition running info.

## 2.2.11.20 Source node O&M

Displays the information about the source nodes of Monitoring System.

- List of source nodes sorted by traffic
  - Time: Recording time.
  - address: Node address.
  - inflow: Incoming traffic.
  - uuid: Source node ID.
- Read-data count, indicating the load of a node
  - Time: Recording time.
  - address: Node address.
  - readCount: Number of times data is read.
- In/out flow: Incoming and outgoing traffic statistics.
- In/out count: Total read or compute count.

- Abnormal indicator: Abnormal data statistics.
- Source recorded slsshard latency: Recorded SLS shard delay.
- Endpoint list: Number of times that the endpoint sends data to the source.

## 2.2.11.21 Container monitoring - cluster

- Load
- CPU
- Memo
- Disk Uasge
- Traffic
- TCP state
- TCP retrains
- DiskIO

## 2.2.11.22 Container monitoring - single machine

Statistical items include:

- Load
- CPU
- Memo
- Disk Uasge
- Traffic
- TCP state
- TCP retrains
- DiskIO

## 2.2.11.23 JVM monitoring - cluster

- Heap Memory
- Non-heap Memory
- GC Count-Old
- GC Count-New
- GC Time-Old
- GC Time-New
- Deadlock Info.

- Thread Info.
- Classloader
- Memory Ddetails

## 2.2.11.24 JVM monitoring - single machine

Displays the monitoring information of Java VMs on the machine. The information is used by Monitoring System.

- Heap Memory
- Non-heap Memory
- GC Count-Old
- GC Count-New
- GC Time-Old
- GC Time-New
- Deadlock Info.
- Thread Info.
- Classloader
- Memory Ddetails

## 2.2.11.25 Reference error check of service exposure variables

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 Maintenance role authorization

### 3.1.1 OAM introduction

**Overview**

Operation Administrator Manager (OAM) is a centralized permission management platform of the Alibaba Cloud Operation and Maintenance system. OAM uses a simplified role-based access control (RBAC) model. Administrators can use OAM to assign different roles to Operation and Maintenance personnel, granting them corresponding operation permissions on Operation and Maintenance 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 includes a group of permissions. Once a role is assigned to a user, the user is granted all the operation permissions of that role. Therefore, when creating a user, administrators only need 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 permission management and reducing system overhead.

### 3.1.2 Basic concepts

**Subject**

Operator of the resource access management system. OAM subjects include **`User`** and **`Group`**.

**User**

Administrators and operators of the Operation and Maintenance system.

**Group**

Set of users.

**Role**

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`**.

**Role Hierarchy**

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 Operation and Maintenance platform, see *Operation permissions of Operation and Maintenance platforms*.

**ActionSet**

Description of authorized operations. An ActionSet can contain multiple operations. For operations of Operation and Maintenance platforms, see *Operation permissions of Operation and Maintenance 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:**
The OAM system 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

**Prerequisites**

The administrator account and OAM logon address have been obtained.

**Procedure**

1. Start Chrome.
2. Enter the OAM logon address in the address box and press Enter.

   The OAM logon page is displayed.
3. Click **Primary Account**, enter the user name and password, and click **Log On**.

   **Note:**
   Users who have activated RAM can select **Primary Account** and use a subaccount to log on.

## 3.1.4 Quick start

## 3.1.4.1 Create a group

Create a user group to simplify user management.

**Context**

All users can create user groups, but only creators (group owners) can see user groups that they have created.

**Procedure**

1. Choose **Group Management** > **Managed Groups**.
2. Click **Create** in the upper-right corner of the page.

   The **Create Group** dialog box is displayed.
3. Enter the group name and description and click **OK**.

   You can choose **Group Management** > **Managed Groups** and view the groups that you have created.

## 3.1.4.2 Add group members

Add members to an existing group so you can grant permissions to them more efficiently.

操作步骤

1. Choose **Group Management** > **Managed Groups**.
2. Click **Manage** next to the target group.

   The **Group Information** page is displayed.
3. Click **Add** in the upper-right corner of the **Group Members** area.

   The **Add Member** dialog box is displayed.

4. Select the search mode, enter target information, and click **Details**. The user details are displayed.

   Three search modes are available:

   - **`AliyunPK`**: search by unique ID of the user's cloud account
   - **`RamAliasName`**: search by *subaccount name@primary account ID*

     Use this mode for users who have activated RAM.
5. Click **Add**.
6. You can repeat the preceding steps to add more group members.

   To delete a member from a group, find the member and click **Delete**.

## 3.1.4.3 Add a group role

You can assign a role to an existing group.

**Prerequisites**

- The role to be assigned has been created. For more information about how to create a role, see *Create a role*.
- The operator is the owner of the group and role.

**Procedure**

1. Choose **Group Management** > **Managed Groups**.
2. Click **Manage** next to the target group.

   The **Group Information** page is displayed.
3. Click **Add** in the upper-right corner of the **Role List** area.

   The **Add Role** dialog box is displayed.
4. Find the corresponding roles by searching for **`Role name`**, select one or multiple roles, and set the expiration time.
5. Click **OK**.

   To delete a role, find the role in the **Role List** area and click **Delete**.

## 3.1.4.4 Create a role

**Procedure**

1. Choose **Role Management** > **Managed Roles**.
2. Click **Create Role** in the upper-right corner of the **Managed Roles** page.

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

3. Enter the **Role name** and **Description** and select the **Role type**.
4. Optional: Set the role tag, which can be used for role search.
   a) Click **Edit Tag**.
   b) Click **Create Tag** on the **Edit Tag** page.
   c) Enter the **Key** and the corresponding **Value** of the tag and click **OK**.
   d) Enter other **Keys** and **Values** and click **OK** to create more tags.

      The created tags are displayed in the dotted-line box.
   e) Click **OK** to close the **Edit Tag** dialog box.
5. Click **OK** after role information editing.

## 3.1.4.5 Add an inherited role to a role

After an inherited role is added to a role, the permissions of the former are granted to the latter.

**Prerequisites**

You are the owner of the current role and the inherited role to be added.

For more information about how to query your roles, see *Query roles*.

**Procedure**

1. Choose **Role Management** > **Managed Roles**.
2. Click **Manage** next to the target role.

   The **Role Information** page is displayed.
3. Click **Add Role** on the right of **Inherited Roles**.
4. Find the corresponding roles by searching for **Role name** and select one or multiple roles.
5. Click **OK**.

## 3.1.4.6 Add resources to a role

After creating a role, you need to add resources to it.

**Procedure**

1. Choose **Role Management** > **Managed Roles**.
2. Click **Manage** next to the target role.

   The **Role Information** page is displayed.
3. Select **Resource List**.

4. Click **Add Resources**.

   The **Add Resources** dialog box is displayed.

5. Enter resource information. *Table 3-1: Key resource parameters* describes the related parameters.

   **Table 3-1: Key resource parameters**

| Parameter | Description |
| --- | --- |
| BID | Deployment region ID. |
| Product | Cloud product to be added, for example, rds.<br>**Note:**<br>The cloud product name must be lower-case. For example, enter **rds**, instead of **RDS**. |
| Resource path | For more information about resources of cloud products and Operation and Maintenance platforms, see *Operation permissions of Operation and Maintenance platforms*. |
| Action | Action set. An action set can contain multiple actions.<br>For operations of Operation and Maintenance platforms, see *Operation permissions of Operation and Maintenance platforms*. |
| Authorization 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. |
| Description | Resource description. |

6. Click **OK**.

## 3.1.4.7 Add authorized users to a role

You can assign a role to users and user groups.

**Prerequisites**

The authorized users or user groups have been created. Users are created on the cloud management platform DTCenter. For information about how to create user groups, see *Create a group*.

**Procedure**

1. Choose **Role Management** > **Managed Roles**.
2. Click **Manage** next to the target role.

   The **Role Information** page is displayed.
3. Select **Authorized User List**.
4. Click **Add Authorized User**.

   The **Add Authorized User** dialog box is displayed.
5. Select the search mode and enter target information.

   Three search modes are available:

   - **`AliyunPK`**: search by unique ID of the user's cloud account
   - **`RamAliasName`**: search by *subaccount name@primary account ID*

     Use this mode for users who have activated RAM.
   - **`Group Name`**: search by group name

   **Note:**
   You can search for a single user or user group. For information about how to create a user group, see *Create a group*.
6. Optional: Click **Details** to view the user information or user group information.
7. Set the permission expiration time.

   After the expiration time is reached, the user does not have the permissions of the role any more. To authorize the user again, the role creator needs to find the authorized user in the **Authorized User List**, click **Renew**, and set the new expiration time.
8. Click **Add** to assign the role to the user.

   To cancel the authorization, find the authorized user in the **Authorized User List** and click **Remove**.

## 3.1.5 Manage a group

## 3.1.5.1 Modify group information

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

**Procedure**

1. Choose **Group Management** > **Managed Groups**.
2. Click **Manage** next to the target group.

   The **Group Information** page is displayed.
3. Click **Edit** in the upper right corner.
4. Modify the group name and description on the **Modify Group** dialog box that is displayed.
5. Click **OK**.

## 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 assigned to the group.

**Procedure**

1. Choose **Group Management** > **Managed Groups**.
2. Click **Manage** next to the target group.

   The **Group Information** page is displayed.
3. Find the role in the **Role List** area and click **Details**.

   The **Role Information** page is displayed.
4. You can perform the following operations on the **Role Information** page:

   - Click **Inherited Roles** and view information about the inherited roles.

     To view detailed information about an inherited role, find the role on the **Inherited Roles** tag page and click **Details**.

     For more information about how to add an inherited role.
   - Click **Resource List** and view resource information of the role.

     For more information about how to add resources to a role.

- Click **Inheritance Tree**, view the basic information and resource information of a role and its inherited roles on the inheritance tree on the left.

## 3.1.5.3 Delete a group

Based on your needs, you can delete a group when it is no longer required.

**Prerequisites**

Before deleting a group, ensure that it does not contain any member.

**Procedure**

1. Choose **Group Management** > **Managed Groups**.
2. Select a group, and click **Delete**.

## 3.1.5.4 View assigned groups

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

**Context**

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

**Procedure**

1. Choose **Group Management** > **Assigned Groups**.
2. On the **Assigned Groups** page, you can view the names, owners, description, and modification time of the groups to which you belong.

## 3.1.6 Manage roles

## 3.1.6.1 Query roles

You can view the roles that you and your group have on the **Managed Roles** page.

**Procedure**

1. Choose **Role Management** > **Managed Roles**.
2. Select the display mode, that is, to display the roles of the current user or the current user's group.

   By default, roles of the current user are displayed.
3. Optional: Enter the target role name.
4. Click **Search**.

**Note:**

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

## 3.1.6.2 Modify role information

You can modify information about a role that you have created.

**Procedure**

1. Choose **Role Management** > **Managed Roles**.
2. Click **Manage** next to the target role.

   The **Role Information** page is displayed.
3. Click **Edit** in the upper right corner.
4. Modify the name, description, type, and tag information of the role on the **Modify Role** dialog box that is displayed.
5. Click **OK**.

## 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. Choose **Role Management** > **Managed Roles**.
2. Click **Manage** next to the target role.

   The **Role Information** page is displayed.
3. Choose **Inheritance Tree**.
4. In the left-hand inheritance tree, you can view the basic information and resource information of a role and its inherited roles.

## 3.1.6.4 Transfer a role

You can transfer a role to other groups or users.

**Procedure**

1. Choose **Role Management** > **Managed Roles**.
2. Enter the search criteria to search for the role to be transferred.
3. Select one or multiple roles in the search results and click **Transfer**.
4. Select the search mode, enter target information, and click **Details** on the **Transfer** page. The user information or user group information is displayed.

Three search modes are available:

- **`AliyunPK`**: search by unique ID of the user's cloud account
- **`RamAliasName`**: search by *subaccount name@primary account ID*

  Use this mode for users who have activated RAM.
- **`Group Name`**: search by group name

5. Click **Transfer** to transfer the role to the user or user group.

## 3.1.6.5 Delete a role

Based on your business needs, you can delete a role when it is no longer required.

**Prerequisites**

Before deleting a role, ensure that it has no inherited roles, authorized users, or resources.

**Procedure**

1. Choose **Role Management** > **Managed Roles**.
2. Click **Delete** next to the role to delete it.

## 3.1.6.6 View assigned roles

After logging on to the system, you can view the roles assigned to you and permissions granted to the roles.

**Procedure**

1. Choose **Role Management** > **Assigned Roles**.
2. On the **Assigned Roles** page, you can view the names, owners, description, modification time, and expiration time of the roles assigned to you.
3. Click **Details** for a role to view its inherited roles, resources, and inheritance tree information.

## 3.1.6.7 View all roles

The **All Roles** page allows you to view information about all roles in the OAM system.

**Procedure**

1. Choose **Role Management** > **All Roles**.
2. On the **All Roles** page, view all the roles in the system.

   You can enter a **`role name`** in the search box on the page to search for a role.
3. Click **Details** to view the inherited roles, resources, and inheritance tree information for a role.

## 3.1.7 Search resources

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

**Procedure**

1. Choose **Role Management** > **Search Resources**.
2. Enter the **`resource description`** and **`action`** in the search box, and click **Search** to search for roles that meet the conditions.
3. After the search result is displayed, click **Details** to view the inherited roles, resources, and inheritance tree information for a role.

## 3.1.8 View personal information

The **Personal Information** page allows you to view your personal information and perform permission tests.

**Procedure**

1. On the left-hand navigation pane, choose **Personal Information**.
2. In the **Personal Information** area, you can view your user name, user type, creation time, AccessKey ID, and AccessKey Secret.

   **Note:**
   Click **Display** or **Hide** to display or hide AccessKey Secret.
3. In the **Permission Test** area, perform a permission test to check whether you have a certain permission.
   a) In the **`Resource Description`** text box, enter the resource information.
   b) In the **`Action`** text box, enter a permission, such as create, read, and write. Separate multiple permissions with commas.
   c) Click **Permission Test**.

## 3.1.9 Typical applications

## 3.1.9.1 Assign a default role to a user

**Prerequisites**

The user ID of Alice has been obtained.

**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 for managing all database instances.

**Procedure**

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

   For more information about how to log on to the OAM system, see *Log on to OAM*.

2. Assign the **rds_instance administrator** role to Alice.
   a) Choose **Role Management** > **Managed Roles**.
   b) Find the **rds_instance administrator** role and click **Manage**.

      The **Role Information** page is displayed.
   c) Select **Authorized User List**.
   d) Click **Add Authorized User**.

      The **Add Authorized User** dialog box is displayed.
   e) Select **AliyunPK** from the drop-down list box next to **Search**, enter Alice's user ID, and click **Details**.
   f) Set the expiration time.
   g) Click **Add** and assign the **rds_instance administrator** role to Alice.

## 3.1.9.2 Use groups and RoleHierarchy

**Context**

Scenario:

With further development of cloud computing, the database instance count and Operation and Maintenance workload have significantly increased. As the DBA, Alice often needs to check the system status in Dukang. 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 assigning permissions to each employee while preventing permission granting 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 more information about how to log on to the OAM system, see *Log on to OAM*.

2. Create the **rds_senior DBA** role.

   For more information about how to create a role, see *Create a role*.

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

   For more information about how to do this, see *Add an inherited role to a role*.

4. Create (as Alice) the **Common DBA** and **Senior DBA** group.

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

   b) Create the **Common DBA** and **Senior DBA** groups. For more information about how to do this, 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) For more information about how to assign the **rds_instance administrator** role to the **Common DBA** group, see *Add a group role*.

   c) For more information about how to assign the **rds_senior DBA** role to the **Senior DBA** group, see *Add a group role*.

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) For more information about how to add Alice and Bob to the **Senior DBA** group, see *Add group members*.

   c) For more information about how to ad Dave to the **Common DBA** group, see *Add group members*.

## 3.1.9.3 Use custom roles

**Context**

Scenario:

Carol, from the internal audit team of the company, needs to log on to the systems and view the statistical data in the Dukang and Chiji systems to check whether the earlier data reports are true.

**Procedure**

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

   For more information about 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 operation is **`["HOME", "RDS_HOME"]`**, and the WithGrantOption is **`0`**. For more information, see *Add resources to a role*.

4. When assigning OSS permissions to the **`Internal audit only`** role, include the **`OSS_public permissions`** role, which has all the required OSS permissions, in the **`Internal audit only`** role.

   Add the **`OSS_public permissions`** role, as an inherited role, to the **`Internal audit only`** role. For more information, see *Add an inherited role to a role*.

5. Assign the **`Internal audit only`** role to Carol. For more information, see *Add authorized users to a role*.